



UNIONE TERRED'ACQUA

Costituita fra i Comuni di:

Anzola dell'Emilia
Calderara di Reno
Crevalcore
Sala Bolognese
San Giovanni in Persiceto
Sant'Agata Bolognese

DELIBERAZIONE DELLA GIUNTA DELL'UNIONE NR. 30 DEL 30/06/2025

OGGETTO: APPROVAZIONE DEL MANUALE DI GESTIONE DEL PROTOCOLLO, DEI FLUSSI DOCUMENTALI E DELL'ARCHIVIO.

Il giorno **30 giugno 2025**, alle ore **15:30**, in modalità audio/video conferenza, si è riunita la Giunta dell'Unione.

Risultano presenti:

	Componente	Qualifica	Presente
1	MARTELLI MARCO	PRESIDENTE	SI
2	PELLEGATTI LORENZO	COMPONENTE	SI
3	FALZONE GIAMPIERO	COMPONENTE	SI
4	BASSI EMANUELE	COMPONENTE	SI
5	IOVINO PAOLO	COMPONENTE	SI
6	ARGENIO HUPPERTZ DIANA	COMPONENTE	SI

Il **Presidente, MARTELLI MARCO**, riconosciuta legale l'adunanza ai sensi dell'art. 25 dello Statuto dell'Unione, invita la Giunta a prendere in esame l'oggetto sopra indicato.

Partecipa il **SEGRETARIO DELL'UNIONE, LAURENZANO LUCA**, il quale provvede alla redazione del presente verbale.



OGGETTO:

APPROVAZIONE DEL MANUALE DI GESTIONE DEL PROTOCOLLO, DEI FLUSSI DOCUMENTALI E DELL'ARCHIVIO.

LA GIUNTA DELL'UNIONE

Premesso:

- Il presente Manuale di gestione del sistema documentario (d'ora in poi Manuale) è adottato ai sensi del paragrafo 3.5 delle Linee Guida sulla formazione e conservazione dei documenti informatici di AGID (d'ora in poi LL. GG.) per la gestione delle attività di formazione, registrazione, classificazione, fascicolazione, gestione e conservazione dei documenti, oltre che la gestione dei flussi documentali e dei procedimenti dell'Amministrazione;
- che ai sensi del DPCM 3 dicembre 2013 le Pubbliche Amministrazioni devono adeguare i loro sistemi di gestione documentale alle Regole tecniche in esso contenute;
- che l'intento del DPCM è quello di introdurre concretamente modificazioni organizzative ed operative e disciplinare la realizzazione di una gestione completamente informatica dei flussi documentali e che lo strumento attraverso cui ottenere tale riforma è il Manuale di gestione;

Tenuto conto del testo del Manuale di gestione attualmente in uso, per il quale si ritiene di prevedere una nuova struttura aggiornata, articolata in capitoli, paragrafi e punti;

Richiamati:

- il DPR 28/12/2000, n.445 recante "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa";
- la Direttiva del 9/12/2002 del Ministro per l'innovazione e le tecnologie recante "Direttiva sulla trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali";
- Il DPCM 14/10/2003 pubblicato sulla G.U. del 25/10/2003, concernente l'Approvazione delle Linee guida per l'adozione del Protocollo informatico e per il trattamento informatico dei procedimenti amministrativi";
- il Codice dell'Amministrazione Digitale – CAD – approvato con D. Lgs. n. 82/2005 e s.m.i.;
- il DPCM 03/12/2013 ad oggetto "Regole tecniche per il protocollo informatico ai sensi degli articoli 40 – bis, 41, 47, 57 – bis e 71 del Codice dell'Amministrazione Digitale di cui al D.Lgs. n. 82/2005;
- il DPCM 13/11/2014 avente ad oggetto "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-

DELIBERAZIONE DI GIUNTA DELL'UNIONE NR.30 DEL 30/06/2025

- ter, 40, comma 1, 41, e 71 del Codice dell'amministrazione digitale di cui al D.Lgs. n. 82/2005;
- Regolamento europeo eIDAS 910/2014 del Parlamento europeo del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;
 - Circolare n. 41 del 14 dicembre 2015 della Direzione Generale Archivi (*Autorizzazione alla distruzione di originali unici riprodotti secondo le regole tecniche di cui al DPCM 13.11.2014 e conservati secondo le regole tecniche di cui al DPCM 13.12.2013*);
 - Regolamento europeo 679/2016 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
 - Circolare AgiD n. 2 del 18 aprile 2017 (*«Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)»*);

Ritenuto opportuno dotarsi del Manuale di gestione del protocollo e dei flussi documentali e dell'archivio, adeguato alle più recenti normative in materia come sopra richiamate, approvando il medesimo come da allegato A) al presente atto;

Ritenuto di individuare nel Responsabile del Servizio Segreteria il responsabile per la tenuta del protocollo informatico, della gestione dei flussi documentali e dell'archivio ai sensi dell'art. 61 del D.P.R. n. 445/2000;

Visti:

- il D.Lgs. n. 267/2000;
- il D.Lgs. n. 165/2001;
- il D.Lgs. n. 118/2011;
- il D.Lgs. n. 33/2013;
- la Delibera di Giunta n. 12 del 10/05/2022 che ha approvato "la Disciplina per il funzionamento della Giunta Unione", in particolare art. 5 che ha normato le "Sedute in modalità telematica";
- il regolamento sull'ordinamento generale degli uffici e dei servizi;

Dato atto che il presente provvedimento non ha riflessi diretti o indiretti sulla situazione economico-finanziaria o sul patrimonio dell'ente, ai sensi degli artt. 49, comma 1 e 147 bis, comma 1 del D.Lgs. n. 267/2000, per cui non viene richiesto il parere di regolarità contabile;

Acquisito il parere favorevole, firmato digitalmente, espresso sulla proposta di deliberazione n. 37/2025 dalla Responsabile del Servizio Segreteria Affari Generali,

DELIBERAZIONE DI GIUNTA DELL'UNIONE NR.30 DEL 30/06/2025

dott.ssa Nadia Marzano, in ordine alla regolarità tecnica e correttezza amministrativa, ai sensi degli artt. 49, comma 1, e 147 bis, comma 1, del D. Lgs. n. 267/2000;

Con voti UNANIMI FAVOREVOLI, espressi in forma palese,

DELIBERA

per tutto quanto in premessa esposto:

1) di approvare il nuovo Manuale di gestione del protocollo, dei flussi documentali e dell'archivio, che unitamente ai relativi allegati da 1 a 6 di cui si compone, si allega al presente atto per formarne parte integrante e sostanziale (allegato A);

2) di dare atto che il Manuale di gestione è strumento di lavoro necessario alla corretta tenuta del protocollo ed alla gestione del flusso documentale e dell'archivio, e pertanto dovrà essere aggiornato quando innovazioni tecnologiche, nuove situazioni organizzative o normative lo richiedano o, comunque, ogni qualvolta si renda necessario alla corretta gestione documentale;

3) di provvedere alla pubblicazione del Manuale sul sito internet dell'Unione.

Stante l'urgenza di rispettare la scadenza del 30/06/2025 indicata dalle Linee Guida dell'Agid, la presente deliberazione con voti UNANIMI FAVOREVOLI, espressi in forma palese, viene dichiarata immediatamente eseguibile, ai sensi dell'art. 134, comma 4, del D.Lgs n. 267/00.

Allegati:

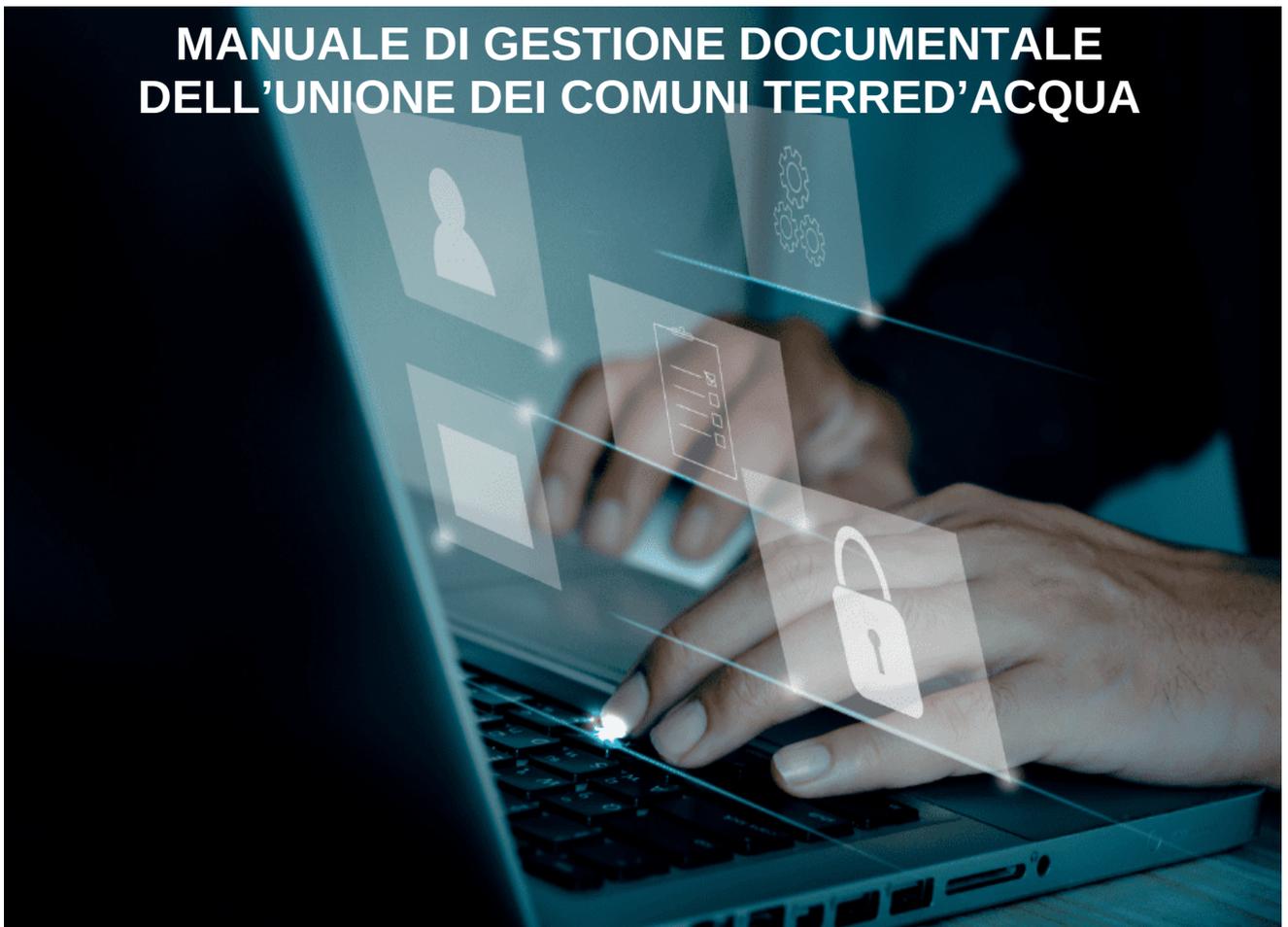
- *Allegato A-Manuale di gestione del protocollo, dei flussi documentali*
- *Allegato n. 1 - Riferimenti normativi;*
- *Allegato n. 2 - Documenti dell'Unione dei comuni di Terred'Acqua soggetti a registrazione particolare ed esclusi dalla protocollazione ed elenco dei relativi registri;*
- *Allegato n. 3 – Titolario dell'Unione dei comuni di Terred'Acqua;*
- *Allegato n. 4 - Manuale di conservazione dell'Unione dei comuni di Terred'Acqua che riversa su ParER;*
- *Allegato n. 5 - Disciplinare tecnico per lo svolgimento della funzione di conservazione dei documenti informatici da parte del conservatore Regione Emilia-Romagna (Servizio Polo Archivistico dell'Emilia Romagna – ParER);*
- *Allegato n. 6 - Piano della sicurezza informatica del Sistema di gestione informatica dei documenti dell'Unione dei comuni di Terred'Acqua.*



UNIONE TERRED'ACQUA

CITTÀ METROPOLITANA DI BOLOGNA

**MANUALE DI GESTIONE DOCUMENTALE
DELL'UNIONE DEI COMUNI TERRED'ACQUA**



Adottato con Delibera di Giunta n. 30 del 30/06/2025

1 Il Manuale di gestione documentale.....	4
1.1 Ambito di applicazione.....	4
1.2 Modalità di redazione, pubblicazione ed aggiornamento.....	4
2 Aspetti organizzativi.....	4
2.1 Area Organizzativa Omogenea e Unità Organizzative Responsabili.....	4
2.2 Domicilio digitale.....	5
2.3 Indice dei domicili digitali delle pubbliche amministrazioni.....	5
2.4 Il Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi e modalità di utilizzo della componente «sistema di protocollo informatico».....	5
2.5 Il Responsabile della gestione documentale.....	6
3 Redazione e formazione dei documenti amministrativi.....	7
3.1 Informazioni minime previste.....	7
3.2 Formazione dei documenti amministrativi informatici.....	7
3.2.1 Formati dei documenti amministrativi informatici.....	9
3.2.2 Firme e sigilli elettronici.....	9
3.2.3 Validazione temporale elettronica.....	10
3.3 Duplicati informatici.....	11
3.4 Copie ed estratti informatici.....	11
3.5 Copie analogiche di documenti amministrativi informatici.....	12
4 Gestione documentale.....	12
4.1 Le fasi di vita dell'archivio: archivio corrente, archivio di deposito e archivio storico.....	13
4.1.1 Archivio corrente.....	13
4.1.2 Archivio di deposito.....	13
4.2 Ricezione e trasmissione dei documenti.....	14
4.2.1 Modalità di ricezione e trasmissione dei documenti analogici.....	14
4.2.2 Modalità di ricezione e trasmissione dei documenti informatici.....	14
4.3 Registrazione informatica dei documenti.....	15
4.3.1 Registrazione e segnatura di protocollo.....	15
4.3.2 Il Registro giornaliero di protocollo.....	17
4.3.3 Annullamento e modifica delle informazioni registrate nel registro di protocollo.....	17
4.3.4 Registro di protocollo di emergenza.....	17
4.3.5 Registrazione di protocollo: casistiche e comportamenti.....	18

4.3.6 Registrazione particolare.....	20
4.4 Scansione dei documenti pervenuti su supporto analogico.....	20
4.5 Classificazione dei documenti.....	20
4.6 Assegnazione dei documenti.....	21
4.7 Formazione delle aggregazioni documentali informatiche.....	21
4.7.1 I fascicoli.....	21
4.7.2 Le serie.....	22
4.8 I metadati.....	22
4.9 Flussi di lavorazione dei documenti.....	22
4.9.1 Flusso di lavorazione dei documenti in ingresso.....	22
4.9.2 Flusso di lavorazione dei documenti in uscita.....	22
4.9.3 Flusso di lavorazione dei documenti interni.....	23
4.10 Pubblicazione dei documenti all'albo pretorio online.....	23
4.10.1 Ambito di applicazione.....	23
4.10.2 Principi e finalità.....	23
4.10.3 Servizio albo pretorio.....	23
4.10.4 Acquisizione dei documenti da parte degli utenti.....	23
4.10.5 Modalità di pubblicazione dei documenti.....	23
4.10.6 Annullamento della pubblicazione.....	24
4.10.7 Competenze e responsabilità.....	24
4.10.8 Gestione del servizio per la pubblicazione di atti su richiesta di terzi.....	24
4.10.9 Registro dell'Albo pretorio e attestazione di pubblicazione.....	24
5 Conservazione dei documenti.....	25
5.1 Conservazione dei documenti amministrativi su supporto analogico: l'Archivio storico.....	25
5.2 Conservazione dei documenti amministrativi informatici: il sistema di conservazione.....	25
6 Sicurezza del Sistema di gestione informatica dei documenti.....	25

Allegato n. 1 - Riferimenti normativi;
Allegato n. 2 - Documenti dell'Unione dei comuni di Terred'Acqua soggetti a registrazione particolare ed esclusi dalla protocollazione ed elenco dei relativi registri;
Allegato n. 3 - Titolare dell'Unione dei comuni di Terred'Acqua
Allegato n. 4 - Manuale di conservazione dell'Unione dei comuni di Terred'Acqua che riversa su ParER;
Allegato n. 5 - Disciplinare tecnico per lo svolgimento della funzione di conservazione dei documenti informatici da parte del conservatore Regione Emilia-Romagna (Servizio Polo Archivistico dell'Emilia Romagna - ParER)
Allegato n. 6 - Piano della sicurezza informatica del Sistema di gestione informatica dei documenti dell'Unione dei comuni di Terred'Acqua

1 Il Manuale di gestione documentale

1.1 Ambito di applicazione

Il Manuale di gestione documentale è il documento amministrativo informatico che descrive il sistema di gestione informatica dei documenti di un ente e, nel caso delle pubbliche amministrazioni, fornisce le istruzioni per il corretto funzionamento del Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi nel rispetto di quanto previsto dalla vigente normativa (allegato 1). In esso, infatti, sono descritte le modalità di formazione, gestione, trasmissione, interscambio e accesso ai documenti prodotti e acquisiti dall'ente durante l'esercizio delle proprie funzioni.

Il Manuale consiste quindi in uno strumento pratico-operativo finalizzato a guidare il personale dell'ente durante le diverse attività previste nell'ambito dei processi di formazione e gestione documentale (in particolare registrazione, classificazione e fascicolazione). Contestualmente, poiché la struttura dell'archivio deve essere progettata al fine di assicurare certezza amministrativa e trasparenza, il Manuale di gestione documentale è destinato anche ai cittadini, ai professionisti e alle imprese che si rapportano con l'ente contestualmente allo svolgimento di procedimenti amministrativi ed attività diversi.

Infine, il Manuale contiene le istruzioni per la conservazione dell'archivio, con riferimento sia alla documentazione analogica, sia a quella informatica.

1.2 Modalità di redazione, pubblicazione ed aggiornamento

Il Manuale di gestione documentale dell'Unione dei comuni di Terred'Acqua, in conformità con quanto previsto dalle Linee guida sulla formazione, gestione e conservazione dei documenti informatici adottate da Agenzia per l'Italia Digitale (d'ora in avanti Linee guida AgID), è predisposto dal Responsabile della gestione documentale, adottato con provvedimento formale (deliberazione di Giunta dell'Unione) e pubblicato sul proprio sito istituzionale, in una parte chiaramente identificabile dell'Amministrazione Trasparente.

Considerati la continua evoluzione del contesto normativo e tecnologico, e in particolare l'obsolescenza degli oggetti e degli strumenti digitali utilizzati, nonché il necessario e costante lavoro di valutazione, monitoraggio, riprogettazione e reingegnerizzazione cui devono essere sottoposti i processi e le attività di formazione e gestione documentale, il Manuale di gestione documentale è sottoposto a continuo aggiornamento.

Il presente Manuale di gestione documentale sostituisce integralmente quello precedentemente approvato con Deliberazione della Giunta dell'Unione n. 30 del 5 settembre 2016.

Per una maggiore comprensione del significato dei termini utilizzati nel presente Manuale di gestione documentale e negli allegati si rimanda all'allegato 1 alle Linee guida AgID (Glossario dei termini e degli acronimi).

2 Aspetti organizzativi

2.1 Area Organizzativa Omogenea e Unità Organizzative Responsabili

Le pubbliche amministrazioni sono tenute ad individuare, nell'ambito del proprio ordinamento, gli uffici (unità organizzative responsabili, d'ora in avanti UOR) da considerare ai fini della gestione unica o coordinata dei documenti per grandi aree organizzative omogenee (d'ora in avanti AOO), assicurando criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna tra le aree stesse, e ad adottare, per ogni AOO, il manuale di gestione documentale.

Nel caso dell'Unione dei comuni di Terred'Acqua, questa ha individuato un'unica AOO e le UOR identificate nell'Indice dei domicili digitali delle pubbliche amministrazioni (d'ora in avanti IPA).

2.2 Domicilio digitale

Per ogni AOO deve essere eletto (e pubblicato nell'IPA) almeno un domicilio digitale, inteso come l'indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio di recapito certificato qualificato valido ai fini delle comunicazioni elettroniche aventi valore legale, da cui provengono o sono trasmesse comunicazioni, istanze, dichiarazioni e notifiche che formano oggetto di registrazione di protocollo.

Con riferimento alle UOR, il loro domicilio digitale coincide con quello della AOO cui è associata, in quanto ogni UOR può essere associata ad una sola AOO.

Nel caso dell'Unione dei comuni di Terred'Acqua, sono eletti due domicili digitali presso i seguenti indirizzi di posta elettronica certificata:

- unione.terredacqua@cert.provincia.bo.it
- anticorruzione.terredacqua@cert.cittametropolitana.bo.it (utilizzato per la trasmissione e la ricezione esclusiva di comunicazioni riguardanti questioni attinenti la normativa anticorruzione)

Inoltre, è attivo il seguente ulteriore indirizzo di posta elettronica certificata, integrato con il Sistema di protocollo e dedicato alla ricezione esclusiva delle fatture elettroniche destinate all'Unione: fatturaPA.terredacqua@cert.cittametropolitana.bo.it

2.3 Indice dei domicili digitali delle pubbliche amministrazioni

In conformità con quanto previsto dalla normativa vigente per le pubbliche amministrazioni, l'Unione dei comuni di Terred'Acqua è iscritto all'IPA, che consiste nell'elenco pubblico di fiducia contenente i domicili digitali da utilizzare per le comunicazioni e per lo scambio di informazioni e per l'invio di documenti validi a tutti gli effetti di legge tra le pubbliche amministrazioni, i gestori di pubblici servizi e i privati.

Oltre al domicilio digitale, nell'IPA sono pubblicati gli ulteriori dati obbligatori previsti da Agenzia per l'Italia digitale (d'ora in avanti AgID), inseriti dall'Unione e relativi all'ente, all'AOO e alle UOR individuate. Oltre a questi, nell'IPA sono pubblicati i codici identificativi dell'ente (udctd) e dell'AOO (A04C4E4), che sono assegnati dal Gestore IPA.

2.4 Il Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi e modalità di utilizzo della componente «sistema di protocollo informatico»

Le pubbliche amministrazioni sono tenute ad istituire un servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi in ciascuna delle AOO individuate. Il Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, cui è preposto il responsabile della gestione documentale, è tenuto allo svolgimento dei compiti previsti dall'art. 61, c. 3, del DPR 445/2000. Il Servizio, oltre a vigilare sull'osservanza generale delle disposizioni normative vigenti in ambito archivistico e a garantire il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali (incluse le funzionalità di accesso e le attività di gestione degli archivi), svolge infatti le seguenti attività:

- attribuisce il livello di autorizzazione per l'accesso alle informazioni conservate nel sistema di gestione informatica dei documenti, distinguendo tra utenti abilitati alla sola consultazione ed utenti con diritti di inserimento o modifica;
- garantisce la corretta produzione e conservazione del registro giornaliero di protocollo (con le modalità descritte nel presente manuale);
- cura che le funzionalità del sistema di gestione informatica dei documenti in caso di guasti/anomalie siano ripristinate entro ventiquattro ore dal blocco delle attività e comunque nel più breve tempo possibile;
- autorizza le operazioni di annullamento delle registrazioni di protocollo.

L'Unione dei comuni di Terred'Acqua ha istituito il predetto servizio nell'ambito del Servizio Segreteria Affari generali.

Al fine dello svolgimento dei compiti previsti dalla normativa, il Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi sfrutta le funzioni del sistema di protocollo, la componente del Sistema di gestione informatica dei documenti dell'Unione dei comuni di Terred'Acqua fornita dalla società Datagraph Srl che consente:

- lo svolgimento delle operazioni di registrazione, segnatura di protocollo e classificazione;
- la gestione dei flussi documentali, la conservazione e l'accesso alle informazioni;
- il rispetto delle disposizioni in materia di sicurezza predisposte da AgID e dagli altri organismi preposti e in materia di protezione dei dati personali garantendo
 - l'univoca identificazione e autenticazione degli utenti;
 - la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
 - il tracciamento permanente di qualsiasi evento di modifica delle informazioni trattate e del suo autore.

2.5 Il Responsabile della gestione documentale

L'Unione dei comuni di Terred'Acqua, così come previsto dalla vigente normativa, ha formalmente nominato, in seno all'unica AOO individuata, il proprio responsabile della gestione documentale, definendone le attribuzioni. In particolare, il responsabile della gestione documentale, che coincide con il Responsabile del Servizio Segreteria Affari generali, oltre ad essere il responsabile del Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, è tenuto a:

- predisporre il manuale di gestione documentale, d'intesa con il responsabile della conservazione e il responsabile per la transizione digitale e acquisito il parere del responsabile della protezione dei dati personali;
- predisporre, in accordo con il responsabile della conservazione e acquisito il parere del Responsabile della protezione dei dati personali, il piano della sicurezza del sistema di gestione informatica dei documenti (che è allegato e parte integrante del presente manuale di gestione documentale);
- definire il piano di organizzazione delle aggregazioni documentali (fascicoli e serie);
- verificare periodicamente la rispondenza del piano di classificazione ai procedimenti amministrativi e agli affari in essere ed eventualmente procedere con il suo aggiornamento;
- verificare l'avvenuta eliminazione dei protocolli di settore, dei protocolli multipli e - più in generale - dei protocolli diversi dal protocollo informatico previsto dal Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- trasmettere al sistema di conservazione, almeno una volta l'anno, i fascicoli e le serie documentarie anche relative a procedimenti non conclusi;
- svolgere il ruolo di Produttore dei pacchetti di versamento¹ e assicurarne la trasmissione al sistema di conservazione secondo le modalità operative definite nel manuale di conservazione del conservatore Regione Emilia-Romagna, a cui l'Unione dei comuni di Terred'Acqua ha affidato il servizio di conservazione dei propri documenti informatici.

Nel caso dell'Unione, il Responsabile della gestione documentale ricopre anche il ruolo di Responsabile della conservazione.

3 Redazione e formazione dei documenti amministrativi

Il presente capitolo descrive le modalità di redazione, formazione ed acquisizione dei documenti amministrativi, ed in particolare dei documenti amministrativi informatici, che le Linee guida AgID definiscono come ogni rappresentazione grafica, foto cinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni o comunque, da queste ultime utilizzati ai fini dell'attività amministrativa. In particolare, le disposizioni di seguito riportate si riferiscono a:

- informazioni minime previste che devono essere contenute nel documento amministrativo;
- modalità di formazione e acquisizione dei documenti amministrativi informatici;
- formati dei documenti amministrativi informatici;
- firme e sigilli elettronici;
- validazione temporale elettronica;
- duplicati, copie ed estratti informatici;
- copie analogiche di documenti amministrativi informatici.

3.1 Informazioni minime previste

Sui documenti amministrativi formati l'Unione dei comuni di Terred'Acqua devono essere riportate le seguenti informazioni minime:

¹ Il pacchetto di versamento è il pacchetto informativo che può contenere uno o più oggetti di conservazione con i relativi metadati oppure anche i soli metadati riferiti agli oggetti di conservazione.

- denominazione e stemma dell'Amministrazione;
- indicazione dell'AOO e dell'Ufficio utente che ha prodotto il documento;
- indirizzo completo dell'Amministrazione con: numero di telefono, domicilio digitale e C.F.;
- data completa con luogo, giorno, mese, anno;
- nominativo del responsabile del procedimento, indirizzo di posta elettronica ordinaria, numero di telefono;
- numero di protocollo;
- eventuale numero del repertorio (numero di registrazione nel registro particolare);
- indice di classificazione: titolo/classe;
- numero e descrizione degli allegati;
- numero e data del documento cui si risponde;
- oggetto del documento che risponda a criteri di sinteticità e chiarezza;

Nelle lettere in partenza, infine, occorre specificare che chi risponde è tenuto a citare i riferimenti di protocollo della lettera cui fa riscontro.

3.2 Formazione dei documenti amministrativi informatici

L'Unione dei comuni di Terred'Acqua forma gli originali dei propri documenti, inclusi quelli inerenti ad albi, elenchi e pubblici registri, attraverso strumenti informatici oppure acquisendo le istanze, le dichiarazioni e le comunicazioni previste dalla normativa vigente.

In conformità con quanto previsto dalle Linee guida AgID, la formazione dei documenti amministrativi informatici dell'Unione dei comuni di Terred'Acqua può quindi avvenire con una delle seguenti modalità:

- a creazione tramite l'utilizzo di strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità di cui all'allegato 2 alle Linee guida AgID: ad esempio, un qualsiasi provvedimento redatto in formato Word 2007 e memorizzato in formato PDF/A prima che su di esso sia apposta la firma digitale del dirigente che lo adotta;
- b acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico: ad esempio, un'istanza trasmessa al domicilio digitale dell'Unione dei comuni di Terred'Acqua, sia che si tratti di un documento informatico nativo, sia che questa consista nella copia per immagine (scansione) di un documento analogico;
- c memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente: ad esempio, i dati inseriti dai cittadini che tramite il sito istituzionale dell'Unione dei comuni di Terred'Acqua accedono ai servizi online disponibili e compilano online la modulistica messa a loro disposizione;
- d generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica: ad esempio, il registro giornaliero di protocollo, costituito da registrazioni effettuate da operatori diversi che sono memorizzate in forma statica (documento in formato PDF/A).

Nel caso del documento amministrativo informatico creato con le modalità di cui alla lettera a), l'Unione dei comuni di Terred'Acqua ne garantisce l'immodificabilità e l'integrità attraverso lo svolgimento di una o più delle seguenti operazioni:

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza per contrastare i rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati;
- trasferimento a soggetti terzi attraverso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato valido ai fini delle comunicazioni elettroniche aventi valore legale;
- versamento ad un sistema di conservazione.

Nel caso del documento amministrativo informatico formato con le modalità di cui alla lettera b), l'Unione dei comuni di Terred'Acqua ne garantisce l'immodificabilità e l'integrità attraverso le stesse operazioni previste per i documenti creati con gli strumenti di cui alla lettera a) ad eccezione del trasferimento a soggetti terzi tramite PEC/altro servizio elettronico di recapito certificato qualificato.

Nel caso dei documenti amministrativi informatici formati con le modalità di cui alle lettere c) e d), infine, l'immodificabilità e l'integrità possono essere garantite da una o più delle seguenti operazioni:

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- registrazione nei log di sistema dell'esito dell'operazione di formazione del documento informatico, compresa l'applicazione di misure per la protezione dell'integrità della base di dati e per la produzione e conservazione dei log di sistema;
- produzione di una estrazione statica dei dati e trasferimento della stessa nel sistema di conservazione (come nel caso del registro giornaliero di protocollo).

In tutti i casi, come previsto dalle Linee guida AgID, il documento amministrativo informatico assume le caratteristiche di immodificabilità e di integrità anche con la sua registrazione nel registro di protocollo, negli ulteriori registri, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenute nel sistema di gestione informatica dei documenti.

3.2.1 Formati dei documenti amministrativi informatici

Il formato di un documento informatico è la modalità di rappresentazione della sequenza di bit che lo costituisce (solitamente è identificato con la sua estensione).

La scelta dei formati con cui l'Unione dei comuni di Terred'Acqua crea i propri documenti amministrativi informatici avviene tra quelli previsti dalle Linee guida AgID, privilegiando in particolare formati aperti, non proprietari, standard *de iure*, estendibili, parlanti, completamente robusti e indipendenti dal dispositivo.

In particolari contesti applicativi è possibile l'utilizzo di formati diversi da quelli previsti dalle predette Linee guida, individuati dall'Unione dei comuni di Terred'Acqua tenendo conto della valutazione periodica di interoperabilità effettuata dal conservatore ParER, cui l'Unione ha affidato il servizio di conservazione dei propri documenti informatici, che prevede anche le necessarie

procedure di riversamento per garantire la conservazione nel tempo e l'accesso ai documenti informatici attraverso la produzione di copie informatiche per la conservazione.

Il riversamento, infatti, è la procedura tramite cui uno o più documenti informatici sono convertiti da un formato di file ad un altro, lasciando invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato dei file e delle codifiche di destinazione.

Con riferimento ai formati dei documenti amministrativi informatici ricevuti, l'Unione dei comuni di Terred'Acqua garantisce sempre la gestione dei formati classificati come «generici» nell'allegato 2 alle Linee guida AgID, definiti come quei formati che tutte le pubbliche amministrazioni sul territorio nazionale devono essere in grado di leggere. Esempi di formati generici tra i più diffusi sono: PDF (.pdf); Word 2007 (.docx, .dotx); ODT (.odt); RichText (.rtf), XML (.xml), HTML (.html, .htm), EML (.eml), Excel 2007 (.xlsx, .xltx), Power Point 2007 (.pptx, .ppsx, .potx), ODS (.ods), ODP (.odp), PNG (.png), JPEG (.jpg, .jpeg), TIFF (.tiff, .tif), GIF (.gif), ODG (.odg), WAF (.waf, .bwf, .rf64), MP3 (.mp3), MP4 (.mp4, .m4a, m4v), ZIP (.zip, .zipx), 7-Zip (.7z), RAR (.rar, .r).

Nel caso in cui un formato sia indicato nelle Linee guida AgID come generico, ma una sua particolare applicazione in un determinato settore specialistico fornisca anche un formato di file specifico, la specializzazione del formato prevale su quella generale. È il caso del documento informatico contenente informazioni fiscali relative ad una prestazione, cessazione di beni o servizi, che le organizzazioni devono produrre e trasmettere alle pubbliche amministrazioni non in qualsiasi file nel formato generico XML ma sotto forma di fattura elettronica nello specifico formato FatturaPA individuato dal legislatore come il dialetto XML per quell'utilizzo specifico.

3.2.2 Firme e sigilli elettronici

La firma elettronica, secondo quanto previsto dal Regolamento UE n. 910/2014 - eIDAS (d'ora in avanti Regolamento eIDAS), consiste nell'insieme dei dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare.

Il D.Lgs. 82/2005 (Codice dell'amministrazione digitale, d'ora in avanti CAD), in particolare, stabilisce che il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'art. 2702 del Codice civile quando vi è apposta una firma digitale, un altro tipo di firma elettronica qualificata o una firma elettronica avanzata oppure è formato - previa identificazione informatica del suo autore attraverso un processo avente i requisiti fissati da AgID nel Codice dell'amministrazione digitale (CAD) - con modalità tali da garantire la sicurezza, l'integrità e l'immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore.

L'Unione dei comuni di Terred'Acqua prevede la formazione di documenti e atti amministrativi informatici sottoscritti con firma elettronica digitale da parte del Presidente dell'Unione, dei componenti della Giunta dell'Unione, dei responsabili dei Servizi in cui l'Unione è articolata e - in generale - di coloro cui è stato riconosciuto formalmente il potere di firma in rappresentanza dell'Amministrazione.

Inoltre, come meglio precisato qui di seguito, l'apposizione della firma digitale è necessaria per procedere con l'attestazione di conformità delle copie generate all'interno del Sistema di gestione informatica dei documenti.

La firma digitale consiste in un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo - tramite la chiave pubblica - di rendere manifesta e verificare la provenienza e l'integrità di un documento informatico.

L'Unione dei comuni di Terred'Acqua, inoltre, può altresì garantire l'origine e l'integrità dei documenti amministrativi informatici prodotti attraverso l'apposizione del sigillo elettronico, che al pari della firma elettronica consiste in dati in forma elettronica acclusi oppure connessi tramite associazione logica ad altri dati elettronici, ma che a differenza della firma elettronica si riferisce ad una persona giuridica e non ad una persona fisica; in particolare, l'Unione dei comuni di Terred'Acqua, appone sempre il proprio sigillo elettronico qualificato² sul file Segnatura di protocollo, in conformità con quanto previsto dalle Linee guida AgID.

Nel caso di documenti amministrativi informatici formati dall'Unione dei comuni di Terred'Acqua, l'apposizione della firma elettronica digitale o del sigillo elettronico qualificato conclude la fase di formazione dei documenti e deve quindi necessariamente precedere l'operazione di registrazione informatica del documento nel registro di protocollo/nei registri particolari previsti.

3.2.3 Validazione temporale elettronica

Il Regolamento eIDAS definisce la validazione temporale come i dati in forma elettronica che collegano altri dati in forma elettronica a una determinata ora e data così da provare che questi ultimi esistevano in quel momento.

La normativa italiana vigente in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, in particolare, definisce quali riferimenti temporali possano essere considerati opponibili a terzi e costituire validazione temporale.

Nel caso dei documenti prodotti e acquisiti dall'Unione dei comuni di Terred'Acqua costituiscono validazione temporale:

- il riferimento temporale contenuto nella segnatura di protocollo;
- il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti informatici prevista dalle Linee guida AgID;
- il riferimento temporale ottenuto attraverso l'utilizzo di posta elettronica certificata.

3.3 Duplicati informatici

Un duplicato informatico è il documento informatico ottenuto mediante la memorizzazione – sullo stesso dispositivo o su dispositivi diversi – della medesima sequenza di valori binari del documento originario; ha il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui è tratto se prodotto in conformità con quanto previsto dalle Linee guida AgID.

Esempi di duplicati informatici sono i documenti amministrativi trasmessi dall'Unione dei comuni di Terred'Acqua a coloro che hanno presentato istanza di accesso agli atti (ovviamente nell'eventualità in cui la richiesta di accesso riguardi documenti amministrativi informatici nativi). In questo caso, infatti, il sistema di gestione informatica dei documenti e il soggetto che ha trasmesso la richiesta di accesso agli atti conserveranno file identici costituiti dalla medesima sequenza di bit e con lo stesso valore probatorio.

² Il regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, all'art. 3, definisce un sigillo elettronico qualificato come un sigillo elettronico avanzato creato da un dispositivo per la creazione di un sigillo elettronico qualificato e basato su un certificato qualificato per sigilli elettronici. Un sigillo elettronico avanzato è connesso univocamente al creatore del sigillo, è idoneo a identificare il creatore del sigillo, è creato mediante dati per la creazione di un sigillo elettronico che il creatore del sigillo elettronico può, con un elevato livello di sicurezza, usare sotto il proprio controllo per creare sigilli elettronici ed è collegato ai dati cui si riferisce così da consentire l'identificazione di ogni successiva modifica dei dati.

3.4 Copie ed estratti informatici

L'Unione dei comuni di Terred'Acqua, durante lo svolgimento dell'attività amministrativa, può procedere con la generazione di copie informatiche di documenti analogici o informatici ed estratti informatici di documenti informatici in conformità con quanto previsto dal CAD e dalle Linee guida AgID.

Nel caso delle copie informatiche di documenti analogici, queste possono consistere in:

- documenti informatici il cui contenuto è identico a quello dei documenti analogici da cui le copie sono tratte;
- copie per immagini su supporto informatico di documenti analogici (scansioni), ovvero documenti informatici con contenuto e forma identici a quelli dei documenti analogici da cui le copie sono tratte.

Nel caso di copie ed estratti informatici (anche per riassunto) di documenti informatici, questi consistono, rispettivamente:

- in documenti informatici con contenuto identico a quello dei documenti da cui sono tratti ma con diversa sequenza di bit, che richiedono quindi, per la loro generazione, lo svolgimento di un'attività di riversamento (per la sua definizione si rimanda al punto 3.2.1);
- in documenti informatici che consistono in una parte del documento tratto dal documento originale (estratti informatici) ovvero documenti in cui si attestano in maniera sintetica fatti, stati o qualità desunti da documenti informatici (estratti per riassunto di documenti informatici).

Tali documenti, se formati nel rispetto delle Linee guida AgID, hanno lo stesso valore probatorio dell'originale da cui sono tratti:

- se la stessa conformità non viene espressamente disconosciuta;
- nel caso in cui un pubblico ufficiale/un notaio attesti la conformità delle copie e degli estratti agli originali da cui sono tratti.

L'attestazione di conformità è prodotta dal pubblico ufficiale che ha verificato la corrispondenza del contenuto (e, nel caso delle copie per immagine, anche della forma) delle copie e degli estratti con quello dei documenti originali da cui sono tratti attraverso uno dei seguenti metodi:

- raffronto dei documenti;
- certificazione di processo in conformità con quanto previsto dall'allegato 3 alle Linee guida AgID (introdotta dal legislatore con la finalità di favorire la dematerializzazione di grosse quantità di documenti analogici nei casi in cui lo strumento del raffronto dei documenti sia impraticabile).

L'attestazione di conformità:

- può essere inserita nel documento informatico che contiene la copia o l'estratto; il documento che contiene l'attestazione deve essere sottoscritto con firma digitale/firma elettronica avanzata del pubblico ufficiale a ciò autorizzato;
- nel caso di più copie ed estratti l'attestazione può essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia o estratto informatico, che anche in questo caso deve essere sottoscritto con firma digitale/firma elettronica avanzata del pubblico ufficiale a ciò autorizzato.

Le copie informatiche conformi di documenti analogici sono idonee ad assolvere gli obblighi di conservazione previsti dalla legge, mentre permane l'obbligo della conservazione dell'originale analogico per le tipologie di documenti analogici originali unici individuate dal DPCM 21 marzo

2013 in relazione alla documentazione statale, come ad esempio atti giudiziari, processuali e di polizia giudiziaria (per i venti anni successivi), documenti di valore storico-artistico e atti notarili.

In generale, la distruzione della documentazione analogica deve essere sempre autorizzata dalla Soprintendenza archivistica che, ai sensi di quanto previsto dalla Circolare della Direzione Generale Archivi (DGA) n. 41 del 14 dicembre 2015, prima di procedere con l'autorizzazione, dovrà valutare con particolare attenzione tutte le tipologie documentali grazie alle quali possano essere riconosciuti diritti, doveri e legittime aspettative di terzi (la predetta Circolare fornisce anche esempi di tipologie di documenti che, per analogia con quanto previsto dal DPCM 21 marzo 2013, devono essere conservati in formato analogico: tutta la documentazione conservata negli archivi storici, statuti, vincoli paesaggistici, mappe catastali).

3.5 Copie analogiche di documenti amministrativi informatici

Nel caso di generazione di copie analogiche di documenti amministrativi informatici, anche sottoscritti con firma elettronica digitale, qualificata o avanzata, queste hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale in tutte le sue componenti è attestata da un pubblico ufficiale a ciò autorizzato ovvero se la loro conformità non è espressamente disconosciuta.

L'Unione dei comuni di Terred'Acqua, ad esempio nel caso in cui deve trasmettere un documento ad un soggetto privo di domicilio digitale, ovvero nei casi di domicili non attivi/non funzionanti/non raggiungibili, può quindi procedere:

- con la formazione del documento amministrativo informatico sottoscritto con firma digitale o altra firma elettronica qualificata (che sarà conservato in conformità con quanto previsto dalle Linee guida AgID);
- con l'invio, tramite raccomandata con avviso di ricevimento o posta ordinaria, della copia analogica del predetto documento amministrativo informatico recante una dicitura che specifichi che il documento informatico, da cui la copia è tratta, è stato predisposto come documento informatico nativo digitale ed è disponibile presso l'Amministrazione.

4 Gestione documentale

Il presente capitolo, dopo aver illustrato le diverse fasi di vita dell'archivio (archivio corrente, archivio di deposito e archivio storico), descrive le seguenti operazioni effettuate dall'Unione dei comuni di Terred'acqua durante la gestione dei documenti amministrativi formati e acquisiti, fino al loro trasferimento al Sistema di conservazione (nel caso dei documenti amministrativi informatici) o all'Archivio storico (nel caso di documenti analogici):

- modalità di ricezione e trasmissione dei documenti;
- generazione delle copie per immagine dei documenti ricevuti su supporto cartaceo;
- registrazione informatica dei documenti (registrazione di protocollo e registrazione particolare);
- generazione del file Segnatura informatica;
- classificazione;
- assegnazione;
- formazione delle aggregazioni documentali informatiche: serie e fascicoli;
- metadattazione;
- flusso di lavorazione dei documenti amministrativi in entrata, in uscita e interni.

Infine, il capitolo contiene le disposizioni dedicate alle modalità con cui avviene la gestione della documentazione soggetta per legge a obblighi di pubblicazione nell'Albo pretorio online.

4.1 Le fasi di vita dell'archivio: archivio corrente, archivio di deposito e archivio storico

La disciplina archivistica, tradizionalmente, articola la vita di un archivio nelle seguenti tre fasi sulla base delle finalità per cui la documentazione che lo costituisce è conservata:

- archivio corrente: comprende documentazione necessaria allo svolgimento degli affari in corso;
- archivio di deposito: comprende documentazione ancora utile per finalità amministrative/giuridiche ma non più necessaria per la trattazione delle attività correnti;
- archivio storico: comprende documentazione relativa ad affari esauriti, selezionata per la conservazione permanente per il suo valore storico e culturale.

Mentre si rimanda al capitolo dedicato alla conservazione per ciò che riguarda l'archivio storico, si specificano qui di seguito le modalità di gestione dell'archivio corrente e di quello di deposito, che variano sulla base del supporto (analogico/informatico) della documentazione.

4.1.1 Archivio corrente

I fascicoli analogici che costituiscono l'archivio corrente sono formati e conservati, fino al versamento nell'archivio di deposito, presso gli uffici a cui sono state assegnate le pratiche.

Nel caso di fascicoli informatici, questi sono aperti e chiusi nel Sistema di gestione informatica dei documenti tramite la componente Sistema di protocollo informatico. Come già ricordato, il Responsabile della gestione documentale deve trasferire al Sistema di conservazione, almeno una volta l'anno, i fascicoli aperti contestualmente all'avvio dei procedimenti amministrativi, anche se questi ultimi non sono conclusi. Quindi, mentre nel caso dei fascicoli analogici il trasferimento all'archivio di deposito dall'archivio corrente (ovvero dai diversi uffici dove i fascicoli sono stati aperti e gestiti durante lo svolgimento delle pratiche) avviene solamente una volta terminato il procedimento/l'attività/l'affare cui i fascicoli si riferiscono, nel caso dei fascicoli informatici, il loro versamento al sistema di conservazione deve avvenire almeno una volta l'anno (indipendentemente dal fatto che i fascicoli si riferiscano a procedimenti, attività o affari conclusi).

4.1.2 Archivio di deposito

Periodicamente, gli uffici individuano i fascicoli analogici relativi ad affari o procedimenti conclusi o comunque non più necessari allo svolgimento delle attività correnti. I servizi provvedono allo sfoltimento del fascicolo eliminando le bozze, fotocopie e altro materiale che non deve essere conservato.

I fascicoli sono quindi sottoposti a verifica del responsabile dei servizi in cui l'unità archivistica si è formata in merito alla completezza del loro contenuto e trasferiti all'archivio di deposito con un'apposita funzione del sistema di protocollo informatico, curando anche il trasferimento fisico degli eventuali carteggi.

Il trasferimento deve essere effettuato rispettando l'organizzazione che i fascicoli e le serie avevano nell'archivio corrente.

Contestualmente ai fascicoli, i predetti responsabili consegnano al Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi l'elenco dei fascicoli consegnati, con sottoscrizione che ne attesta la completezza.

Il responsabile della gestione documentale cura quindi la formazione e la conservazione di un elenco dei fascicoli e delle serie trasferite nell'archivio di deposito.

Gli uffici utente possono richiedere in ogni momento al Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, per motivi di consultazione, fascicoli già versati.

Dei fascicoli prelevati dagli archivi deve essere tenuta traccia del movimento effettuato e della richiesta di prelevamento.

Prima di trasferire i fascicoli all'archivio storico, l'Unione dei comuni di Terred'acqua procede con le necessarie operazioni di selezione e scarto sulla base di quanto previsto dal Piano di conservazione (allegato 4).

Nel caso dei fascicoli informatici, questi possono essere conservati nel sistema di gestione informatica dei documenti/nel sistema di conservazione (o in entrambi): infatti, a differenza di quanto previsto per la documentazione analogica, per i documenti e le aggregazioni documentali informatiche non esiste un sistema intermedio tra il sistema di gestione documentale (dove il fascicolo è aperto, alimentato, consultato e infine chiuso) e il sistema di conservazione (dove il fascicolo può essere consultato ed eventualmente scartato sulla base di quanto previsto dal piano di conservazione).

4.2 Ricezione e trasmissione dei documenti

4.2.1 Modalità di ricezione e trasmissione dei documenti analogici

I documenti su supporto cartaceo possono essere ricevuti tramite servizio postale tradizionale, corrieri autorizzati e apparecchi fax: sono consegnati al Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi che, dopo aver registrato e classificato la documentazione, procede con l'inoltro agli uffici competenti.

Nel caso di trasmissione di documenti su supporto cartaceo, questa avviene tramite servizio postale tradizionale; i documenti da spedire su supporto cartaceo sono trasmessi all'ufficio abilitato alla spedizione dopo che, l'ufficio che ha prodotto il documento, ha eseguito le operazioni di registrazione, classificazione e fascicolazione.

4.2.2 Modalità di ricezione e trasmissione dei documenti informatici

Per la ricezione e la trasmissione di comunicazioni, istanze, dichiarazioni e notifiche in formato digitale che formano oggetto di registrazione di protocollo, l'Unione dei comuni di Terred'acqua utilizza il proprio domicilio digitale dichiarato in IPA.

Nel caso di scambio di documenti amministrativi informatici protocollati con un'altra pubblica amministrazione, un messaggio di protocollo trasmesso o ricevuto è costituito sempre da una struttura logica che:

- deve contenere il documento amministrativo informatico principale;
- può contenere un numero qualsiasi di documenti amministrativi informatici allegati;
- deve contenere la segnatura di protocollo del messaggio protocollato.

I documenti amministrativi informatici possono essere ricevuti anche:

- nell'ambito dei servizi online predisposti dall'Unione dei comuni di Terred'Acqua, accessibili dal sito istituzionale previa autenticazione tramite identità digitale SPID/Carta di identità elettronica (CIE)/Carta nazionale dei servizi (CNS); tramite i predetti servizi i soggetti che si autenticano (cittadini, professionisti, enti pubblici e privati) possono anche

accedere a documenti amministrativi informatici formati dall'Unione dei comuni di Terred'Acqua nell'ambito dei procedimenti e delle attività cui i servizi si riferiscono;

- dai diversi uffici/servizi (agli indirizzi di posta elettronica ordinaria da loro gestiti);
- dal personale (agli indirizzi di posta elettronica ordinaria loro assegnati);

4.3 Registrazione informatica dei documenti

La registrazione informatica dei documenti consiste nell'insieme di dati in forma elettronica allegati o connessi al documento amministrativo informatico per l'identificazione univoca di tutti i documenti prodotti o acquisiti dall'Unione dei comuni di Terred'acqua.

In conformità con quanto previsto dalla normativa vigente (DPR 445/2000, art. 53, comma 5), l'Unione registra nel registro di protocollo tutti i documenti inviati e ricevuti e tutti i documenti informatici, esclusi quelli soggetti a registrazione particolare nonché le seguenti tipologie che per la predetta normativa sono esclusi dalla registrazione di protocollo: le gazzette ufficiali, i bollettini ufficiali e notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, atti e documenti interni di preminente carattere informativo che non costituiscono fasi obbligatorie e imprescindibili dei procedimenti amministrativi, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni.

Inoltre, non sono oggetto di registrazione nel registro di protocollo le seguenti tipologie di documenti interni:

- convocazioni ad incontri o riunioni;
- memorie informali;
- appunti;
- richieste di servizi di pulizia;
- richieste di forniture di cancelleria;
- dismissioni di beni e attrezzature;
- trasmissione di documenti e atti già protocollati o repertoriati;
- semplici avvertenze di arrivi/scadenze offerte;
- comunicazioni relative a corsi di formazione interni;
- lettere di trasmissione di copie di leggi e decreti.

4.3.1 Registrazione e segnatura di protocollo

La registrazione di protocollo è l'insieme dei metadati che il registro di protocollo deve memorizzare, per tutti i documenti amministrativi registrati, ai sensi di quanto previsto dall'art. 53, comma 1 e dalle Linee guida AgID.

I documenti in arrivo sono registrati (classificati e assegnati) dal Servizio Segreteria Affari generali nell'ambito del Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi; la registrazione (così come la classificazione e la fascicolazione) sono invece prerogativa dei servizi competenti allo svolgimento dei procedimenti amministrativi, degli affari e delle attività.

La registrazione di protocollo dei documenti informatici è effettuata in modo da far corrispondere ad ogni messaggio una registrazione, nell'ambito della quale devono essere identificati il documento principale (che si può riferire sia al corpo del messaggio, sia ad uno o più file ad esso allegati) e gli eventuali relativi allegati.

I metadati previsti obbligatoriamente dalla normativa e memorizzati nel registro di protocollo del dall'Unione dei comuni di Terred'acqua sono i seguenti (in corsivo le informazioni generate automaticamente dalla componente sistema di protocollo):

- a *numero di protocollo* (la numerazione si rinnova ad ogni anno solare, inizia quindi il 1° gennaio e termina il 31 dicembre);
- b *data di registrazione di protocollo* (nel formato gg/mm/aaaahh:mm:ss);
- c mittente per i documenti ricevuti oppure destinatario/destinatari per i documenti spediti;
- d oggetto;
- e *data e protocollo del documento ricevuto*, se disponibili;
- f *impronta* (del documento principale, degli eventuali documenti allegati e del file Segnatura di protocollo);
- g assegnazione (soggetto a cui è destinato il documento, area/ufficio di appartenenza, data di assegnazione del documento e stato dell'assegnazione);
- h indice di classificazione;

Inoltre, l'Unione può memorizzare nel registro di protocollo anche i seguenti metadati non previsti dalla normativa:

- i *anno del registro di protocollo*;
- j documento in partenza/in arrivo/interno
- k data del documento;
- l tipo documento (ad es.: 'lettera', 'preventivo');
- m numero allegati;
- n fascicolo ed eventuale sottofascicolo;
- o indirizzo mittente/destinatario;
- p descrizione documento;
- q note
- r documento antecedente/sussequente;
- s *utente responsabile della registrazione di protocollo*.

Contemporaneamente all'operazione di registrazione di protocollo, il sistema di protocollo procede con la segnatura di protocollo, ovvero con l'associazione ai documenti amministrativi informatici protocollati, in forma permanente e non modificabile di informazioni riguardanti i documenti stessi, utili alla loro identificazione certa.

Le predette informazioni sono memorizzate dal sistema di protocollo nel file Segnatura, in formato XML, la cui struttura è definita nell'allegato 6 alle Linee guida AgID.

In particolare, il file Segnatura, su cui è apposto il sigillo qualificato dell'Unione dei comuni di Terred'acqua, è articolato nelle seguenti sezioni:

- Intestazione: contiene i dati identificativi e le informazioni fondamentali del messaggio (amministrazione e AOO mittente, registro in cui è avvenuta la registrazione, numero progressivo di protocollo, data di registrazione, oggetto del messaggio di protocollo, classificazione e fascicolo del messaggio di protocollo); con riferimento ai dati relativi ad amministrazione e AOO mittente, questi devono essere valorizzati con i relativi codici identificativi dell'amministrazione e dell'AOO del Comune di Crevalcore pubblicati sull'IPA.
- Riferimento: può contenere i dati per permettere al mittente di indicare il messaggio di protocollo ricevuto che ha determinato la segnatura.

- Descrizione: deve contenere le informazioni che descrivono i corrispondenti (mittente e destinatario) interessati nello scambio e i riferimenti al documento principale e agli eventuali allegati del messaggio di protocollo (in particolare, contiene l'impronta informatica del documento principale e degli eventuali allegati necessari per associarli in forma permanente alla segnatura di protocollo)
- Signature: deve contenere le informazioni per assicurare l'apposizione del sigillo elettronico qualificato sulla segnatura di protocollo da parte della AOO mittente al fine di garantire la sua autenticità e integrità.

Nel caso di scambio di documenti amministrativi informatici ad un'altra pubblica amministrazione un messaggio di protocollo trasmesso è costituito sempre da una struttura logica che:

- deve contenere il documento amministrativo informatico principale;
- può contenere un numero qualsiasi di documenti amministrativi informatici allegati;
- deve contenere la segnatura di protocollo del messaggio protocollato.

4.3.2 Il Registro giornaliero di protocollo

Il registro giornaliero di protocollo è formato automaticamente dal software di gestione documentale entro il giorno lavorativo seguente, mediante la generazione o il raggruppamento delle informazioni registrate secondo una struttura logica predeterminata e memorizzato in forma statica, imm modificabile e integra.

Il registro giornaliero è trasmesso al Sistema di conservazione entro la giornata lavorativa successiva alla sua produzione.

4.3.3 Annullamento e modifica delle informazioni registrate nel registro di protocollo

Le seguenti informazioni memorizzate nel registro di protocollo non possono essere modificate ma solo annullate con la procedura prevista dall'art. 54 del DPR 445/2000:

- a numero di protocollo;
- b data di registrazione di protocollo;
- c mittente per i documenti ricevuti oppure destinatario/destinatari per i documenti spediti;
- d oggetto;
- e data e protocollo del documento ricevuto, se disponibili;
- f impronta.

Tra le informazioni che devono essere memorizzate nel registro di protocollo, infatti, le Linee guida AgID prevedono esplicitamente che le uniche che possono essere modificate senza procedere con l'annullamento sono l'assegnazione e la classificazione.

La procedura di annullamento prevede l'emanazione, a fronte della richiesta trasmessa al Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, di un apposito provvedimento di autorizzazione.

Sia nel caso di annullamento che di modifica delle informazioni registrate nel registro di protocollo, il sistema di protocollo storicizza tutte le informazioni annullate o modificate rendendole entrambe visibili e comparabili in conformità con quanto previsto dal DPR 445/2000.

4.3.4 Registro di protocollo di emergenza

Il Responsabile della gestione documentale autorizza con apposito provvedimento lo svolgimento, anche manuale, delle operazioni di registrazione di protocollo su registri di emergenza ogni qualvolta, per cause tecniche, non sia possibile utilizzare il sistema di protocollo informatico. Il

registro di emergenza è unico ed è tenuto presso l'Ufficio protocollo e archivio e viene utilizzato con le seguenti modalità:

- sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema di protocollo;
- qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro (24) ore, per cause di eccezionale gravità, il Responsabile della gestione documentale può autorizzare l'uso del registro di emergenza per periodi successivi di non più di una settimana. Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione;
- per ogni giornata di registrazione di emergenza è riportato sul registro di emergenza il numero totale di operazioni registrate;
- la sequenza numerica utilizzata sul registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'AOO;
- le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando un'apposita procedura di recupero dei dati, senza ritardo al ripristino delle funzionalità del sistema. Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza.

4.3.5 Registrazione di protocollo: casistiche e comportamenti

4.3.5.1 Termini di registrazione

Le registrazioni di protocollo dei documenti pervenuti presso l'Amministrazione sono effettuate nella giornata di arrivo e comunque non oltre le 48 ore dal loro ricevimento.

Qualora non possa essere effettuata la registrazione di protocollo nei tempi sopra indicati si provvede a protocollare, in via prioritaria, i documenti che rivestono una particolare importanza, previo motivato provvedimento del Responsabile della gestione documentale, che autorizza l'addetto al protocollo a differire le operazioni relative agli altri documenti.

4.3.5.2 Registrazione di protocollo dei documenti amministrativi informatici trasmessi e ricevuti attraverso il domicilio digitale

La registrazione di protocollo dei documenti informatici è effettuata in modo da far corrispondere ad ogni messaggio una registrazione, nell'ambito della quale devono essere identificati il documento principale (che si può riferire sia al corpo del messaggio di posta elettronica inviato/ricevuto, sia ad uno o più file ad esso allegati) e gli eventuali relativi allegati.

4.3.5.3 Protocollazione multipla

Le comunicazioni che abbiano più destinatari, i cui nominativi non sono elencati nel medesimo documento, si registrano con tanti numeri di protocollo quanti sono i destinatari, utilizzando la modalità "Protocollazione multipla".

4.3.5.4 Registrazione informatica dei documenti amministrativi informatici ricevuti tramite i servizi online accessibili dal sito istituzionale

I diversi servizi online messi a disposizione dall'Unione dei comuni di Terred'Acqua sono integrati con il Sistema di protocollo informatico: i documenti amministrativi informatici formati ed acquisiti nell'ambito dello svolgimento di procedimenti ed attività diversi sono quindi registrati e classificati automaticamente.

4.3.5.5 Rilascio di ricevute attestanti la ricezione dei documenti

Nel caso di consegna diretta di un documento cartaceo, da parte dell'utenza, l'ufficio che riceve il documento - su richiesta - consegna al mittente la stampa dell'operazione di registrazione o appone il numero di protocollo sulla copia del documento che si consegna per la protocollazione, oppure rilascia la ricevuta prodotta dal sistema di protocollo informatico con gli estremi della segnatura.

Nel caso di ricezione dei documenti informatici, la notifica al mittente dell'avvenuta ricezione è assicurata dal sistema di posta elettronica certificata utilizzato dall'Amministrazione.

4.3.5.6 Registrazione di protocollo dei documenti amministrativi interni

Per ogni documento prodotto dagli uffici (richiesto nell'ambito di uno specifico procedimento amministrativo), non spedito a soggetti esterni all'Amministrazione e non rientrante nelle categorie di documenti esclusi dalla registrazione, indipendentemente dal supporto sul quale è formato, è effettuata una registrazione di protocollo.

Per i protocolli interni il destinatario è il servizio a cui si scrive e, durante l'operazione di assegnazione, il campo Consegnatario va valorizzato come segue:

- con il codice "E" il responsabile che sta scrivendo;
- con il codice "T" il destinatario;
- con il codice "I" gli eventuali incaricati di accettazione del destinatario;
- con il codice "C" altri servizi che devono essere messi a conoscenza dell'atto.

4.3.5.7 Documenti indirizzati nominativamente al personale dell'A00

La posta cartacea indirizzata nominativamente al personale dell'Amministrazione viene regolarmente aperta e registrata al protocollo a meno che non rechi la dicitura "riservata" o "personale", caso in cui è recapitata al destinatario che, dopo averla aperta e preso visione del contenuto, valuta se il documento ricevuto è di natura personale o se riguarda procedimenti, affari e attività dell'Amministrazione. In questa seconda eventualità, procede con la tempestiva consegna al Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi dell'Unione dei comuni di Terred'Acqua. La stessa valutazione è effettuata dai dipendenti nel caso di ricezione di messaggi di posta elettronica ordinaria ai propri indirizzi personali: se la documentazione è riconducibile allo svolgimento dell'attività amministrativa del Unione dei comuni di Terred'Acqua questi procedono con l'inoltro immediato al domicilio digitale dell'Amministrazione.

4.3.5.8 Lettere anonime e documenti non firmati

Le lettere anonime non vengono registrate al protocollo né inoltrate alle diverse aree.

I documenti ricevuti non firmati, per i quali è invece prescritta la sottoscrizione, sono comunque registrati nel registro di protocollo ed inoltrati all'area di competenza per la valutazione della loro ammissibilità.

4.3.5.9 Documenti ricevuti prima via fax e successivamente su supporto cartaceo

I documenti ricevuti via fax sono registrati al protocollo e gestiti con le seguenti modalità:

- qualora pervengano successivamente gli originali per posta tradizionale, verranno attribuiti a questi lo stesso numero e la stessa data di protocollo assegnati ai relativi fax;
- qualora si rilevi che l'originale è stato registrato con un numero diverso la registrazione relativa all'originale deve essere annullata;
- qualora il documento inviato per posta risultasse difforme da quello inviato via fax lo si sottopone ad una nuova registrazione di protocollo.

4.3.5.10 Documenti di competenza di altre amministrazioni o di altri soggetti

Qualora pervenga all'Amministrazione un documento cartaceo di competenza di un altro ente o altra persona fisica o giuridica, lo stesso deve essere riconsegnato in busta chiusa all'Ufficio postale per il corretto inoltro a chi di competenza. Nel caso di erronea apertura della busta, il Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi provvede direttamente a predisporre una nuova busta indirizzandola direttamente al destinatario di competenza, ed inserendo nella stessa sia il documento che la busta originariamente pervenuta, allegando una breve nota informale recante la dicitura "pervenuta ed aperta erroneamente".

Nel caso in cui un documento della fattispecie sopra indicata sia stato erroneamente registrato al protocollo, sarà spedito a chi di competenza, oppure restituito al mittente, con lettera accompagnatoria protocollata, conservando una copia nel fascicolo di riferimento e provvedendo ad inserire nel sistema di protocollo, nel campo "note", la dicitura "pervenuto erroneamente".

Nel caso di documenti informatici, il sistema di protocollo consente di utilizzare la funzione 'Respingi al mittente': il documento non è protocollato ma resta conservato nel sistema insieme ai messaggi respinti unitamente alla motivazione del respingimento (ad es. "pervenuto per errore").

4.3.6 Registrazione particolare

L'Unione dei comuni di Terred'Acqua applica ove possibile i requisiti fissati per la registrazione di protocollo anche all'operazione di registrazione dei documenti soggetti a registrazione particolare, che sono elencati nell'allegato 2.

4.4 Scansione dei documenti pervenuti su supporto analogico

I documenti pervenuti su supporto cartaceo, di formato inferiore o uguale all'A4, dopo le operazioni di registrazione e segnatura di protocollo, vengono acquisiti in formato immagine con l'ausilio di scanner da parte del Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

I documenti di formato superiore all'A4 sono acquisiti in formato immagine solo se esplicitamente richiesto dagli uffici di competenza, avvalendosi eventualmente, in caso di assenza di strumentazione interna adeguata, dei servizi di una società specializzata.

Il processo di scansione dei documenti pervenuti si articola nelle seguenti fasi:

- acquisizione delle immagini in modo tale che ad ogni documento, anche composto da più pagine, corrisponda un unico file;
- verifica della leggibilità delle immagini acquisite e della loro esatta corrispondenza con gli originali cartacei;

- collegamento delle immagini alle rispettive registrazioni di protocollo, in modo non modificabile;
- memorizzazione delle immagini nel Sistema di protocollo informatico.

Le immagini dei documenti cartacei acquisite con lo scanner sono rese disponibili agli uffici, attraverso il Sistema di protocollo informatico, immediatamente dopo le operazioni di scansione, classificazione e assegnazione.

4.5 Classificazione dei documenti

L'operazione di classificazione è finalizzata ad organizzare logicamente tutti i documenti amministrativi informatici prodotti o acquisiti dell'Unione dei comuni di Terred'Acqua indipendentemente dal fatto che siano registrati nel registro di protocollo.

Consiste nell'attività di assegnazione, ai documenti e ai fascicoli in cui sono aggregati, dell'indice di classificazione desunto dal titolario (o piano di classificazione), la struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'Unione.

Il titolario dell'Unione dei comuni di Terred'Acqua (allegato 3), è articolato su due livelli (Titolo e Classe).

Nel caso ad esempio di un documento amministrativo informatico ricondotto al Titolo IV (Risorse finanziarie e patrimonio), Classe 5 (Partecipazioni finanziarie), l'indice di classificazione è IV.5.

4.6 Assegnazione dei documenti

L'assegnazione dei documenti ai diversi uffici ed utenti (per competenza ed eventualmente anche per conoscenza) è effettuata dal Responsabile della gestione documentale e dagli utenti abilitati nell'ambito del Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi. Il processo di assegnazione dei documenti può coinvolgere più utenti ed uffici, fino ad arrivare all'ufficio incaricato dello svolgimento del procedimento amministrativo, dell'affare o dell'attività.

Il sistema di protocollo informatico tiene traccia delle assegnazioni memorizzando per ciascuna di esse l'identificativo dell'operatore che effettua la modifica con la data e l'ora di esecuzione.

Nel caso di assegnazione errata, l'ufficio che riceve il documento è tenuto, esclusivamente tramite la funzione del sistema di gestione documentale "respingi non di competenza", a restituirlo, con la massima tempestività, indicando obbligatoriamente la motivazione della non accettazione dello stesso, al Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi che provvederà all'assegnazione corretta.

I documenti ricevuti dall'Amministrazione su supporto cartaceo, anche se acquisiti in formato immagine con l'ausilio di scanner, al termine delle operazioni di registrazione, segnatura di protocollo e assegnazione, sono consegnati materialmente in originale agli uffici di competenza.

4.7 Formazione delle aggregazioni documentali informatiche

Le Linee guida AgID definiscono le aggregazioni documentali informatiche come l'insieme di documenti informatici o di fascicoli informatici riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente. Le possibili tipologie di aggregazioni documentali informatiche che possono essere formate sono le seguenti:

- Fascicoli

- Serie documentarie
- Serie di fascicoli informatici

4.7.1 I fascicoli

Nell'ambito dell'AOO istituita presso l'Unione dei comuni di Terred'Acqua i flussi documentali sono gestiti mediante fascicoli informatici che di norma sono aperti al livello più basso del titolario in uso (Classe) e conservano documenti recanti il medesimo indice di classificazione. È comunque possibile che, durante lo svolgimento di un procedimento/di un'attività, in un fascicolo informatico siano archiviati documenti con indici di classificazione diversi rispetto a quello associato al fascicolo.

Possono rappresentare delle eccezioni i fascicoli di persona fisica, come ad esempio il fascicolo del personale, che è aperto a livello del Titolo III (Risorse umane) in quanto possono confluire in esso documenti relativi al dipendente che possono essere ricondotti a classi diverse del predetto titolo, come ad esempio la classe 4 (Attribuzione di funzioni, ordini di servizio e missioni) piuttosto che la classe 13 (Giudizi, responsabilità e provvedimenti disciplinari).

L'Unione dei comuni di Terred'Acqua, in conformità con quanto previsto dalle Linee guida AgID, può quindi formare le seguenti tipologie di fascicoli:

- Fascicolo di procedimento: conserva una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento finale.
- Fascicolo di attività: comprende i documenti prodotti nello svolgimento di un'attività amministrativa semplice che implica risposte obbligate o meri adempimenti, per la quale quindi non è prevista l'adozione di un provvedimento finale. Ha in genere durata annuale.
- Fascicolo di affare: conserva i documenti relativi a una competenza non proceduralizzata, ma che nella consuetudine amministrativa la pubblica amministrazione deve concretamente portare a buon fine. Il fascicolo per affare ha una data di apertura e una durata circoscritta.
- Fascicolo di persona fisica/giuridica: Comprende tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona fisica o giuridica. Quasi sempre i fascicoli intestati alle persone restano correnti per molti anni, costituendo serie aperte.

4.7.2 Le serie

L'Unione dei comuni di Terred'Acqua può formare serie documentali annuali aggregando i documenti soggetti a registrazione particolare elencati nell'allegato 2 oppure serie di fascicoli con caratteristiche omogenee, memorizzando nel sistema di gestione informatica dei documenti i metadati previsti dalla vigente normativa per le aggregazioni documentali informatiche.

4.8 I metadati

I metadati consistono in dati associati a un documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo. L'allegato 5 alle Linee guida AgID stabilisce una serie di metadati - obbligatori e facoltativi - che, con riferimento ai documenti amministrativi informatici e alle aggregazioni documentali informatiche, devono essere generati e associati permanentemente ad essi.

Inoltre, L'Unione dei comuni di Terred'Acqua associa ai documenti e alle aggregazioni documentali informatiche ulteriori metadati rilevanti ai fini amministrativi o per finalità gestionali o conservative.

I metadati generati, associati alle diverse tipologie documentali prodotte ed acquisite e trasmessi al Sistema di conservazione unitamente ai documenti cui si riferiscono, sono elencati nel Disciplinare tecnico per lo svolgimento della funzione di conservazione dei documenti informatici condiviso dall'Unione dei comuni di Terred'Acqua con il conservatore ParER (allegato 5).

4.9 Flussi di lavorazione dei documenti

4.9.1 Flusso di lavorazione dei documenti in ingresso

Le operazioni previste per la gestione dei documenti in ingresso sono le seguenti:

- Ricezione
- Registrazione informatica dei documenti (registrazione di protocollo/registrazione particolare) e generazione del file Segnatura di protocollo
- Scansione dei documenti ricevuti in formato cartaceo
- Classificazione
- Assegnazione
- Fascicolazione

4.9.2 Flusso di lavorazione dei documenti in uscita

Le operazioni previste per la gestione dei documenti in uscita sono le seguenti:

- Formazione
- Registrazione informatica dei documenti (registrazione di protocollo/registrazione particolare) ed eventuale generazione del file Segnatura di protocollo
- Classificazione
- Fascicolazione
- Spedizione (o pubblicazione su portali dedicati nell'ambito dei servizi online)

4.9.3 Flusso di lavorazione dei documenti interni

Le operazioni previste per la gestione dei documenti interni sono le seguenti:

- Formazione
- Registrazione informatica dei documenti (registrazione di protocollo/registrazione particolare) ed eventuale generazione del file Segnatura di protocollo
- Classificazione
- Fascicolazione
- Assegnazione
- Eventuale Trasmissione

4.10 Pubblicazione dei documenti all'albo pretorio online

4.10.1 Ambito di applicazione

L'albo pretorio on line, ai sensi dell'art. 32, comma 1, della Legge 69/2009, dal 1 gennaio 2011 rappresenta l'unica forma di pubblicità legale degli atti e provvedimenti amministrativi soggetti per legge a obblighi di pubblicazione.

4.10.2 Principi e finalità

L'Albo pretorio informatico è istituito in apposita area individuata nel portale istituzionale dell'Unione al fine di assicurare l'adempimento degli obblighi di pubblicazione di atti e provvedimenti aventi effetto di pubblicità legale.

Restano, in ogni caso, salve le ulteriori forme di pubblicità previste da leggi e/o regolamenti per particolari tipi di atti.

4.10.3 Servizio albo pretorio

La tenuta dell'Albo pretorio online è a cura del Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, che procede alla pubblicazione degli atti esterni, mentre i singoli servizi dell'Unione sono responsabili della pubblicazione degli atti di loro competenza.

Il Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi individua i responsabili competenti per l'inserimento degli atti all'Albo pretorio.

4.10.4 Acquisizione dei documenti da parte degli utenti

Limitatamente al periodo di pubblicazione, l'acquisizione dei documenti pubblicati da parte dell'utenza avviene gratuitamente e senza formalità, mentre le disposizioni in materia fiscale e di bollo sono applicate solo in caso d'uso. Decorso il termine di pubblicazione legale, trova applicazione la disciplina in materia di diritto di accesso.

4.10.5 Modalità di pubblicazione dei documenti

I documenti soggetti ad obbligo di pubblicazione sono pubblicati in versione integrale e conforme all'originale, compresi gli eventuali allegati informatici.

I documenti sono pubblicati all'Albo pretorio informatico per il tempo stabilito dalle singole disposizioni di legge o di regolamento e sono rimossi dall'Albo al termine del periodo di pubblicazione.

Il periodo di pubblicazione è di quindici giorni consecutivi, salvo termini diversi previsti da norme speciali.

4.10.6 Annullamento della pubblicazione

Dopo la pubblicazione dell'atto, la registrazione di pubblicazione è immodificabile, salva la possibilità di inserire note interne di pubblicazione.

Il responsabile del procedimento amministrativo o il soggetto esterno istante possono richiedere l'annullamento della pubblicazione. L'atto rimane pubblicato fino al termine di pubblicazione originario con la dicitura "Annullato in data ...". Contestualmente è possibile richiedere la pubblicazione del documento corretto: in tal caso il termine di pubblicazione ricomincia a decorrere dalla data della nuova richiesta.

4.10.7 Competenze e responsabilità

Il programma di pubblicazione dei documenti integrato con il software gestionale del protocollo e degli atti amministrativi permette la gestione decentrata della pubblicazione degli atti all'Albo pretorio on line. Ciascun Servizio provvede quindi autonomamente alla pubblicazione degli atti di propria competenza, inserendo i dati richiesti dal sistema.

L'atto da pubblicare deve essere allegato alternativamente secondo le seguenti modalità:

a) in file formato PDF, firmato digitalmente;

b) in file formato PDF con firma a stampa e richiamo nell'atto all'art. 3, c. 2 del D.lgs. 39/1993;

c) in file formato PDF ottenuto dalla scansione del documento in formato cartaceo con firma autografa.

Spetta al responsabile del procedimento amministrativo o comunque al soggetto esterno richiedente garantire che l'atto da pubblicare sia conforme alle norme sulla tutela della riservatezza previste dal D. lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), nonché di ogni altra disposizione di legge o di regolamento che rilevi ai fini del trattamento di dati personali.

Il Responsabile del Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi non è responsabile del contenuto degli atti pubblicati nell'Albo pretorio.

4.10.8 Gestione del servizio per la pubblicazione di atti su richiesta di terzi

Il Responsabile del Servizio per la tenuta del protocollo informatico cura la pubblicazione degli atti su richiesta di soggetti esterni all'Amministrazione.

Le richieste di pubblicazione di atti da parte di soggetti esterni possono pervenire in uno qualunque dei modi di trasmissione di documenti previsti dal Manuale di Gestione, almeno il giorno lavorativo precedente la data di inizio della pubblicazione.

Il soggetto richiedente indica le date di inizio e fine pubblicazione, allegando, in alternativa:

- il file dell'atto da pubblicare in formato PDF, firmato digitalmente;
- il documento in formato cartaceo con firma autografa, che il Servizio per la tenuta del protocollo informatico provvederà a scansionare.

4.10.9 Registro dell'Albo pretorio e attestazione di pubblicazione

Il registro informatico dell'Albo pretorio contiene i dati di registrazione dei documenti pubblicati nell'Albo e si configura quindi come un registro particolare (vedi allegato 2).

L'attestazione di avvenuta pubblicazione nell'Albo pretorio viene rilasciata dal Responsabile del Servizio per la tenuta del protocollo informatico o da suo delegato soltanto ai soggetti terzi:

- tramite invio telematico degli estremi di pubblicazione all'ufficio o al soggetto richiedente, qualora il documento sia stato trasmesso in originale digitale o copia conforme digitale;
- tramite apposita comunicazione al soggetto esterno degli estremi di pubblicazione, qualora il documento sia stato trasmesso in formato analogico.

5 Conservazione dei documenti

Il Codice dei beni culturali obbliga le pubbliche amministrazioni a conservare i propri archivi nella loro organicità e ad ordinarli, nonché ad inventariare i propri archivi storici.

Il tempo di conservazione dei documenti, dei fascicoli e delle serie, indipendentemente dal loro formato analogico o digitale, è stabilito dal Piano di conservazione dell'ente (allegato 4), ovvero il documento, integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'art. 68 del DPR 445/2000.

Nel caso di documenti, fascicoli e serie per cui il Piano di conservazione non prevede la conservazione permanente, questi possono essere scartati solamente previa autorizzazione fornita dal Ministero della cultura (e precisamente nel caso dell'Unione dei comuni di Terred'Acqua, dalla

Soprintendenza archivistica e bibliografica per l'Emilia - Romagna), così come previsto dall'art. 21, comma 1, del predetto Codice.

5.1 Conservazione dei documenti amministrativi su supporto analogico: l'Archivio storico

La documentazione destinata alla conservazione permanente e relativa agli affari esauriti da oltre trent'anni sarà trasferita dall'archivio di deposito all'archivio storico.

5.2 Conservazione dei documenti amministrativi informatici: il sistema di conservazione

L'Unione dei comuni di Terred'Acqua ha affidato la conservazione di gran parte della documentazione informatica prodotta e acquisita durante lo svolgimento della propria attività al conservatore Regione Emilia Romagna (Servizio polo archivistico dell'Emilia-Romagna - ParER). Il conservatore, in conformità con quanto previsto dal CAD, assicura, per quanto in esso conservato, caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità secondo le modalità indicate nelle Linee guida AgID.

Lo svolgimento della funzione di conservazione affidata al ParER avviene con le modalità specificate nel Disciplinare tecnico (allegato 5) redatto d'intesa tra l'Unione dei comuni di Terred'Acqua (soggetto produttore dei documenti) e Regione Emilia-Romagna (soggetto conservatore), che ne regola i rapporti sulla base di quanto specificato nel Manuale di conservazione redatto dal ParER (che ne consente la consultazione sul proprio sito internet).

Come nel caso della documentazione cartacea conservata presso l'Archivio di deposito, anche la procedura di scarto dei documenti amministrativi informatici conservati, che avviene con le modalità descritte nel manuale di conservazione dei conservatori, si svolge in conformità con quanto previsto dal Piano di conservazione adottato dall'Unione dei comuni di Terred'Acqua (allegato 4) e deve essere preventivamente autorizzata dalla Soprintendenza archivistica per l'Emilia-Romagna, ai sensi di quanto previsto dal Codice dei beni culturali.

Nell'Unione dei comuni di Terred'Acqua il Responsabile della conservazione coincide con il Responsabile della gestione documentale.

6 Sicurezza del Sistema di gestione informatica dei documenti

Le pubbliche amministrazioni, al fine di attuare le Linee guida AgID, sono tenute ad ottemperare alle misure minime di sicurezza ICT emanate dalla stessa Agenzia con apposita circolare. In tale ottica, il Responsabile della gestione documentale - che nel caso dell'Unione dei comuni di Terred'Acqua ricopre anche il ruolo di Responsabile della conservazione - in accordo con il Responsabile per la transizione digitale e acquisito il parere del Responsabile della protezione dei dati personali, predispone il Piano della sicurezza del Sistema di gestione informatica dei documenti (allegato 6).

Il Piano prevede opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli articoli 9-10 del Regolamento

UE 679/2016 (GDPR): dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale; dati genetici o biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute/alla vita sessuale/all'orientamento sessuale della persona, dati personali relativi alle condanne penali e ai reati.

Il Piano, che è redatto nell'ambito del Piano generale della sicurezza, contiene anche la descrizione della procedura da adottarsi in caso di violazione dei dati personali, coerentemente con quanto previsto dal vigente Piano triennale per l'informatica nella Pubblica amministrazione.



UNIONE TERRED'ACQUA CITTÀ METROPOLITANA DI BOLOGNA

RIFERIMENTI NORMATIVI

ALLEGATO 1 AL MANUALE DI GESTIONE DOCUMENTALE DELL'UNIONE DEI COMUNI DI TERRED'ACQUA

Il presente allegato riporta la norme che contengono le disposizioni di riferimento in materia di formazione, gestione e conservazione documentale¹, di seguito riportate secondo il criterio gerarchico di ordinazione delle fonti:

- Regolamento europeo eIDAS 910/2014 del Parlamento europeo del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;
- Regolamento europeo 679/2016 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- Legge 241/1990 (*Nuove norme sul procedimento amministrativo*);
- Legge 244/2007 (*Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato*)²;
- Legge 9 gennaio 2004, n. 4, aggiornata dal decreto legislativo 10 agosto 2018, n. 106 (*Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici*);
- RD 262/1942 (*Codice Civile*);
- DPR 445/2000 (Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa);
- DPR 68/2005 (*Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3*);
- D.Lgs. 196/2003 (*Codice per la protezione dei dati personali*);
- D. Lgs. 42/2004 (*Codice dei beni culturali e del paesaggio*);
- D.Lgs. 82/2005 (*Codice dell'amministrazione digitale*);
- D.Lgs. 33/2013 (*Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*);

¹ Si è ritenuto opportuno non includere tra i riferimenti normativi quelli esclusivamente riguardanti le pubbliche amministrazioni statali come ad esempio il D.P.R. 37/2001 (*Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato*).

² Si tratta della Legge Finanziaria 2008, che introduce l'obbligo della fatturazione elettronica nei confronti della Pubblica Amministrazione.

- DM 2 novembre 2005 (*Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata*);
- DM 3 aprile 2013, n. 55 (*Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'articolo 1, commi da 209 a 213, della legge 24 dicembre 2007, n. 244*);
- DM 17 giugno 2014 (*Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005*);
- DPCM 22 febbraio 2013 (*Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71*);
- DPCM 21 marzo 2013 (*Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni*);
- DPCM 3 dicembre 2013 (*Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005*), articoli 2 comma 1, 6, 9, 18 commi 1 e 5, 20-21;
- Linee guida del 15 aprile 2019 dell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi;
- Linee guida del 6 giugno 2019 contenenti le Regole tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate;
- Linee guida del 9 gennaio 2020 sull'Accessibilità degli strumenti informatici;
- Linee guida sulla formazione, gestione e conservazione dei documenti informatici del maggio 2021;
- Circolare n. 41 del 14 dicembre 2015 della Direzione Generale Archivi (*Autorizzazione alla distruzione di originali unici riprodotti secondo le regole tecniche di cui al DPCM 13.11.2014 e conservati secondo le regole tecniche di cui al DPCM 13.12.2013*);
- Circolare AgID n. 2 del 18 aprile 2017 (*«Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)»*).



UNIONE TERRED'ACQUA
CITTÀ METROPOLITANA DI BOLOGNA

**DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE ED ESCLUSI DALLA
PROTOCOLLAZIONE, ED ELENCO DEI RELATIVI REGISTRI**

**ALLEGATO 2 AL MANUALE DI GESTIONE DOCUMENTALE DELL'UNIONE DEI COMUNI DI
TERRED'ACQUA**

Tipologia documentale	Registro particolare
Contratti	Registro dei contratti e delle convenzioni
Convenzioni	
Decreti	Registro dei decreti
Delibere	Registro delle delibere del Consiglio dell'Unione
	Registro delle delibere della Giunta dell'Unione
Determine	Registro delle determine dirigenziali
Fatture passive	Registro unico delle fatture
Notifiche	Registro delle notifiche
Ordinanze	Registro delle ordinanze
Buoni d'ordine	Registro dei buoni d'ordine

ALLEGATO 3

UNIONE TERRED'ACQUA		
Titolario di classificazione		
Titolo	Classe	Descrizione
1	0	Amministrazione generale
1	1	Legislazione e circolari esplicative
1	2	Denominazione, territorio e confini, circoscrizioni di decentramento, toponomastica
1	3	Statuto
1	4	Regolamenti
1	5	Stemma, gonfalone, sigillo
1	6	Archivio generale
1	7	Sistema informativo
1	8	Informazioni e relazioni con il pubblico
1	9	Politica del personale; ordinamento degli uffici e dei servizi
1	10	Relazioni con le organizzazioni sindacali e di rappresentanza del personale
1	11	Controlli interni ed esterni
1	12	Editoria e attività informativo-promozionale interna ed esterna
1	13	Cerimoniale, attività di rappresentanza; onorificenze e riconoscimenti
1	14	Interventi di carattere politico e umanitario; rapporti istituzionali
1	15	Forme associative e partecipative per l'esercizio di funzioni e servizi e adesione dell'Unione ad Associazioni
1	16	Area e città metropolitana
1	17	Associazionismo e partecipazione

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
2	0	Organi di governo, gestione, controllo, consulenza e garanzia
2	1	Presidente
2	2	Vice-Presidente
2	3	Consiglio
2	4	Presidente del Consiglio
2	5	Conferenza dei capigruppo e Commissioni del Consiglio
2	6	Gruppi consiliari
2	7	Giunta
2	8	Commissario prefettizio e straordinario
2	9	Segretario e Vice-segretario
2	10	Direttore generale e dirigenza
2	11	Revisori dei conti
2	12	Difensore civico
2	13	Commissario ad acta
2	14	Organi di controllo interni
2	15	Organi consultivi
2	16	Consigli circoscrizionali
2	17	Presidente dei Consigli circoscrizionali
2	18	Organi esecutivi circoscrizionali
2	19	Commissioni dei Consigli circoscrizionali
2	20	Segretari delle circoscrizioni
2	21	Commissario ad acta delle circoscrizioni
2	22	Conferenza dei Presidenti di quartiere

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
3	0	Risorse umane
3	1	Concorsi, selezioni, colloqui
3	2	Assunzioni e cessazioni
3	3	Comandi e distacchi; mobilità
3	4	Attribuzione di funzioni, ordini di servizio e missioni
3	5	Inquadramenti e applicazione contratti collettivi di lavoro
3	6	Retribuzioni e compensi
3	7	Trattamento fiscale, contributivo e assicurativo
3	8	Tutela della salute e sicurezza sul luogo di lavoro
3	9	Dichiarazioni di infermità ed equo indennizzo
3	10	Indennità premio di servizio e trattamento di fine rapporto, quiescenza
3	11	Servizi al personale su richiesta
3	12	Orario di lavoro, presenze e assenze
3	13	Giudizi, responsabilità e provvedimenti disciplinari
3	14	Formazione e aggiornamento professionale
3	15	Collaboratori esterni

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
4	0	Risorse finanziarie e patrimonio
4	1	Bilancio preventivo e Piano esecutivo di gestione (PEG)
4	2	Gestione del bilancio e del PEG (con eventuali variazioni)
4	3	Gestione delle entrate: accertamento, riscossione, versamento
4	4	Gestione della spesa: impegno, liquidazione, ordinazione e pagamento
4	5	Partecipazioni finanziarie
4	6	Rendiconto della gestione; adempimenti e verifiche contabili
4	7	Adempimenti fiscali, contributivi e assicurativi
4	8	Beni immobili
4	9	Beni mobili
4	10	Economato
4	11	Oggetti smarriti e recuperati
4	12	Tesoreria
4	13	Concessionari ed altri incaricati della riscossione delle entrate
4	14	Pubblicità e pubbliche affissioni

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
5	0	Affari legali
5	1	Contenzioso
5	2	Responsabilità civile e patrimoniale verso terzi; assicurazioni
5	3	Pareri e consulenze

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
6	0	Pianificazione e gestione del territorio
6	1	Urbanistica: piano regolatore generale e varianti
6	2	Urbanistica: strumenti di attuazione del piano regolatore generale
6	3	Edilizia privata
6	4	Edilizia pubblica
6	5	Opere pubbliche
6	6	Catasto
6	7	Viabilità
6	8	Servizio idrico integrato, luce, gas, trasporti pubblici, gestione dei rifiuti e altri servizi
6	9	Ambiente: autorizzazioni, monitoraggio e controllo
6	10	Protezione civile ed emergenze

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
7	0	Servizi alla persona
7	1	Diritto allo studio e servizi
7	2	Asili nido e scuola materna
7	3	Promozione e sostegno delle istituzioni di istruzione e della loro attività
7	4	Orientamento professionale; educazione degli adulti; mediazione culturale
7	5	Istituti culturali (Musei, Biblioteche, Teatri, Scuola comunale di musica, etc.)
7	6	Attività ed eventi culturali
7	7	Attività ed eventi sportivi
7	8	Pianificazione e accordi strategici con enti pubblici e privati e con il volontariato sociale
7	9	Prevenzione, recupero e reintegrazione dei soggetti a rischio
7	10	Informazione, consulenza ed educazione civica
7	11	Tutela e curatela di incapaci
7	12	Assistenza diretta e indiretta, benefici economici
7	13	Attività ricreativa e di socializzazione
7	14	Politiche per la casa
7	15	Politiche per il sociale

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
8	0	Attività economiche
8	1	Agricoltura e pesca
8	2	Artigianato
8	3	Industria
8	4	Commercio
8	5	Fiere e mercati
8	6	Esercizi turistici e strutture ricettive
8	7	Promozione e servizi

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
9	0	Polizia locale e sicurezza pubblica
9	1	Prevenzione ed educazione stradale
9	2	Polizia stradale
9	3	Informative
9	4	Sicurezza e ordine pubblico

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
10	0	Tutela della salute
10	1	Salute e igiene pubblica
10	2	Trattamento Sanitario Obbligatorio
10	3	Farmacie
10	4	Zooprofilassi veterinaria
10	5	Randagismo animale e ricoveri

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
11	0	Servizi demografici
11	1	Stato civile
11	2	Anagrafe e certificazioni
11	3	Censimenti
11	4	Polizia mortuaria e cimiteri

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
12	0	Elezioni ed iniziative popolari
12	1	Albi elettorali
12	2	Liste elettorali
12	3	Elezioni
12	4	Referendum
12	5	Istanze, petizioni e iniziative popolari

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
13	0	Affari militari
13	1	Leva e servizio civile sostitutivo
13	2	Ruoli matricolari
13	3	Caserme, alloggi e servitù militari
13	4	Requisizioni per utilità militari

UNIONE TERRED'ACQUA		
Titolario di classificazione		
Titolo	Classe	Descrizione
14	0	Oggetti diversi

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
15	0	Centrale Unica di Committenza
15	1	Procedure gare
15	2	Procedure affidamenti diretti
15	3	Comunicazioni varie
15	4	Accessi

MANUALE DI CONSERVAZIONE

<i>Codice documento</i>	ManualeConservazione
<i>Versione</i>	3.0

	<i>Data</i>	<i>Nominativo</i>	<i>Funzione</i>
<i>Redazione</i>	10/05/2023	Camilla Broccoli	Responsabile Servizi di conservazione digitali
		Cristiano Casagni	Responsabile Sistema di conservazione
<i>Verifica</i>	18/05/2023	Riccardo Righi	Responsabile funzione archivistica di conservazione
<i>Approvazione</i>	19/05/2023	Giuliano Franceschi	Responsabile dell'Area Polo Archivistico e Gestione Documentale

Il presente documento è rilasciato sotto la licenza

Attribuzione-Non commerciale

delle Creative Commons.



REGISTRO DELLE VERSIONI

Versione	Variazioni	Data
1.0	Prima emissione	30/11/2020
1.1	Aggiornamenti e correzioni minori	28/12/2021
2.0	Aggiornamenti a seguito della riorganizzazione regionale	17/06/2022
3.0	<p>Aggiornamenti a seguito della riorganizzazione regionale e correzioni minori. Sono stati specificamente aggiornati:</p> <ul style="list-style-type: none"> • Paragrafo 4.4 • Capitolo 5: revisione completa • Paragrafo 7.5 • Paragrafo 8.4 • Paragrafi 9.4, 9.5, 9.6 • Capitolo 10 	19/05/2023

SOMMARIO

1	SCOPO E AMBITO DEL DOCUMENTO	7
2	TERMINOLOGIA (GLOSSARIO, ACRONIMI).....	8
3	NORMATIVA E STANDARD DI RIFERIMENTO	19
3.1	Normativa di riferimento	19
3.2	Standard di riferimento.....	20
4	RUOLI E RESPONSABILITÀ.....	23
4.1	Modello organizzativo	23
4.2	Titolare e Produttore	25
4.3	Utente abilitato.....	27
4.4	Responsabile della conservazione.....	28
4.5	Conservatore.....	29
4.6	Organismi di tutela e vigilanza.....	30
5	STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE	33
5.1	Organigramma	33
5.2	Struttura organizzativa	34
6	OGGETTI SOTTOPOSTI A CONSERVAZIONE	41
6.1	Oggetti conservati.....	41
6.1.1	Unità archivistiche e Unità documentarie.....	45
6.1.2	Formati.....	46
6.1.3	Metadati.....	47
6.2	Pacchetto di versamento (SIP).....	48
6.3	Pacchetto di archiviazione (AIP).....	49
6.4	Pacchetto di distribuzione (DIP)	50
7	PROCESSO DI CONSERVAZIONE	51
7.1	Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico	51
7.1.1	Preacquisizione	53
7.1.2	Acquisizione	54
7.2	Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti.....	54
7.3	Accettazione e presa in carico dei pacchetti di versamento e generazione del rapporto di versamento	55
7.4	Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie.....	56
7.4.1	Monitoraggio	56
7.4.2	Gestione delle anomalie	58
7.5	Preparazione e gestione del Pacchetto di archiviazione.....	59
7.6	Preparazione e gestione del Pacchetto di distribuzione (DIP) ai fini dell'esibizione.....	62
7.7	Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti	63
7.8	Scarto dei pacchetti di archiviazione.....	64
7.9	Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori ..	64

8	IL SISTEMA DI CONSERVAZIONE.....	66
8.1	Componenti logiche.....	66
8.2	Componenti tecnologiche	69
8.2.1	SacER.....	70
8.2.2	VersO	72
8.2.3	PING	72
8.2.4	DPI.....	73
8.2.5	Interfacce di Acquisizione e di Recupero (Web Service)	73
8.2.6	TPI	74
8.2.7	DIPS.....	74
8.2.8	SIAM	75
8.2.9	Sacerlog	75
8.2.10	Componenti di supporto.....	76
8.3	Componenti fisiche.....	77
8.3.1	Schema generale	77
8.3.2	Caratteristiche tecniche dei Sistemi	80
8.4	Procedure di gestione e di evoluzione	83
8.4.1	Gestione dell'Esercizio.....	83
8.4.2	Gestione delle utenze	83
8.4.3	Gestione dei Malfunzionamenti.....	84
8.4.4	Gestione degli Incidenti di Sicurezza	84
8.4.5	Evoluzione pianificata	86
8.4.6	Richieste di Cambiamento	86
8.4.7	Progettazione e Realizzazione di Software Applicativo	87
8.4.8	Gestione dei Rilasci	88
8.4.9	Gestione e conservazione dei Log.....	88
8.5	Asset.....	89
9	MONITORAGGIO E CONTROLLI.....	90
9.1	Procedure di monitoraggio	90
9.2	Funzionalità per la verifica e il mantenimento dell'integrità e della consistenza degli archivi... 90	90
9.3	Soluzioni adottate in caso di anomalie	91
9.4	Verifica periodica di conformità a normativa e standard di riferimento.....	93
9.5	Audit e gestione delle Non Conformità	93
9.6	Controlli di sicurezza	94
10	TRATTAMENTO DEI DATI PERSONALI.....	95
11	DOCUMENTI DI RIFERIMENTO E ALLEGATI	98

INDICE DELLE FIGURE

Figura 1 - Sistema e attori	25
Figura 2 - Organizzazione della DGREI.....	34
Figura 3 - Struttura organizzativa di ParER	Errore. Il segnalibro non è definito.
Figura 4 - Modello di ordinamento di archivio derivato da ISAD	41
Figura 5 - Pacchetto informativo (da OAIS).....	44
Figura 6 - Struttura dell'Unità documentaria.....	45
Figura 7 - Schema logico del Sistema di conservazione.....	66
Figura 8 - Flussi di dati nel Sistema di conservazione	68
Figura 9 - Schema Tecnologico del Sistema di conservazione	69
Figura 10 - Schema Infrastrutturale del Sistema di conservazione	78
Figura 11 - Schema dei Sistemi di ParER	80
Figura 12 - Schema del Sito Primario	81
Figura 13 - Procedura di Gestione utenze.....	Errore. Il segnalibro non è definito.
Figura 14 - Procedura di Gestione delle Richieste di Informazioni, Reclami e Segnalazioni.....	Errore. Il segnalibro non è definito.
Figura 15 - Procedura di Gestione incidenti di sicurezza	Errore. Il segnalibro non è definito.
Figura 16 - Procedura di Gestione richieste di cambiamento	Errore. Il segnalibro non è definito.
Figura 17 - Procedura di Progettazione e realizzazione di software applicativo.....	Errore. Il segnalibro non è definito.
Figura 18 - Procedura di Gestione dei rilasci	Errore. Il segnalibro non è definito.
Figura 19 - Procedura di Audit del SGI.....	Errore. Il segnalibro non è definito.
Figura 20 - Gestione delle Non Conformità	Errore. Il segnalibro non è definito.
Figura 21 - Procedura di Verifiche Tecniche e VA/PT.....	Errore. Il segnalibro non è definito.

1 SCOPO E AMBITO DEL DOCUMENTO

Il presente documento è il *Manuale di conservazione* (d'ora in poi Manuale) della Regione Emilia-Romagna, che descrive il sistema di conservazione applicato dalla Regione Emilia-Romagna in quanto Conservatore sia all'interno della sua organizzazione che per altri soggetti pubblici. È predisposto dal Polo Archivistico regionale dell'Emilia-Romagna (d'ora in poi ParER), che realizza e gestisce il *processo di conservazione*.

In particolare, il presente Manuale, redatto secondo quanto previsto dal paragrafo 4.6 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici (d'ora in poi Linee Guida), descrive il modello organizzativo della conservazione adottato e illustra nel dettaglio l'organizzazione della struttura che realizza il *Processo di conservazione*, definendo i soggetti coinvolti e i ruoli svolti dagli stessi nel modello organizzativo di funzionamento dell'attività di *conservazione*. Descrive inoltre il processo, le architetture e le infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del *Sistema di conservazione*.

Gli elementi illustrati e descritti sono validi e rilevanti per Regione Emilia-Romagna e per tutti gli enti per i quali Regione Emilia-Romagna svolge la funzione di *conservazione* e realizza e gestisce il *processo di conservazione* ai sensi della normativa nazionale e regionale, secondo il modello organizzativo descritto al paragrafo 4.1.

In riferimento a quanto indicato nel paragrafo 4.3 delle Linee Guida il processo di conservazione viene svolto all'interno della struttura organizzativa dell'ente Regione, che si definisce costituito dalla Regione Emilia-Romagna (nelle sue articolazioni di Giunta regionale, comprese le Agenzie senza personalità giuridica, e Assemblea legislativa) e dalle seguenti Agenzie regionali con personalità giuridica: Agenzia Regionale per le Erogazioni in Agricoltura; Agenzia Regionale per la sicurezza territoriale e la Protezione Civile; Agenzia Regionale per lo Sviluppo dei Mercati Telematici, mentre viene svolta anche per altri soggetti all'esterno, quali gli enti e gli organismi regionali non precedentemente indicati e le aziende del Servizio Sanitario Regionale, oltre che gli enti del territorio regionale appositamente concordati. Inoltre, il presente Manuale è valido e rilevante anche per gli enti fuori dal territorio regionale, con cui sono stati stipulati appositi accordi.

Per le tipologie degli oggetti sottoposti a *conservazione* e i rapporti con i *Produttori* il presente Manuale è integrato da un **Disciplinare tecnico** specifico generato e aggiornato direttamente dal sistema di conservazione per ogni *Produttore*, che definisce le specifiche operative e le modalità di descrizione e di versamento nel *Sistema di conservazione* digitale dei *Documenti informatici* e delle *Aggregazioni documentali informatiche* oggetto di *conservazione*.

In osservanza di quanto stabilito dalle Linee Guida il presente Manuale di conservazione è adottato con provvedimento formale (Determina dirigenziale) e pubblicato sul sito istituzionale della Regione Emilia-Romagna.

La documentazione di riferimento sia tecnica (p.e. specifiche tecniche di versamento, modelli di *pacchetti informativi*) che amministrativa (p.e. schemi di accordo) ed altra eventuale documentazione di analisi di interesse generale sono pubblicate nel sito di ParER: <https://poloarchivistico.regione.emilia-romagna.it/>.

[\[Torna al Sommario\]](#)

2 TERMINOLOGIA (GLOSSARIO, ACRONIMI)

Per i termini utilizzati nel presente Manuale si rimanda al Glossario di cui all'Allegato 1 delle Linee Guida e alle definizioni del D.lgs. 82/2005 e del DPR 445/2000 e loro successive modificazioni e integrazioni. In generale la terminologia utilizzata si riferisce alle norme citate o a standard nazionali e internazionali.

Le definizioni riportate in ordine alfabetico in questo capitolo riguardano termini impiegati ripetutamente nel testo non presenti nelle fonti citate di cui si ritiene necessario fornire una definizione. Inoltre, sono riportate le definizioni sintetiche usate nel testo per citare la normativa e gli standard di riferimento, con la descrizione completa della fonte citata.

Nel testo del Manuale sono riportati in *corsivo* i termini riferiti al Glossario delle Linee Guida e in ***corsivo grassetto*** i termini contenuti nel presente capitolo.

Accordo: accordo tra il *Produttore* e ParER, che regola i rapporti di servizio, e più precisamente: la natura dei servizi offerti, le responsabilità delle parti e le condizioni economiche, oltre agli strumenti di consultazione e controllo. Con il termine "Accordo" si intendono anche le convenzioni sottoscritte con gli Enti del territorio dell'Emilia-Romagna.

Allegato: **Documento** che compone l'**Unità documentaria** per integrare le informazioni contenute nel **Documento principale**. È redatto contestualmente o precedentemente al **Documento principale**.

Annesso: **Documento** che compone l'**Unità documentaria**, generalmente prodotto e inserito nell'**Unità documentaria** in un momento successivo a quello di creazione dell'**Unità documentaria**, per fornire ulteriori notizie e informazioni a corredo del **Documento principale**.

Annotazione: **Documento** che compone l'**Unità documentaria** riportante gli elementi identificativi del **Documento** e del suo iter documentale (un tipico esempio di Annotazione è rappresentato dalla segnatura di protocollo).

Applet: programma che viene eseguito come "ospite" nel contesto di un altro programma, detto per questo container, su un computer client [...]. In altre parole, un applet è un programma progettato per essere eseguito all'interno di un programma-container; ne consegue che l'applet non può essere eseguito indipendentemente da un altro programma. (Fonte: Wikipedia)

Appliance: particolare dispositivo elettronico hardware provvisto di un software integrato con funzione di sistema operativo, utilizzato per eseguire particolari complesse e massicce funzioni applicative software. La differenza sostanziale con i normali server o le normali apparecchiature di rete è che l'appliance non è progettato per essere flessibile alle modifiche del software o dell'hardware successive alla configurazione e installazione fatta per la sua specifica funzione applicativa. (Fonte: Wikipedia)

Application server: tipologia di server che fornisce l'infrastruttura e le funzionalità di supporto, sviluppo ed esecuzione di applicazioni nonché altri componenti server in un contesto distribuito. Si tratta di un complesso di servizi orientati alla realizzazione di applicazioni ad architettura multilivello ed enterprise, con alto grado di complessità, spesso orientate per il web (applicazioni web). (Fonte: Wikipedia)

Archiving: processo di spostamento di dati, che non sono utilizzati frequentemente, su un dispositivo che ne garantisce la memorizzazione nel lungo periodo.

Autenticazione forte: procedura basata sull'utilizzo di due o più dei seguenti elementi [...] (i) qualcosa che solo l'utente conosce, p.e. una password [...] (ii) qualcosa che solo l'utente possiede, p.e. [...] un telefono cellulare (iii) qualcosa che caratterizza l'utente, p.e. [...] un'impronta digitale. (Fonte: Traduzione di citazione di Wikipedia inglese di un testo della Banca Centrale Europea)

Backup: replicazione, su un qualunque supporto di memorizzazione, di materiale informativo archiviato nella memoria di massa dei computer, al fine di prevenire la perdita definitiva dei dati in caso di eventi malevoli accidentali o intenzionali. (Fonte: Wikipedia)

Bilanciatore di carico: tecnica informatica che consiste nel distribuire il carico di elaborazione di uno specifico servizio tra più server. Si aumentano in questo modo la scalabilità e l'affidabilità dell'architettura nel suo complesso. (Fonte: Wikipedia)

BLOB: acronimo per Binary Large object; tipo di dato usato nei database per la memorizzazione di dati di grandi dimensioni in formato binario. (Fonte: Wikipedia)

Business intelligence (BI): un'applicazione di BI è uno strumento software che, acquisendo e manipolando masse di dati presenti su database o anche archivi de-strutturati, fornisce report, statistiche, indicatori, grafici costantemente aggiornati, facilmente adattabili e configurabili. (Fonte: Wikipedia)

Client: componente del sistema che accede ai servizi o alle risorse di un altro componente, detto **server**. Il termine client indica anche il software usato sul computer client per accedere alle funzionalità offerte dal **server**. (Fonte: Wikipedia)

Cloud computing: paradigma di erogazione di servizi offerti su richiesta da un fornitore a un cliente finale attraverso la rete internet (come l'archiviazione, l'elaborazione o la trasmissione dati), a partire da un insieme di risorse preesistenti, configurabili e disponibili in remoto sotto forma di architettura distribuita. (Fonte: Wikipedia)

Cloud Marketplace di AgID: piattaforma che espone i servizi e le infrastrutture qualificate da AgID secondo quanto disposto dalle Circolari AgID n. 2 e n.3 del 9 aprile 2018. A decorrere dal 1 aprile 2019, le Amministrazioni Pubbliche possono acquisire esclusivamente servizi qualificati da AgID e pubblicati nel Cloud Marketplace. (Fonte: AgID)

Cluster: insieme di dispositivi di elaborazione connessi in maniera più o meno stretta che operano insieme in modo tale da poter essere considerati un unico sistema. (Fonte: Wikipedia)

Componente: elemento che compone il **Documento**. Generalmente è un file, ma può essere anche composto solo da *metadati*.

Comunità di riferimento: un gruppo ben individuato di potenziali *Utenti* che dovrebbero essere in grado di comprendere un particolare insieme di informazioni. La Comunità di riferimento può essere composta da più comunità di *Utenti*. [Fonte: **OAIS**]

Contenuto informativo: l'insieme delle informazioni che costituisce l'obiettivo originario della *conservazione*. È composto dall'**Oggetto-dati** e dalle **Informazioni di rappresentazione**.
[Fonte: **OAIS**]

Continuità Operativa (Business Continuity): capacità di un'organizzazione di continuare a erogare prodotti o servizi a livelli predefiniti accettabili a seguito di un incidente. Si tratta di una disciplina di gestione che consente all'organizzazione - privata o pubblica che sia - di diventare più resiliente agli incidenti che potrebbero causarne l'interruzione delle attività o addirittura minacciarne l'esistenza. [...] Erroneamente, viene spesso confusa con il **Disaster Recovery** che è solo una parte specifica della business continuity, relativa in particolare ai processi informatici. La continuità operativa ha un campo di applicazione più ampio e si riflette anche su persone, siti, risorse e fornitori dell'organizzazione.

Data Center: struttura utilizzata per ospitare computer e componenti associati, quali dispositivi di telecomunicazioni e di **storage**, in generale con adeguati livelli di prestazioni e di sicurezza.
(Fonte: Wikipedia)

Data Breach: violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali. (Fonte: GarantePrivacy)

Data Guard: estensione del database Oracle che consente di mantenere dei database secondari allineati ad un database primario. (Fonte: Wikipedia)

DICOM (Digital Imaging and COmmunications in Medicine): standard che definisce i criteri per la comunicazione, la visualizzazione, l'archiviazione e la stampa di informazioni di tipo biomedico quali ad esempio immagini radiologiche. (Fonte: Wikipedia)

Disaster recovery: insieme delle misure tecnologiche e logistico / organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business per imprese, associazioni o enti, a fronte di gravi emergenze che ne intacchino la regolare attività.
(Fonte: Wikipedia)

Disciplinare tecnico: documento redatto con ogni *Produttore*, che definisce le specifiche operative e le modalità di descrizione e di versamento nel *Sistema di conservazione* digitale dei *Documenti informatici* e delle *Aggregazioni documentali informatiche* oggetto di *conservazione*.

DNS (Domain Name System): sistema utilizzato per la risoluzione di nomi dei nodi della rete in indirizzi IP e viceversa. (Fonte: Wikipedia)

Documenti di conservazione: evidenze informatiche prodotte nel corso del processo di conservazione o da altri *sistemi di conservazione*.

Documento: nell'uso del presente Manuale, elemento dell'**Unità documentaria**. Si distingue in **Documento principale, Allegato, Annesso, Annotazione**. Si tratta comunque di un **Documento archivistico (Record)**.

Documento archivistico (Record): Informazioni memorizzate su qualsiasi supporto o tipologia documentaria, prodotte o ricevute e conservate da un ente o da una persona nello svolgimento delle proprie attività o nella condotta dei propri affari. [fonte: **ISAD**]

Documento principale: Documento che deve essere obbligatoriamente presente nell'**Unità documentaria**, della quale definisce il contenuto primario.

EJB (Enterprise JavaBean): componenti software che implementano, lato server, la logica di business di un'applicazione web all'interno della piattaforma **J2EE**. (Fonte: Wikipedia)

Elenco di versamento: documento in formato XML in cui sono indicati i *Documenti informatici* e le *Aggregazioni documentali informatiche* acquisiti dal *Sistema di conservazione* e una serie di informazioni relative alle verifiche a cui sono stati sottoposti durante il processo di acquisizione e *presa in carico*.

Esito versamento: documento in formato XML prodotto al termine delle verifiche in fase di **versamento**, memorizzato nel *Sistema di conservazione* e inviato al sistema versante.

File system: meccanismo con il quale i file sono posizionati e organizzati o su un dispositivo di archiviazione o su una memoria di massa, come un disco rigido o un CD-ROM e, in casi eccezionali, anche sulla RAM. (Fonte: Wikipedia)

Firma detached: firma digitale che è tenuta separata dai dati firmati, a differenza della firma digitale completa, che è inglobata nel file stesso. Ciò permette di poter lavorare con il file originale senza dover aprire un file firmato digitalmente, ma, ovviamente, qualsiasi modifica al file originale interrompe lo stretto legame con la firma, nel senso che un file differente non possiederà la medesima firma. (Fonte: Wikipedia)

Firewall: componente di difesa perimetrale di una rete informatica, che può anche svolgere funzioni di collegamento tra due o più tronconi di rete, garantendo dunque una protezione in termini di sicurezza informatica della rete stessa. (Fonte: Wikipedia)

Framework di sviluppo: architettura logica di supporto su cui un software può essere progettato e realizzato, spesso facilitandone lo sviluppo da parte del programmatore. (Fonte: Wikipedia)

FTP (File Transfer Protocol): protocollo per la trasmissione di dati tra host (client) e server, particolarmente adatto al trasferimento di file di grandi dimensioni. (Fonte: Wikipedia)

FTPS (File Transfer Protocol Secure): estensione del protocollo **FTP** con utilizzo di protocolli crittografici. (Fonte: traduzione di Wikipedia inglese)

FTP server: programma che permette di accettare connessioni in entrata e di comunicare con un **client** attraverso il protocollo **FTP**. (Fonte: Wikipedia)

GDPR: Regolamento (UE) del 27 aprile 2016, n. 679, del Parlamento europeo e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), noto con l'acronimo GDPR (General Data Protection Regulation).

Grant: istruzione SQL utilizzata per fornire a uno specifico utente o ruolo o a tutti gli utenti i privilegi necessari per eseguire delle azioni su oggetti di data base. (Fonte: tradotto da Oracle inglese)

HSM (Hardware Security Module): dispositivo fisico che garantisce e gestisce chiavi digitali per l'**autenticazione forte** e realizza processi di crittografia. Questi moduli in generale hanno la forma di una scheda o di un dispositivo esterno che si connette a un computer o a un server di rete (Fonte: tradotto da Wikipedia inglese)

HTTP (HyperText Transfer Protocol): principale protocollo utilizzato per la trasmissione d'informazioni sul web. (Fonte: Wikipedia)

HTTPS (HyperText Transfer Protocol over Secure Socket Layer): risultato dell'applicazione di un protocollo di crittografia al protocollo di trasmissione **HTTP**. (Fonte: Wikipedia)

IdP (Identity Provider): strumento per rilasciare le informazioni di identificazione di tutti i soggetti che cercano di interagire con un sistema. Ciò si ottiene tramite un modulo di autenticazione che verifica un token di sicurezza come alternativa all'autenticazione esplicita di un utente all'interno di un ambito di sicurezza. (Fonte: Wikipedia)

Incidente di sicurezza delle informazioni: evento o serie di eventi relativo alla sicurezza delle informazioni, non voluti o inattesi, che hanno una probabilità significativa di compromettere le attività istituzionali o di affari e di minacciare la sicurezza delle informazioni. (Def. 2-36 STD ISO27000:2014).

Indice dell'AIP: file XML che contiene tutti gli elementi del *Pacchetto di archiviazione*, derivati sia dalle informazioni contenute nel SIP (o nei SIP) trasmessi dal *Produttore*, sia da quelle generate dal *Sistema di conservazione* nel corso del *processo di conservazione*.

Indice del SIP: file XML che contiene i *metadati* e la struttura del *Sistema di versamento*, nonché i riferimenti ai file dei **Componenti**.

Indirizzo IP: etichetta numerica che identifica univocamente un dispositivo detto host collegato a una rete informatica che utilizza l'Internet Protocol come protocollo di rete. (Fonte: Wikipedia)

Informazioni descrittive: descrivono il *pacchetto informativo* e consentono di ricercarlo nel *sistema di conservazione*. In base alle caratteristiche della tipologia di oggetto contenuto nel *Pacchetto*, tali informazioni possono essere un sottoinsieme di quelle presenti nel *pacchetto informativo*, possono coincidere o possono anche essere diverse.

Informazioni sulla conservazione (PDI): informazioni necessarie a conservare il **Contenuto informativo** e a garantire che lo stesso sia chiaramente identificato e che sia chiarito il contesto in cui è stato creato. Sono costituite da *metadati* che definiscono la provenienza, il contesto, l'identificazione e l'*integrità* del **Contenuto informativo** oggetto della *conservazione*. [Fonte: **OAIS**]

Informazioni sulla rappresentazione: informazioni che associano un **Oggetto-dati** a concetti più significativi. [Fonte: **OAIS**]

Informazioni sull'impacchettamento (PI): informazioni che consentono di mettere in relazione nel *Sistema di conservazione*, in modo stabile e persistente, il **Contenuto informativo** con le relative **Informazioni sulla conservazione**. [Fonte: **OAIS**]

ISAD: ICA - ISAD (G): General International Standard Archival Description - Second Edition - Adopted by the Committee on Descriptive Standards Stockholm, Sweden, 19-22 September 1999.

Istanza: copia dell'applicativo dedicata ad uno scopo specifico.

JAVA: piattaforma software che ha come caratteristica peculiare il fatto di rendere possibile la scrittura e l'esecuzione di applicazioni scritte in linguaggio Java, che siano indipendenti dall'hardware sul quale poi sono eseguite. (Fonte: Wikipedia)

J2EE (Java Platform, Enterprise Edition): specifica le cui implementazioni vengono principalmente sviluppate in linguaggio di programmazione Java e ampiamente utilizzata nella programmazione Web. Ha come scopo la separazione delle funzionalità relative alla visualizzazione delle pagine web da quelle per la gestione della logica di business e del salvataggio delle informazioni sulla base dati. (Fonte: Wikipedia)

Lepida: rete delle Pubbliche Amministrazioni dell'Emilia-Romagna istituita dalla legge regionale n. 11/2004, principalmente costituita da collegamenti in fibra ottica ed estesa nel territorio appenninico attraverso dorsali radio in tecnologia Hyperlan. (Fonte: sito di Lepida s.c.p.a.)

Linee Guida: Linee Guida sulla formazione, gestione e conservazione dei documenti informatici pubblicate da AgID

Magic number: sequenza di bit, normalmente posta prima della sequenza di dati, che serve per definire il formato in cui i dati sono memorizzati. [...] Oggi la maggior parte dei formati del file hanno un magic number, costituito da un numero di byte variabile (solitamente da 2 a 10). I file immagine GIF, per esempio, cominciano sempre con la stringa ASCII GIF87a o GIF89a che definisce lo standard al quale il file aderisce. [...] I file PDF iniziano con "%PDF". (Fonte: Wikipedia)

Marca temporale: sequenza di caratteri che rappresentano una data e/o un orario per accertare l'effettivo avvenimento di un certo evento. La data è di solito presentata in un formato compatibile, in modo che sia facile da comparare con un'altra per stabilirne l'ordine temporale. La pratica dell'applicazione della marca temporale è detta *timestamping*. (Fonte: Wikipedia)

Massimario di scarto: vedi **Piano di Conservazione**.

Microservizi: approccio architetturale alla realizzazione di applicazioni caratterizzata dalla suddivisione dell'applicazione nelle sue funzioni di base. Ciascuna funzione, denominata servizio, può essere compilata e implementata in modo indipendente. Pertanto, i singoli servizi possono funzionare, o meno, senza compromettere gli altri (Fonte: RedHat)

Migrazione: procedimento atto a trasformare il software, l'hardware, oppure i dati nell'ambito di un sistema informativo o nel passaggio da un sistema ad un altro.

Mimetype: identificatore standard utilizzato su internet per indicare il tipo di dati contenuti in un file. I mimetype sono definiti in un Registro ufficiale gestito dalla Internet Assigned Numbers Authority (IANA). (Fonte: Wikipedia)

Multi-tenant: architettura software in cui una singola istanza del software è eseguita da un server ed è fruita da diverse organizzazioni che, ciascuna con le sue peculiarità ambientali, che costituiscono concettualmente uno specifico tenant, vedono il software come a loro utilizzo esclusivo. (Fonte: Wikipedia)

Near-line: termine usato in informatica per descrivere un tipo intermedio di archiviazione dati che rappresenta un compromesso tra lo storage on-line (con accesso ai dati frequente, molto rapido) e storage/archiviazione off-line (usato ad esempio per i backup, con accesso infrequente ai dati). (Fonte: Wikipedia)

NOC (Networking Operations Center): sito (o insieme di siti) da cui viene effettuato il controllo dell'operatività di una rete di apparecchiature informatiche e di server (Fonte: tradotto da Wikipedia inglese)

NTP (Network Time Protocol): protocollo per sincronizzare gli orologi dei computer all'interno di una rete. (Fonte: Wikipedia)

OAIS: ISO 14721:2012: Space data and information transfer systems -- Open archival information system - Reference model, OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione.

Object storage: architettura di calcolatori dedicati alla memorizzazione di dati, che gestisce i dati come oggetti, anziché come gerarchia di file, come fanno invece i file system; ogni oggetto contiene i dati, una quantità variabile di metadati e un identificatore univoco. (Fonte: tradotto da Wikipedia inglese)

Oggetto-dati: un oggetto composto da un insieme di sequenze di bit. [Fonte: **OAIS**]

PACS: acronimo anglosassone di Picture Archiving and Communication System (Sistema di archiviazione e trasmissione di immagini). Consiste in un sistema hardware e software dedicato all'archiviazione, trasmissione, visualizzazione e stampa delle immagini diagnostiche digitali. (Fonte: Wikipedia)

Partitioning: suddivisione di un database o dei suoi costituenti in parti indipendenti; viene utilizzata per ragioni di performance, gestibilità e disponibilità dei dati. (Fonte: tradotto da Wikipedia inglese)

Penetration test: processo operativo di valutazione della sicurezza di un sistema o di una rete che simula l'attacco di un utente malintenzionato. (Fonte: Wikipedia)

Persistenza: possibilità di far sopravvivere delle strutture dati all'esecuzione di un singolo programma, salvando i dati in uno storage non volatile, come su un *file system* o su un database. (Fonte: Wikipedia)

Piano di conservazione: l'art. 68 del DPR 445/2000 (Disposizioni per la conservazione degli archivi), prevede la dotazione da parte dell'ente di un piano di conservazione degli archivi, che

deve consentire di selezionare i documenti destinati alla conservazione permanente e di identificare quelli passibili di scarto, secondo quanto indicato nel Massimario di Scarto, nel rispetto delle disposizioni vigenti in materia di tutela dei beni culturali.

Protocollo di rete: descrizione a livello logico del processo di comunicazione (meccanismi, regole o schema di comunicazione) tra terminali e apparati preposto al funzionamento efficace della comunicazione in rete. (Fonte: Wikipedia)

Proxy: un server proxy è un server (inteso come sistema informatico o applicazione), che funge da intermediario per le richieste da parte dei client alla ricerca di risorse su altri server, disaccoppiando l'accesso al web dal browser. Un client si connette al server proxy, richiedendo qualche servizio (ad esempio un file, una pagina web o qualsiasi altra risorsa disponibile su un altro server), e quest'ultimo valuta ed esegue la richiesta in modo da semplificare e gestire la sua complessità. (Fonte: Wikipedia)

RAC: in un ambiente Oracle RAC due o più computer, ognuno con un'istanza del software accedono contemporaneamente allo stesso database. Ciò consente a un'applicazione o a un utente di connettersi a ambedue i computer, mantenendo un accesso coordinato ai dati. (Fonte: tradotto da Wikipedia inglese)

Raccolta di archiviazione (AIC): *Pacchetto di archiviazione* (AIP), il cui contenuto informativo è costituito da un insieme di altri Pacchetti di archiviazione, in particolare aggregazione di AIP delle singole unità documentarie appartenenti all'aggregazione. [Fonte: **OAIS**]

Regione: Regione Emilia-Romagna, nelle sue articolazioni di Giunta regionale, comprese le Agenzie senza personalità giuridica, e l'Assemblea legislativa

Release: specifica versione di un software resa disponibile ai suoi utenti finali. La release è univocamente identificata da un numero in modo da distinguerla dalle precedenti e future altre release del software. Convenzionalmente si distinguono release maggiori, dette *major release*, quando le differenze dalla release precedente riguardano sostanziali evoluzioni delle funzionalità del software, e release minori, dette *minor release*, quando le differenze riguardano principalmente correzioni di malfunzionamenti del software. (Fonte: Wikipedia)

ReST (REpresentational State Transfer): insieme di principi di architetture di rete, i quali delineano come le risorse sono definite e indirizzate. Il termine è spesso usato nel senso di descrivere ogni semplice interfaccia che trasmette dati su **HTTP** senza un livello opzionale. (Fonte: Wikipedia)

S3: Servizio di **Object storage** accessibile via web fornito da Amazon; per l'accesso al servizio da parte degli applicativi Amazon mette a disposizione funzionalità di interfaccia che sono diventate uno standard de facto, accettato da molti dei sistemi di **Object storage** presenti sul mercato.

SaaS (Software as a Service): modello di distribuzione del software applicativo dove un produttore di software sviluppa, opera e gestisce un'applicazione web, che mette a disposizione dei propri clienti via Internet; spesso si tratta di un servizio di **cloud computing**. (Fonte: Wikipedia)

SCP (Secure Copy): protocollo per trasferire in modo sicuro un file tra un computer locale ed un host remoto o tra due host remoti. (Fonte: Wikipedia)

Serie: Unità Archivistiche o Unità Documentarie ordinate secondo un *sistema di classificazione* o conservati insieme perché:

- sono il risultato di un medesimo processo di sedimentazione o archiviazione o di una medesima attività;
- appartengono ad una specifica **tipologia documentaria**;
- sussiste qualche altra relazione derivante dalle modalità della loro produzione, acquisizione o uso.

(fonte: **ISAD**)

Server: componente o sottosistema informatico di elaborazione e gestione del traffico di informazioni che fornisce, a livello logico e fisico, un qualunque tipo di servizio ad altre componenti (tipicamente chiamate **client**) che ne fanno richiesta attraverso una rete di computer, all'interno di un sistema informatico o anche direttamente in locale su un computer. (Fonte: Wikipedia)

Servlet container: componente di un web server che interagisce con i servlet, ovvero con programmi in linguaggio Java atti alla generazione dinamica di pagine web. (Fonte: tradotto da Wikipedia inglese)

SGI: Sistema di Gestione Integrato, che armonizza il Sistema di Gestione della Qualità (**SGQ**), il Sistema di Gestione della Sicurezza delle Informazioni (**SGSI**) e il Sistema di Gestione Anticorruzione.

SGQ (Sistema di Gestione della Qualità): insieme formalizzato delle attività collegate e interdipendenti che influenzano la qualità di un prodotto o di un servizio. Documenta i processi, le procedure ISO 9001 e le responsabilità per il raggiungimento delle politiche della qualità e degli obiettivi della qualità.

SGSI (Sistema di Gestione della Sicurezza delle Informazioni): strumento che permette di controllare in modo sistematico e continuativo i processi che riguardano la sicurezza di tutto il patrimonio informativo aziendale, non solo dal punto di vista informatico, ma anche e soprattutto dal punto di vista gestionale ed organizzativo, definendo ruoli, responsabilità e procedure formali per l'operatività dell'organizzazione.

SIEM (Security Information and Event Management): le soluzioni rientranti in questa categoria di sistemi sono contraddistinte dalla capacità di effettuare analisi anche real-time degli allarmi di sicurezza generati dagli apparati hardware di rete e dalle applicazioni software di gestione e monitoraggio. Le soluzioni SIEM sono anche impiegate per effettuare il log delle informazioni di sicurezza e generare dei report funzionali alle tematiche di rispetto delle norme e degli standard. (Fonte: Wikipedia)

SID (Settore Innovazione Digitale, dati, tecnologia e polo archivistico): Settore, appartenente alla Direzione Generale Risorse, Europa, Innovazione e Istituzioni, che si occupa della progettazione e gestione dei Servizi IT, del presidio della Sicurezza informatica, della Statistica e della Conservazione.

SOC (Security Operation Center): centro da cui vengono forniti servizi finalizzati alla sicurezza dei sistemi informativi dell'azienda stessa o di clienti esterni.

Un SOC fornisce tre tipologie di servizi:

- di gestione: tutte le attività di gestione delle funzionalità di sicurezza legate all'infrastruttura IT (rete, sistemi ed applicazioni) sono centralizzate dal SOC;
- di monitoraggio: l'infrastruttura IT e di Sicurezza vengono monitorate in tempo reale al fine di individuare tempestivamente tentativi di intrusione, di attacco o di uso malevolo dei sistemi;
- proattivi: sono servizi finalizzati a migliorare il livello di protezione dell'organizzazione.

(Fonte: Wikipedia)

Sotto componente: *Componente* di un **Componente**. Per esempio, sono Sotto componenti la **marca temporale** (se detached) o la Firma digitale (sempre se detached) di un determinato **Componente**.

SPID: (Sistema Pubblico di Identità Digitale) è il Sistema Pubblico di Identità Digitale che garantisce a tutti i cittadini e le imprese un accesso unico, sicuro e protetto ai servizi digitali della Pubblica Amministrazione e dei soggetti privati aderenti. (Fonte: AgID)

Storage: dispositivo per memorizzare i dati in formato digitale, quale un dispositivo a cassette o un dispositivo a disco.

Struttura versante (o Struttura): ripartizione dell'**Ente produttore** identificativa della specifica funzione di produzione dei documenti versati, in genere coincidente con la *funzione organizzativa omogenea*.

Tape library: sistema automatico composto da alloggiamenti contenenti cassette magnetiche, dispositivi di lettura/scrittura delle cassette stesse e dispositivi di riconoscimento automatico delle cassette. (Fonte: Wikipedia)

Tempo UTC (Tempo coordinato universale): fuso orario di riferimento da cui sono calcolati tutti gli altri fusi orari del mondo. Esso è derivato dal tempo medio di Greenwich (in inglese Greenwich Mean Time, GMT), con il quale coincide a meno di approssimazioni infinitesimali, e perciò talvolta è ancora chiamato, sia pure impropriamente, GMT. (Fonte: Wikipedia)

Tipologia documentaria: categoria di **Documenti** omogenei per natura e funzione giuridica, modalità di registrazione o di produzione, che hanno comuni caratteristiche formali e/o intellettuali; nel sistema SacER, che fa riferimento al più complesso concetto di **Unità Documentaria**, anziché di Documento, si preferisce parlare di "Tipo di Unità Documentaria"

Trouble ticket: sistema informatico che registra e gestisce liste di richieste di assistenza o di problemi, organizzato secondo le necessità di chi offre il servizio. [...] Un ticket serve per mantenere la sequenza di attività derivate di una richiesta. Ad ogni ticket corrisponde un identificativo univoco, che ne consente l'archiviazione e la consultazione in qualunque momento da parte del personale coinvolto nella sua gestione. I ticket vengono 'creati' o 'aperti', all'atto della ricezione di una nuova richiesta, e l'obiettivo è di 'chiuderli' o 'risolverli', fornendo la soluzione al problema segnalato. (Fonte: Wikipedia)

Unità archivistica: insieme organizzato di **Unità documentarie** o **Documenti** raggruppati dal *Produttore* per le esigenze della sua attività corrente in base al comune riferimento allo stesso oggetto, attività o fatto giuridico. Può rappresentare una unità elementare di una **Serie**. [Fonte: **ISAD**]

Unità di archiviazione (AIU): *Pacchetto di archiviazione* (AIP) elementare, il cui contenuto informativo non è ulteriormente decomposto in altri contenuti informativi. Definisce un AIP di **Unità documentaria**. [Fonte: **OAIS**]

Unità documentaria (item): aggregato logico costituito da uno più **Documenti** che sono considerati come un tutto unico. Costituisce l'unità elementare in cui è composto l'*archivio*, cioè l'unità minima, concettualmente non divisibile, di cui è composto un archivio o, in altri termini, la più piccola distinta unità di **Documenti** gestita come entità. Può contenere **Componenti**, come ad esempio una e-mail con allegati; comunque, i **Componenti** dell'Unità documentaria sono gestiti come una singola entità nel sistema. [Fonte: **ISAD e ISO 23081**]

Versamento: azione di *trasferimento* di SIP dal **Produttore** al *Sistema di conservazione*.

Versamento anticipato: **versamento** nel *Sistema di conservazione* di *Documenti informatici* che si trovano ancora nella fase attiva del loro ciclo di vita.

Versamento in archivio: **versamento** nel Sistema di *Aggregazioni documentali informatiche* nella loro forma stabile e definitiva (principalmente Fascicoli chiusi e **Serie** annuali complete), ovvero che hanno esaurito il loro ciclo di vita attivo per entrare in quello semi-attivo.

Vulnerabilità: componente di un sistema, in corrispondenza del quale le misure di sicurezza sono assenti, ridotte o compromesse, il che rappresenta un punto debole del sistema e consente a un eventuale aggressore di compromettere il livello di sicurezza dell'intero sistema. (Fonte: Wikipedia)

Vulnerability assessment: processo che porta a identificare, quantificare, valutare la priorità (o l'importanza) delle **vulnerabilità** in un sistema. (Fonte: tradotto da Wikipedia inglese)

Web Server: applicazione software che, in esecuzione su un server, è in grado di gestire le richieste di trasferimento di pagine web di un **client**, tipicamente un web browser, tramite il protocollo **HTTP** o eventualmente la versione sicura **HTTPS**. (Fonte: Wikipedia)

Web Service: un sistema software progettato per supportare l'*interoperabilità* tra diversi sistemi in una medesima rete oppure in un contesto distribuito. (Fonte: Wikipedia)

ZIP: formato di compressione dei dati molto diffuso nei computer con sistemi operativi Microsoft e supportato di default nei computer con sistema operativo Mac OS X. Supporta vari algoritmi di compressione. (Fonte: Wikipedia)

[\[Torna al Sommario\]](#)

3 NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

Le normative in vigore nei luoghi dove sono conservati i documenti, cioè la normativa europea, nazionale italiana e regionale dell'Emilia-Romagna e gli standard di riferimento sono riportati in modo più dettagliato e secondo la gerarchia delle fonti nell'Allegato 1 "Normativa e standard di riferimento" che viene mantenuto costantemente aggiornato e pubblicato on-line sul sito di ParER.

Alla data l'elenco dei principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti, è costituito da:

Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica.

Legge del 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.

Decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.

Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

Decreto Legislativo 10 agosto 2018, n. 101 che ha dettato disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016.

Decreto Legislativo del 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali.

Decreto Legislativo del 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio.

Decreto Legislativo del 7 marzo 2005 n. 82 e s.m.i – Codice dell'amministrazione digitale (CAD).

Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71.

Decreto del Ministero dell'Economia e delle Finanze del 17 giugno 2014 - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005.

Circolare AgID del 9 aprile 2018, n. 2 – Criteri per la qualificazione dei Cloud Service Provider per la PA

Circolare AgID del 9 aprile 2018, n. 3 – Criteri per la qualificazione di servizi SaaS per il Cloud della PA

Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, pubblicate da AgID nel settembre 2020 e aggiornate nel maggio 2021, con relativi allegati

Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici pubblicato da AgID nel giugno 2021 e aggiornato nel dicembre 2021, con relativi allegati

[\[Torna al Sommario\]](#)

3.2 Standard di riferimento

ICA - ISAD (G): General International Standard Archival Description - Second Edition -Adopted by the Committee on Descriptive Standards Stockholm, Sweden, 19-22 September 1999. Traduzione italiana a cura di Stefano Vitali, con la collaborazione di Maurizio Savoja, Firenze 2000. Standard dell'ICA (International Council on Archives – Conseil International des Archives) che fornisce delle norme generali per l'elaborazione di descrizioni archivistiche.

ISO 14721:2012 – Open Archival Information System (**OAIS**) – Reference model (CCSDS 650.0-M-2, Recommend Practice, Magenta Book June 2012): definisce concetti, modelli e funzionalità inerenti agli archivi digitali e ciò che è richiesto per garantire una conservazione permanente, o per un lungo termine indefinito, di informazioni digitali. Questa versione sostituisce la prima (ISO 14721:2003 - CCSDS 650.0-B-1 – Blue Book, January 2002) di cui è disponibile una traduzione in italiano (Sistema informativo aperto per l'archiviazione: traduzione italiana: *OAIS. Sistema informativo aperto per l'archiviazione*, a cura di Giovanni Michetti, Roma, ICCU 2007).

ISO 15836:2009 - Information and documentation – The Dublin Core metadata element set. Sistema di metadati del Dublin Core (questa versione sostituisce la precedente: ISO 15836:2003).

ISO 16363:2012 - Space data and information transfer systems - Audit and certification of trustworthy digital repositories (CCSDS 652.0-M-1 Recommend Practice, Magenta Book September 2011).

ISO 17025:2018 - General requirements for the competence of testing and calibration laboratories. Norma che esprime i "Requisiti generali per la competenza dei laboratori di prova e di taratura".

ISO 23081-1:2006 - Information and documentation – Records management processes – Metadata for records – Part 1- Principles. Quadro di riferimento per lo sviluppo di un Sistema di metadati per la gestione documentale.

ISO/TS 23081-2:2007: - Information and documentation – Records management processes – Metadata for records – Part 2- Conceptual and implementations issues. Guida pratica per l'implementazione.

ISO 23081-2:2009: - Information and documentation – Managing Metadata for records – Part 2- Conceptual and implementations issues. Guida pratica per l'implementazione.

LTO6: LTO (Linear Tape Open) è uno standard "open" sviluppato alla fine del 1990 come tecnologia di storage dei dati su nastro. La versione 6 è stata definita alla fine del 2012.

PREMIS: Data Dictionary for Preservation Metadata. Risultato dell'attività di un gruppo di lavoro transnazionale costituito nel 2003, definisce l'insieme essenziale di metadati necessari per tracciare il processo di conservazione. La versione 3.0 è stata definita nel giugno del 2015 e rivista nel novembre 2015.

SQL: (Structured Query Language) è un linguaggio standardizzato per database basati sul modello relazionale (RDBMS).

UNI 11386:2020: - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI SInCRO): Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali: definisce la struttura dell'insieme di dati a supporto del processo di conservazione e recupero degli oggetti digitali, individuando gli elementi informativi necessari alla creazione dell'indice di conservazione e descrivendone sia la semantica sia l'articolazione per mezzo del linguaggio formale XML.

UNI ISO 15489-1:2006: Informazione e documentazione – Gestione dei documenti di archivio – Principi generali sul record management.

UNI ISO 15489-2:2007: Informazione e documentazione – Gestione dei documenti di archivio – Linee guida sul record management.

ISO/IEC 9001:2015: requisiti per la realizzazione all'interno di un'organizzazione di un sistema di gestione della qualità.

ISO/IEC 27001:2013: Information technology -- Security techniques -- Information security management systems -- Requirements. Requisiti di un ISMS (Information Security Management System).

ISO/IEC 27017:2015: Codice di condotta per i controlli di sicurezza delle informazioni per i servizi in cloud.

ISO/IEC 27018:2014: - Codice di condotta per la protezione delle informazioni di identificazione personale (PII) in cloud pubblici.

ISO 22301:2012: Societal security -- Business continuity management systems --- Requirements.

ETSI TS 101 533-1 v1.3.1 (2012-04) - Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management. Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.

ETSI TR 101 533-2 v1.3.1 (2012-04) - Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors. Linee guida per valutare sistemi sicuri e affidabili per la conservazione delle informazioni.

[\[Torna al Sommario\]](#)

4 RUOLI E RESPONSABILITÀ

4.1 Modello organizzativo

La Regione Emilia-Romagna con la legge regionale 24 maggio 2004 n. 11 (Sviluppo regionale della società dell'informazione e sue successive modificazioni¹) ha definito la propria declinazione del modello organizzativo per la conservazione stabilendo, all'art. 2 comma 4bis, che:

La Regione, anche in collaborazione con le altre pubbliche amministrazioni interessate, favorisce [...] lo sviluppo integrato della conservazione digitale dei documenti informatici e, nel rispetto dei principi di efficacia, efficienza ed economicità, svolge, con le modalità previste dalle disposizioni vigenti, le funzioni di archiviazione e conservazione digitale dei documenti informatici anche a rilevanza fiscale, prodotti o ricevuti dalla Regione e dagli altri soggetti di cui all'articolo 19, comma 5, lettera a) della legge regionale 24 maggio 2004, n. 11 nonché, mediante apposito accordo, dei documenti informatici prodotti o ricevuti dai soggetti di cui all'articolo 19, comma 5, lettera b) della medesima legge e da altri soggetti pubblici”.

I soggetti indicati al citato articolo 19 sono rispettivamente:

- a) *la Regione, gli enti e gli organismi regionali, le loro associazioni e consorzi, quali le agenzie, le aziende e gli istituti, anche autonomi, nonché gli enti e le aziende del Servizio sanitario regionale, ed inoltre gli organismi di diritto pubblico e le società strumentali partecipate in misura totalitaria o maggioritaria dai soggetti precedenti;*
- b) *gli Enti locali, i loro enti e organismi, le loro associazioni, unioni e consorzi, quali le aziende e gli istituti, anche autonomi, le istituzioni, gli organismi di diritto pubblico e le società strumentali partecipate in misura totalitaria o maggioritaria da tali soggetti, ed inoltre gli istituti di istruzione scolastica e universitaria presenti e operanti nel territorio regionale.*

I soggetti elencati al punto a), ai sensi del comma 3 dell'art. 16 della L.R. 11/2004 sono “obbligati” ad utilizzare le funzioni di archiviazione e conservazione digitale dei documenti informatici svolte dalla Regione Emilia-Romagna. Invece quelli elencati al punto b) hanno la facoltà di utilizzare le funzioni di conservazione svolte dalla Regione Emilia-Romagna.

Riassumendo si può dire che il modello organizzativo definito dalla Regione Emilia-Romagna è che la **Regione Emilia-Romagna stessa svolga le funzioni di archiviazione e conservazione digitale per la Regione e gli altri enti sopracitati, in particolare gli enti e le aziende del Servizio sanitario regionale, nella logica di sviluppo integrato della conservazione digitale dei documenti informatici nel rispetto dei principi di efficacia, efficienza ed economicità.**

Il modello rientra in quanto previsto dall' articolo 34 comma 1 bis del CAD, ma si tratta di un modello rafforzato da una norma di legge regionale ed inserito in una più ampia visione di sistema regionale allargato. Infatti, per garantire risparmi ed efficienza si concentra in un soggetto specializzato una funzione complessa come quella della conservazione degli oggetti digitali.

¹ L'ultima con Legge Regionale 26 novembre 2020 n. 7.

La Regione Emilia-Romagna, ai sensi del citato art. 2 comma 4bis della L.R. 11/2004 può inoltre collaborare con pubbliche amministrazioni interessate di tutto il territorio nazionale.

L'idea progettuale di realizzare centri di conservazione digitale, cioè "strutture dedicate alla conservazione della memoria digitale di più soggetti *Produttori*, dotate di personale archivistico e informatico altamente qualificato" era già presente nel progetto DOCAREA, presentato ed attuato nell'ambito del piano nazionale di e-government su iniziativa e coordinamento della Provincia di Bologna².

All'interno di tale progetto si era infatti maturata l'idea che il complesso delle attività da svolgere, i requisiti giuridici da soddisfare e le competenze professionali necessarie per la corretta conservazione degli *archivi informatici* non fossero alla portata della maggior parte delle pubbliche amministrazioni, richiedendo risorse – finanziarie, umane e strumentali – troppo elevate per ogni singola organizzazione. Di qui la concezione di un polo di conservazione digitale, concepito come archivio unico di concentrazione servente più *Produttori*, che si proponesse di offrire una soluzione condivisa, affidabile e tempestiva al problema della conservazione dei documenti informatici delle pubbliche amministrazioni.

Questa struttura, inizialmente pensata a livello provinciale e denominata Archive Service Center (ASC), già durante lo svolgimento del progetto DOCAREA venne portata, proprio per il livello di complessità e di risorse richieste, ad una dimensione regionale assumendo la denominazione di Polo archivistico regionale dell'Emilia-Romagna (ParER).

Al termine della fase di progettazione nel luglio 2009 il Polo archivistico era stato costituito come struttura operativa presso l'Istituto dei Beni artistici, culturali e naturali della Regione Emilia-Romagna. Ora, a seguito della chiusura di detto Istituto³, tale struttura è ricompresa nella organizzazione interna della Regione Emilia-Romagna.

ParER ha tutte le caratteristiche istituzionali, giuridiche e tecniche indispensabili al corretto svolgimento del proprio ruolo di *archivio* cioè, per utilizzare i termini di **OAIS**, una struttura organizzata di persone e sistemi che accetta la responsabilità di conservare documenti informatici e renderli disponibili ad una **Comunità di riferimento**.

Infatti, la Regione Emilia-Romagna ha dotato ParER di una specifica struttura tecnologica e di un organico con professionalità qualificate, che assommano conoscenze di natura archivistica, informatica, organizzativa e giuridica.

In particolare, in ParER si ritiene fondamentale promuovere l'incontro tra le professionalità archivistiche e informatiche, in quanto la collaborazione tra archivisti e informatici rappresenta, e si rivela sempre più, una risorsa strategica e una condizione, se non sufficiente, sicuramente necessaria per affrontare le sfide poste dalla conservazione digitale.

Le logiche organizzative di ParER e i suoi rapporti con i *Produttori* fanno riferimento come modello concettuale alle risultanze del progetto internazionale sulla conservazione InterPARES e al

² Una scheda sul progetto si trova nella Appendice B di S. Pigliapoco, *La memoria digitale delle amministrazioni pubbliche*, cit., p. 225 - 236

³ Disposta con L.R. 26 novembre 2020 n. 7 "Riordino istituzionale e dell'esercizio delle funzioni regionali nel settore del patrimonio culturale. Abrogazione delle leggi regionali 10 aprile 1995, N. 29 e 1° dicembre 1998 e modifica di leggi regionali".

modello Open Archival Information System (**OAIS**), certificato standard ISO 14721 nel 2003 e successivamente aggiornato nel 2012 (ISO 14721:2012).

Il *Sistema di conservazione* opera secondo modelli organizzativi esplicitamente definiti che garantiscono la sua distinzione logica dal sistema di gestione documentale.

Seguendo quanto indicato dalle **Linee Guida** e sulla base dello stesso modello **OAIS** si possono identificare i seguenti ruoli fondamentali: **Produttore** (o **Ente produttore**, che racchiude i ruoli di *Titolare dell'oggetto della conservazione* e di *produttore dei Pacchetti di Versamento*), **Utente** (o *Utente abilitato*), **Responsabile della conservazione e/o Conservatore**.

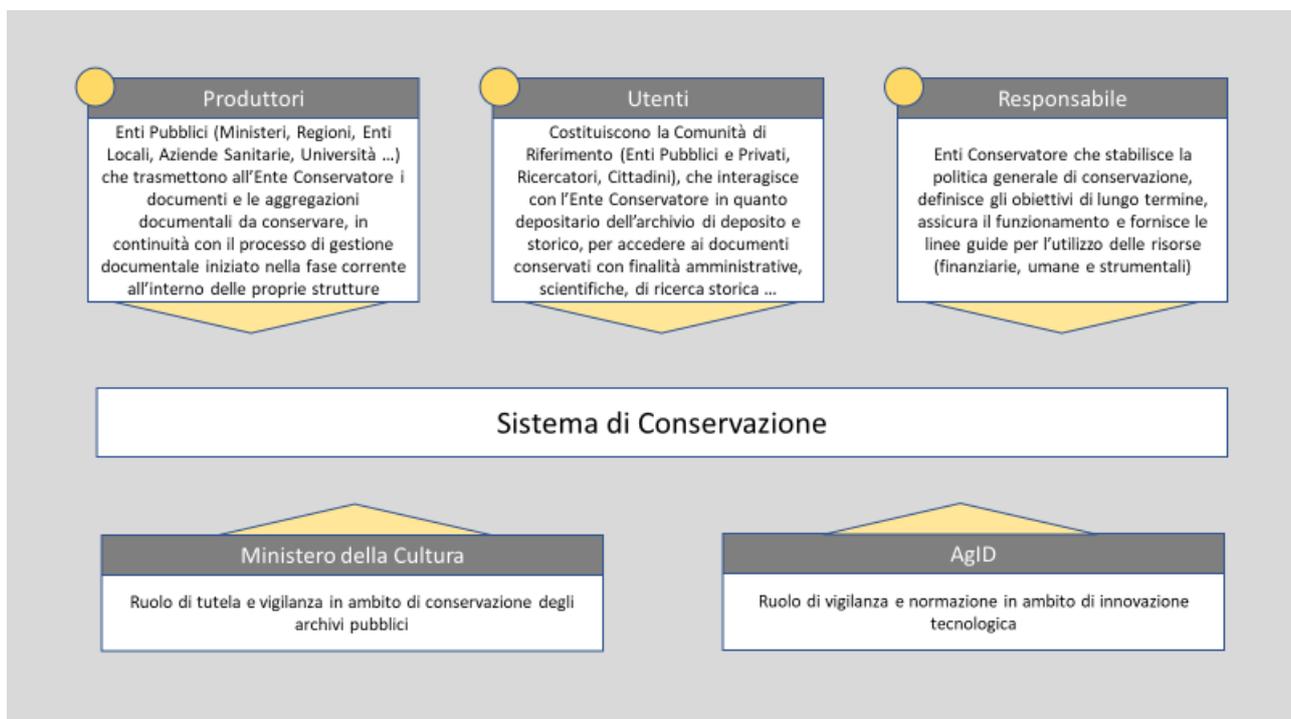


Figura 1 - Sistema e attori

[\[Torna al Sommario\]](#)

4.2 Titolare e Produttore

Le **Linee Guida**, tra i ruoli individuati nel processo di conservazione al primo punto definisce il *titolare dell'oggetto della conservazione*, cioè, in senso archivistico, il soggetto produttore degli oggetti di conservazione, come da definizione contenuta nel Glossario allegato alle **Linee Guida**.

Nello specifico lo si indentifica per la gestione interna della conservazione nella Regione, mentre nel caso di conservazione esterna è il soggetto che affida la conservazione dei propri documenti informatici alla Regione Emilia-Romagna, denominato nell'**Accordo** "Ente Produttore".

Nel ruolo del *Produttore* possono essere definiti tutti gli enti pubblici concordati, che versano i *Documenti informatici* e le *Aggregazioni documentali informatiche* da conservare con gli opportuni *metadati*, in continuità con il processo di gestione documentale iniziato nella fase corrente all'interno delle strutture di produzione.

I rapporti tra la Regione Emilia-Romagna, tramite ParER, e i *Produttori* vengono formalizzati e regolati per mezzo di due documenti fondamentali: l'**Accordo** ed il **Disciplinare tecnico**⁴.

L'**Accordo** regola i rapporti di servizio tra il *Produttore* e ParER, e più precisamente la natura dei servizi offerti, la responsabilità delle parti e le condizioni economiche. Precisa, inoltre, quali sono i servizi offerti da ParER e definisce gli strumenti di consultazione e controllo. Gli attuali **Accordi** prevedono l'erogazione dei servizi di conservazione dei documenti informatici a titolo gratuito per gli enti dell'Emilia-Romagna (Enti locali, Aziende sanitarie, Università) e a titolo oneroso per gli enti di altre regioni.

Il *Produttore*, secondo quanto previsto nell'**Accordo**, si impegna a depositare i *Documenti informatici* e le loro *Aggregazioni documentali informatiche* nei modi e nelle forme definite dalla Regione Emilia-Romagna, tramite ParER, garantendone l'*autenticità* e l'*integrità* nelle fasi di produzione e di archiviazione corrente, effettuata nel rispetto delle norme sulla formazione e sui sistemi di gestione dei documenti informatici. In particolare, garantisce che il trasferimento dei documenti informatici venga realizzato utilizzando formati compatibili con la funzione di conservazione e rispondenti a quanto previsto dalla normativa vigente. Si impegna inoltre a depositare e mantenere aggiornati, nei modi e nelle forme definite tramite ParER dalla Regione Emilia-Romagna, gli strumenti di ricerca e gestione archivistica elaborati a supporto della formazione dei documenti e della tenuta degli *archivi*.

Il *Produttore* mantiene la titolarità e la proprietà dei documenti depositati.

Le **tipologie documentarie** da trasferire, le modalità di versamento e i *metadati* sono concordati e specificati nel **Disciplinare tecnico**.

Il responsabile di riferimento del *Produttore* è di norma il *Responsabile della gestione documentale*, il *Responsabile della conservazione* o il responsabile di specifici sistemi di produzione documentale, quali quelli di produzione di documentazione sanitaria. Se nominato, può essere anche il *Coordinatore della gestione documentale*.

Come indicato nel paragrafo 4.4 delle **Linee Guida** il *Responsabile della gestione documentale* o, se nominato, il *Coordinatore della gestione documentale*, svolge il ruolo di *produttore dei PdV* (Pacchetti di Versamento) e assicura la trasmissione dei pacchetti di versamento al sistema di conservazione in coerenza con le modalità operative definite nel presente manuale di conservazione. Inoltre, verifica il buon esito della operazione di versamento in particolare tramite la verifica della produzione del *rapporto di versamento* da parte del sistema di conservazione.

⁴ Per il dettaglio delle operazioni preliminari all'avvio in produzione di un ente, sia dal punto di vista amministrativo sia tecnico-operativo si vedano le pagine del sito di ParER specificamente dedicate alla attività di conservazione per gli enti; lo schema di Accordo è approvato con apposita delibera della Giunta della REGIONE EMILIA-ROMAGNA e periodicamente aggiornato; i Disciplinari Tecnici specifici sono presenti nel sistema di conservazione per ogni produttore.

Il *Produttore* resta il responsabile del contenuto del *Pacchetto di Versamento* (d'ora in poi SIP) ed è obbligato a trasmetterlo al servizio di conservazione secondo le modalità operative descritte a grandi linee nel presente Manuale e in dettaglio nel ***Disciplinare tecnico*** e nella documentazione tecnica di riferimento.

Nel sistema di conservazione il soggetto che materialmente versa i SIP nel sistema di conservazione è identificato con il termine "Versatore". Normalmente coincide con il *Produttore*, ma in alcuni casi, generalmente per motivi tecnico-organizzativi, quest'ultimo può incaricare un altro Versatore di versare in conservazione i suoi documenti.

Se il Versatore non è un *Produttore* (e in questo caso prende il nome di Versatore esterno), non può versare i SIP direttamente nel sistema - in quanto non può essere titolare di una Struttura versante - ma può versare oggetti per conto del *Produttore* nel sistema di preacquisizione (vedi paragrafo 7.1.1).

Il *Produttore*, nella sua attività di produzione e versamento in conservazione dei SIP, può essere coadiuvato da utenti esterni appartenenti ad altre organizzazioni, definite "Fornitori esterni", che sono normalmente le software house che gestiscono i sistemi di produzione e/o versamento dei documenti.

Il personale dei Fornitori esterni può operare sul Sistema per finalità di supporto tecnico e organizzativo alle attività di conservazione su esplicita autorizzazione del *Produttore*.

Come indicato nel paragrafo 4.3, il *Produttore* ha l'accesso presso la propria sede al *Sistema di conservazione* per la parte relativa alla sua documentazione conservata.

[\[Torna al Sommario\]](#)

4.3 Utente abilitato

In base alla definizione del glossario allegato alle **Linee Guida** si indentifica come *Utente abilitato* una persona, ente o sistema che interagisce con i servizi di un sistema per la conservazione dei *Documenti informatici* al fine di fruire delle informazioni di interesse.

L'*Utente* richiede al *Sistema di conservazione* l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge. Il *Sistema di conservazione* permette ai soggetti autorizzati l'accesso diretto, anche da remoto, ai *Documenti informatici* conservati e consente la produzione di un *Pacchetto di Distribuzione* direttamente acquisibile dai soggetti autorizzati.

In termini **OAIS** la comunità degli *Utenti* può essere definita come **Comunità di riferimento**.

Nel ruolo dell'*Utente* si possono definire al momento solo specifici soggetti abilitati dei *Produttori*, in particolare gli operatori indicati dal *Produttore* che possono accedere esclusivamente ai documenti versati dal *Produttore* stesso o solo ad alcuni di essi secondo le regole di visibilità e di accesso concordate tra ParER e il *Produttore*

L'abilitazione e l'autenticazione di tali operatori avviene in base alle procedure di gestione utenze indicate nel *Piano della sicurezza del sistema di conservazione* e nel rispetto delle misure di

sicurezza previste negli articoli da 31 a 36 del D.lgs. 30 giugno 2003, n. 196, in particolare di quelle indicate all'art. 34 comma 1 e dal Disciplinare tecnico in materia di misure minime di sicurezza di cui all'Allegato B del medesimo decreto.

In prospettiva si possono definire *Utenti* potenzialmente tutti coloro che potranno interagire con ParER, quale conservatore e custode di archivi di deposito e storici, per accedere ai documenti conservati per finalità amministrative, scientifiche e di ricerca storica in relazione alle **tipologie documentarie** conservate e nel rispetto delle normative vigenti in materia di tutela dei beni culturali e di tutela dei dati personali.

[\[Torna al Sommario\]](#)

4.4 Responsabile della conservazione

In base alla normativa vigente il *Responsabile della conservazione* per le pubbliche amministrazioni è identificato con un dirigente o un funzionario formalmente designato e può identificarsi con il *Responsabile della gestione documentale* o, se nominato, con il *Coordinatore della gestione documentale*.

La Regione Emilia-Romagna con Determinazione dirigenziale n. 24766 del 30 dicembre 2021 del Direttore Generale della Direzione Generale Risorse, Europa, innovazioni e istituzioni ha individuato il Responsabile della Conservazione all'interno del Servizio Polo Archivistico e gestione documentale.

A seguito delle successive variazioni organizzative, il ruolo è ora interno all'Area Polo archivistico e gestione documentale del Settore Innovazione Digitale, dati, tecnologie e Polo archivistico della Direzione Generale Risorse, Europa, innovazioni e istituzioni che ha funzioni di Direzione Generale trasversale, finalizzata alla programmazione, organizzazione e gestione di funzioni, processi e servizi di supporto e integrazione dei servizi necessari al funzionamento dell'Ente Regione.

Con determinazione n. 24946 del 20/12/2022 è stata istituita una specifica posizione di Elevata Qualificazione Q0001725 "Responsabile della Conservazione e dell'archivio storico" che svolge la funzione di Responsabile della Conservazione per i documenti informatici della Regione Emilia-Romagna.

I compiti di tale responsabile oltre a quanto previsto dalle Linee Guida sono i seguenti:

- Svolge la funzione di Responsabile della Conservazione per i documenti informatici della Regione Emilia-Romagna;
- Monitora il processo di conservazione dei documenti e delle aggregazioni informatiche dell'Amministrazione regionale;
- Gestisce l'archivio di deposito, predisponendo e monitorando i piani di trasferimento dei dati e dei documenti da e verso altri depositi digitali e i piani di informatizzazione dei documenti e degli archivi cartacei della Regione Emilia-Romagna;
- Gestisce l'Archivio storico della Regione Emilia-Romagna di San Giorgio di Piano assicurando il servizio di accesso ai documenti conservati da parte degli utenti esterni;
- Promuove la redazione di strumenti di corredo di tipo archivistico finalizzati all'accesso di natura storico-culturale e propone nuove funzionalità del sistema di conservazione per i medesimi fini;
- Presidia i rapporti con le strutture del Ministero della Cultura per quanto di competenza gestendo le procedure di scarto dei documenti della Regione Emilia-Romagna;
- Fornisce, relativamente all'ambito di competenza, assistenza specialistica di 2° livello, presidia la gestione tecnica dei contratti monitorando i livelli di servizio e promuove valutazioni sull'impatto della propria attività.

4.5 Conservatore

Il modello organizzativo precedentemente descritto al paragrafo 4.1, ai sensi dell'articolo 34, comma 1 bis, lettera b) del CAD, prevede che il titolare o soggetto produttore affidi la conservazione e il processo di conservazione ad un soggetto conservatore esterno specificamente individuato nella Regione Emilia-Romagna.

La responsabilità del Sistema di conservazione e del servizio di conservazione come soggetto che svolge attività di conservazione è in capo alla Regione Emilia-Romagna, che individua al suo interno nel Polo Archivistico Regionale (ParER) lo specifico soggetto conservatore articolato come descritto nel capitolo 5 nell'ambito delle strutture organizzative regionali.

Il ruolo di ParER come responsabile del servizio di conservazione e del *Sistema di conservazione* va inquadrato alla luce dell'art. 2 della L.R. 11/2004, ossia nel contesto di un più generale impegno, da parte della Regione Emilia-Romagna – nel rispetto delle competenze dello Stato e di concerto con il sistema degli Enti locali – per assicurare a cittadini, imprese ed enti condizioni di sviluppo delle loro attività e relazioni, promuovendo le potenzialità delle tecnologie informatiche nella prestazione di servizi e nell'accessibilità e scambio di dati. In particolare, la Regione persegue lo sviluppo delle reti strumentali, organizzative ed operative e lo sviluppo integrato dei servizi attivi sulla rete della pubblica amministrazione attraverso la collaborazione con le amministrazioni periferiche dello Stato, il sistema delle autonomie locali e, più in generale, tutti i soggetti pubblici e privati e le organizzazioni sociali operanti sul territorio.

Nello specifico, la Regione, anche in collaborazione con le altre pubbliche amministrazioni interessate, favorisce lo sviluppo integrato della *conservazione dei Documenti informatici* e, nel rispetto dei principi di efficacia, efficienza ed economicità, svolge le funzioni di archiviazione e *conservazione digitale dei Documenti informatici*.

In quanto soggetto responsabile la Regione Emilia-Romagna si occupa delle politiche complessive del *Sistema di conservazione* e ne determina l'ambito di sviluppo e le competenze. A tal fine, in coerenza con **OAIS**, provvede alla pianificazione strategica, alla individuazione ed erogazione dei finanziamenti, alla revisione periodica dei risultati conseguiti e ad ogni altra attività gestionale mirata a coordinare lo sviluppo del sistema. Non risulta invece coinvolta nelle operazioni quotidiane di amministrazione del sistema che sono totalmente a carico del soggetto incaricato della sua gestione, cioè il Settore Innovazione Digitale, Dati, Tecnologie e Polo Archivistico (SID), in particolare l'Area Polo Archivistico e gestione documentale, il cui dirigente è specificamente individuato come Responsabile del servizio di conservazione.

La missione di ParER è essere *l'archivio informatico* della Pubblica Amministrazione in Emilia-Romagna per la conservazione e l'accesso dei *Documenti informatici* e in generale di ogni oggetto digitale a supporto dei processi di innovazione e semplificazione amministrativa, con gli obiettivi di:

- garantire la conservazione, archiviazione e gestione dei *Documenti informatici* e degli altri oggetti digitali;
- erogare servizi di accesso basati sui contenuti digitali conservati;
- fornire supporto, formazione e consulenza ai Produttori per i processi di dematerializzazione.⁵

⁵ Da Relazione sulle attività realizzate per gli anni 2009 – 2012 approvata dalla Delibera di Giunta regionale Emilia-Romagna del 01 ottobre 2012, n. 1428.

Di fatto, quindi (come definito dal testo dell'**Accordo**, art. 3, comma 1), la Regione Emilia-Romagna, tramite ParER, si impegna alla *conservazione* dei documenti trasferiti e ne assume la funzione di *Responsabile del servizio di conservazione* ai sensi della normativa vigente, garantendo il rispetto dei requisiti previsti dalle norme in vigore nel tempo per i sistemi di conservazione, e svolge, tramite la struttura organizzativa e di responsabilità di ParER, l'insieme delle attività in capo al *Responsabile della conservazione* elencate nel paragrafo 4.5 delle **Linee Guida**, in particolare quelle indicate alle lettere a), b), c), d), e), f), g), h), i), j), k).

Il *Responsabile del servizio di conservazione* a cui sono affidate tali attività è individuato nel responsabile dell'Area Polo Archivistico e gestione documentale (ParER) all'interno del Settore "Innovazione digitale, Dati, Tecnologie e Polo archivistico" della Direzione Generale Risorse, Europa, innovazioni e istituzioni. Nello svolgimento di tali attività è coadiuvato dal *Responsabile della funzione archivistica di conservazione*, individuato nel funzionario incaricato della posizione di Elevata Qualificazione Q0001003 "Responsabile della funzione archivistica di Conservazione".

Per la descrizione nel dettaglio della struttura organizzativa e di responsabilità si veda il capitolo 5 e per i dati dei soggetti che nel tempo hanno assunto la responsabilità del *Sistema di conservazione* l'Allegato 2 "Registro dei responsabili".

Nell'Allegato, che verrà mantenuto costantemente aggiornato, sono riportati i dati delle persone fisiche che, in base ai loro ruoli in Regione Emilia-Romagna, nel tempo hanno esercitato la rappresentanza del conservatore tramite specifiche azioni e/o eventuali sottoscrizioni. In particolare, il Responsabile del Servizio di Conservazione ed il Responsabile della Funzione Archivistica di Conservazione a cui sono assegnate le funzioni di sottoscrizione previste nell'ambito del *processo di conservazione* e le funzioni di rappresentanza nei rapporti con il MiC e gli altri enti di vigilanza per quanto di competenza.

In taluni casi l'**Accordo** può prevedere che, per semplificare le attività di avviamento e di gestione ordinaria del servizio di conservazione, il rapporto tra il *Produttore* e il Conservatore sia mediato da un ente, chiamato nel sistema di conservazione "Ente gestore", che, pur non assumendo la responsabilità diretta del processo di conservazione, che resta in capo al conservatore, agisce come facilitatore del processo medesimo, svolgendo attività di gestione (quali configurazioni di sistema, definizione di modalità comuni di versamento, monitoraggio) e coordinamento (gestione delle utenze, formazione, supporto di primo livello) rispetto ad un gruppo definito di *Produttori*.

Il ruolo di Gestore è concordato tramite apposito accordo da una parte con il Conservatore, dall'altra parte con i *Produttori*: il Gestore stipula con il Conservatore un accordo generale, cui gli enti Produttori possono aderire, semplificando notevolmente i processi amministrativi di adesione al servizio, anche se è comunque necessaria la stipula di un accordo formale anche tra *Produttore* e Conservatore, riferito all'accordo generale con il Gestore. Il ruolo di gestore viene normalmente svolto da enti territoriali, che svolgono servizi per gli enti del proprio territorio.

[\[Torna al Sommario\]](#)

4.6 Organismi di tutela e vigilanza

Il Ministero della Cultura (MiC) esercita funzioni di tutela e vigilanza dei sistemi di conservazione degli archivi di enti pubblici o di enti privati dichiarati di interesse storico particolarmente

importante e autorizza le operazioni di *scarto* e trasferimento della documentazione conservata ai sensi del D.Lgs 42/2004⁶.

La tutela e vigilanza sugli archivi di enti pubblici non statali è esercitata dal MiC, tramite le Soprintendenze archivistiche e bibliografiche competenti per territorio.

"Lo spostamento, anche temporaneo dei beni culturali mobili" compresi gli archivi storici e di deposito è soggetto ad autorizzazione della Soprintendenza archivistica (D.lgs 22 gen. 2004, n. 42, art. 21, c. 1, lettera b).

Anche "Il trasferimento ad altre persone giuridiche di complessi organici di documentazione di archivi pubblici, nonché di archivi di privati per i quali sia intervenuta la dichiarazione ai sensi dell'articolo 13", sia che comporti o non comporti uno spostamento, rientra tra gli interventi soggetti ad autorizzazione della Soprintendenza archivistica (D.lgs 22 gen. 2004, n. 42, art.21, c. 1, lettera e).

La disposizione si applica anche:

- all'affidamento a terzi dell'archivio (outsourcing), ai sensi del D.lgs 22 gen. 2004, n. 42, art.21, c. 1, lettera e)
- al trasferimento di archivi informatici ad altri soggetti giuridici, nell'ottica della conservazione permanente sia del documento sia del contesto archivistico⁷.

La Soprintendenza archivistica e bibliografica può, in seguito a preavviso, effettuare ispezioni per accertare lo stato di conservazione e custodia degli archivi e può emettere prescrizioni per la tutela degli archivi.

Secondo quanto disposto dall'art. 44, comma 2 lettera a) del recente regolamento di organizzazione del MiC (DPCM 2 dicembre 2019, n. 169, pubblicato sulla GU n. 16 del 21 gennaio 2020, vigente dal 5 febbraio 2020), il Soprintendente archivistico e bibliografico "svolge, sulla base delle indicazioni e dei programmi definiti dalla competente Direzione generale, attività di tutela dei beni archivistici e librari presenti nell'ambito del territorio di competenza nei confronti di tutti i soggetti pubblici e privati, ivi inclusi i soggetti di cui all'articolo 44-bis del Codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82," cioè i conservatori esterni.

In aderenza con le funzioni di tutela sopra indicate è stato stipulato un accordo di collaborazione con la Soprintendenza archivistica e Bibliografica dell'Emilia-Romagna, valido fino al 31 dicembre 2033 che prevede tra i punti più qualificanti:

- la semplificazione delle procedure di autorizzazione al trasferimento mediante l'approvazione preventiva dello schema di **Accordo**;
- l'agevolazione dell'attività ispettiva;
- il supporto e consulenza ai *Produttori*.

In particolare, la Soprintendenza archivistica per l'Emilia-Romagna (ora Soprintendenza Archivistica e Bibliografica dell'Emilia-Romagna) svolge un ruolo di vigilanza del *Sistema di conservazione* per verificare che il *processo di conservazione* avvenga in modo conforme alla normativa e ai principi di corretta e ininterrotta custodia, senza però accedere a informazioni personali / sensibili contenute nei documenti o nel sistema.

In base a tale accordi e secondo quanto indicato nell'**Accordo**, ParER consente alla Soprintendenza archivistica e bibliografica dell'Emilia-Romagna l'accesso ai propri sistemi per rendere possibile e operativo lo svolgimento della funzione di vigilanza e tutela prevista dalla

⁶ Si fa riferimento in particolare agli art. 4, 10, 18 e 21 del citato Decreto legislativo. Il mantenimento delle competenze del MiC in materia di tutela dei sistemi di conservazione degli archivi pubblici è ribadito in diversi paragrafi delle **Linee Guida**, in particolare i paragrafi 4.3 e 3.8

⁷ Dal sito della Soprintendenza archivistica per l'Emilia-Romagna, [Soprintendenza archivistica e bibliografica dell'Emilia-Romagna: Spostamento e trasferimento \(cultura.gov.it\)](http://www.soprintendenzaarchivisticae bibliografica.emilia-romagna.it)

legge ed effettuare le opportune verifiche sul corretto svolgimento dell'attività di *conservazione*, in particolare lo svolgimento dell'attività ispettiva, finalizzata ad accertare lo stato di conservazione e di custodia degli archivi, ai sensi e nel rispetto di quanto previsto dall'articolo 19 del D.lgs. n. 42/2004, con *"modalità concordate che consentano lo svolgimento e la documentazione di tale attività in modalità interamente digitali all'interno del sistema di conservazione sviluppato dalla Regione Emilia-Romagna"*.

La profilazione dell'utente Soprintendente non consente l'accesso ai contenuti dei documenti conservati e ai dati personali / sensibili presenti nei documenti e nei metadati.

Bisogna ricordare che, ai sensi del DPR del 1° novembre 1973 n. 690, le attribuzioni degli organi centrali e periferici dello Stato in materia di ordinamento, tutela, vigilanza, conservazione, custodia e manutenzione del patrimonio storico artistico e popolare sono esercitate, per il rispettivo territorio, dalle province autonome di Trento e di Bolzano. Per la provincia di Trento tali attribuzioni riguardano anche gli archivi e i documenti della provincia, dei suoi enti funzionali, dei comuni e degli altri enti locali, degli altri enti pubblici per le materie di competenza della provincia, nonché gli archivi e i documenti dei privati.

Il servizio di conservazione agli Enti Produttori viene erogato in base al *Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici* pubblicato da AgID nel giugno 2021 ed aggiornato il 17 dicembre 2021. AgID stesso può esercitare le funzioni di vigilanza previste in detto Regolamento o da altra normativa vigente.

La disciplina per la vigilanza e per l'esercizio del potere sanzionatorio previsto all'art. 32-bis del CAD da parte di AgID è oggetto del "Regolamento recante le modalità per la vigilanza ai sensi dell'art. 14-bis comma 2, lett. i) e per l'esercizio del potere sanzionatorio ai sensi dell'art. 32-bis del d. lgs. 7 marzo 2005, n. 82 e successive modificazioni"

[\[Torna al Sommario\]](#)

5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

La Regione Emilia-Romagna in applicazione della Delibera di Giunta n. 324 del 7 marzo 2022 che ha approvato la nuova *"Disciplina organica in materia di organizzazione dell'Ente e gestione del personale"* dall' 1/4/2022 è articolata a livello di macro-organizzazione interna in Direzioni Generali e Settori. Al loro interno, tali strutture organizzative possono essere articolate in:

- a) Posizioni di livello dirigenziale, definite Aree di lavoro dirigenziali;
- b) Posizioni di livello non dirigenziale, definite Posizioni Organizzative⁸.

La Direzione generale è l'unità organizzativa di massima dimensione dell'Ente che può articolarsi in Settori, che a loro volta possono ricomprendere al loro interno Aree di lavoro assegnate a responsabilità dirigenziali e Posizioni Organizzative, secondo raggruppamenti di competenza adeguati all'attività che svolgono.

Al Settore sono assegnate funzioni e attività caratterizzate da elementi di omogeneità con l'obiettivo di perseguire livelli ottimali di efficacia ed efficienza.

Nello specifico, con la successiva Delibera di Giunta n. 325 del 7 marzo 2022 a partire dall'1/4/2022 la Regione Emilia-Romagna ha individuato all'interno della *Direzione Generale Risorse, Europa, innovazioni e istituzioni* il Settore Innovazione digitale, dati, tecnologia e polo archivistico come settore di riferimento per il Polo archivistico (ParER), ponendo nella specifica Declaratoria tra le responsabilità del Settore la progettazione, sviluppo e manutenzione del servizio di conservazione **in qualità di Polo Archivistico Regionale (ParER)** e la cura dello svolgimento dei processi di conservazione e di riversamento sostitutivo dei documenti informatici della Regione e degli Enti in accordo, raccordandosi con analoghe iniziative a livello nazionale ed europeo.

La *Direzione Generale Risorse, Europa, innovazioni e istituzioni*, ha un organigramma riportato nell'Allegato 1 alla citata Delibera di Giunta n. 325 del 07/03/2022.

Nella figura seguente si riporta tale organigramma evidenziando il Settore Innovazione digitale, dati, tecnologia e polo archivistico.

⁸ A seguito della Delibera di Giunta n. 474 del 27/03/2023 le Posizioni Organizzative dal 1° aprile 2023 sono state sostituite da Posizioni di Elevata Qualificazione.



Figura 2 - Organizzazione della DGREI

All'interno del Settore Innovazione digitale, dati, tecnologia e polo archivistico si individuano, a seguito della Determina n. 20935 del 2 novembre 2022, tre strutture organizzative dirigenziali a livello di Area cui sono state attribuite diverse competenze, tra le quali la responsabilità dello svolgimento del *processo di conservazione* dei *Documenti informatici* della Regione e degli altri enti in accordo, e la cura delle modalità di trasferimento, *accesso* e fruizione del patrimonio documentario e informativo conservato.

Si tratta in particolare dell'Area Polo archivistico e gestione documentale, coadiuvata dall'Area Infrastrutture e Sicurezza per la cura dell'evoluzione tecnologica, della sicurezza e l'aggiornamento o la **migrazione** del *Sistema di conservazione* e dall'Area Sviluppo Applicazioni, che si occupa dello sviluppo e manutenzione del Sistema di conservazione.

[\[Torna al Sommario\]](#)

5.2 Struttura organizzativa

All'interno del Settore "Innovazione digitale, Dati, Tecnologie e Polo archivistico", come descritto al paragrafo precedente ed in riferimento alla Figura 2, si situano tre strutture dirigenziali a livello di Area, che collaborano nell'ambito della gestione del sistema di conservazione e di erogazione del Servizio di conservazione:

- Area Polo archivistico e gestione documentale;
- Area Infrastrutture e sicurezza;
- Area Sviluppo Applicazioni.



Le attività che seguono, gestite dalle tre Aree del Settore di cui sopra, enunciate all'interno della Declaratoria definita con Determina Dirigenziale n. 20935 del 02/11/2022 del Direttore della *Direzione Generale Risorse, Europa, innovazioni e istituzioni*, sono svolte anche in relazione al Servizio di Conservazione.

In particolare, in una prospettiva di promozione della dematerializzazione e della conservazione digitale, l'Area Polo archivistico e gestione documentale, come da declaratoria definita con la Determina Dirigenziale n. 20935 del 02/11/2022 del Direttore della *Direzione Generale Risorse, Europa, innovazioni e istituzioni*, svolge le seguenti attività:

- gestisce ed eroga i servizi per il trattamento e la trasmissione tra Pubbliche Amministrazioni dei documenti informatici e multimediali per la Regione e gli Enti in accordo;
- assicura il mantenimento dei requisiti e delle certificazioni necessarie per ottenere e mantenere le qualificazioni per poter erogare i servizi di conservazione digitale alle Pubbliche Amministrazioni;
- promuove e realizza interventi finalizzati ad assicurare l'integrazione tra i sistemi informativi verticali e i sistemi di gestione della documentazione con il sistema di conservazione;
- è responsabile della gestione documentale dell'Ente, cura l'aggiornamento e la manutenzione del Titolare e del Manuale di gestione, la gestione e l'evoluzione dei sistemi di protocollo e degli atti amministrativi in coerenza con gli obiettivi di innovazione digitale ed organizzativa dell'Amministrazione;
- svolge l'attività di gestione delle funzioni di archivio di deposito e storico della Regione a S. Giorgio di Piano;
- cura le relazioni con i livelli interregionali, nazionali ed internazionali sulle materie di competenze, partecipando ad iniziative e gruppi di lavoro;
- partecipa all'analisi dei costi dei servizi IT e alla pianificazione del budget, contribuisce alla stesura dei capitolati di gara per l'acquisizione di beni e servizi IT di competenza, contribuisce alla stesura dei documenti di programmazione e ne monitora l'attuazione,

formula proposte per progetti di innovazione, coordina personale e risorse coinvolte nei progetti affidati anche su ambiti trasversali.

L'Area Infrastrutture e Sicurezza, come da declaratoria definita con la Determina Dirigenziale n. 20935 del 02/11/2022 del Direttore della *Direzione Generale Risorse, Europa, innovazioni e istituzioni*, svolge le seguenti attività anche in relazione al Servizio di Conservazione:

- Individua soluzioni infrastrutturali a supporto dei servizi IT che ne garantiscano la disponibilità, la performance e la sicurezza nel contesto dell'assetto organizzativo dell'Ente, supportandone le sue evoluzioni in coerenza con gli obiettivi indicati negli strumenti di programmazione;
- Presidia le attività di progettazione, realizzazione e sviluppo di tutte le infrastrutture informatiche e telematiche a supporto dei servizi IT erogati tramite i datacenter regionali, anche in cloud pubblico e privato;
- Definisce gli standard tecnologici e architetture dell'infrastruttura IT e delle architetture applicative garantendo l'operatività dei servizi IT, presidiando il monitoraggio dei livelli di servizio e gestendo il processo di presa in carico e rilascio in produzione di nuovi servizi applicativi;
- Contribuisce alla definizione e redazione delle linee guida del sistema informativo regionale, dei disciplinari tecnici e dei modelli di convenzionamento per Istituti ed Agenzie dell'Amministrazione regionale promuovendo il modello di Cloud Service Providing;
- Collabora con la struttura competente in materia di Patrimonio e Logistica al presidio e coordinamento delle attività di sviluppo e gestione della logistica e dell'impiantistica a servizio delle attrezzature informatiche e telematiche, all'interno dei datacenter regionali e presso le sedi regionali nel rispetto delle norme di protezione dei dati personali, dell'efficienza energetica ed in generale della resilienza delle componenti coinvolte;
- Presidia e coordina i processi e le attività finalizzate a garantire l'integrazione infrastrutturale ed applicativa delle soluzioni software e hardware sia nei datacenter regionali che nelle soluzioni cloud (cloud ibrido), l'integrità dei dati ed il corretto dispiegamento delle soluzioni e processi di continuità operativa (business continuity e disaster recovery);
- Presidia e coordina le attività di progettazione e sviluppo dell'infrastruttura di rete locale, geografica e di datacenter realizzando la ridondanza dei collegamenti delle sedi, dei datacenter regionali e promuovendo soluzioni per la connettività remota e soluzioni VPN e di virtualizzazione della rete;
- Gestisce e sviluppa l'infrastruttura tecnica di rilevazione presenze dei dipendenti regionali e i sistemi di monitoraggio e controllo, anche tramite videosorveglianza attiva e passiva dei locali regionali in collaborazione con la struttura competente in materia di Patrimonio e Logistica;
- Definisce le policy di gestione della sicurezza delle informazioni assicurando l'adeguamento delle infrastrutture e le necessarie integrazioni nel rispetto delle vigenti normative; progetta e coordina il sistema di valutazione dei rischi in materia di sicurezza e cybersecurity; presidia i processi di certificazione qualità nelle aree di competenza;
- Formula proposte per la definizione dei livelli di servizio IT, individua soluzioni per problemi e incidenti che coinvolgono le infrastrutture tecnologiche, organizza servizi di assistenza specialistica all'utenza;
- Partecipa all'analisi dei costi dei servizi IT e alla pianificazione del budget, contribuisce alla stesura dei capitolati di gara per l'acquisizione di beni e servizi IT di competenza, contribuisce alla stesura dei documenti di programmazione e ne monitora l'attuazione,

formula proposte per progetti di innovazione, coordina personale e risorse coinvolte nei progetti affidati anche su ambiti trasversali.

L'Area Sviluppo Applicazioni, come da declaratoria definita con la Determina Dirigenziale n. 20935 del 02/11/2022 del Direttore della *Direzione Generale Risorse, Europa, innovazioni e istituzioni*, svolge le seguenti attività:

- Coordina e presidia tutte le attività per la realizzazione, gestione ed evoluzione delle piattaforme applicative di competenza del Settore assicurando il raccordo con l'utenza finale per la definizione dei requisiti funzionali, lo svolgimento dei test ed il rilascio in produzione nel rispetto dei livelli di qualità, usabilità e sicurezza previsti dalle policy adottate
- Sostiene l'assetto organizzativo dell'Ente e il raggiungimento delle finalità pubbliche individuate nei documenti di programmazione promuovendo interventi di razionalizzazione o innovazione sugli applicativi gestiti per l'incremento dei livelli di digitalizzazione e il miglioramento della qualità dei servizi anche attraverso la reingegnerizzazione dei processi e l'integrazione di nuove tecnologie
- Realizza, gestisce e garantisce la manutenzione della piattaforma tecnologica del sistema di conservazione digitale Polo Archivistico regionale;
- Promuove e realizza interventi finalizzati ad assicurare l'integrazione tra i sistemi informativi verticali e i sistemi di gestione della documentazione con il sistema di conservazione;
- Svolge le funzioni di Registration Authority Locale (RAL) per il rilascio dei certificati di firma digitale e coordina le attività degli operatori regionali addetti alle procedure di identificazione, registrazione dei titolari nonché, per quanto di competenza, di manutenzione dei certificati digitali emessi;
- Formula proposte per la definizione dei livelli di servizio IT, individua soluzioni per problemi e incidenti che coinvolgono i servizi applicativi, organizza servizi di assistenza specialistica all'utenza;
- Cura le relazioni con i livelli interregionali, nazionali ed internazionali sulle materie di competenze;
- Partecipa all'analisi dei costi dei servizi IT e alla pianificazione del budget, contribuisce alla stesura dei capitolati di gara per l'acquisizione di beni e servizi IT di competenza, contribuisce alla stesura dei documenti di programmazione e ne monitora l'attuazione, formula proposte per progetti di innovazione, coordina personale e risorse coinvolte nei progetti affidati anche su ambiti trasversali.

Inoltre, all'interno del citato Settore, struttura organizzativa della Regione Emilia-Romagna, si collocano le responsabilità relative al Servizio di Conservazione di seguito dettagliate.

All'interno dell'Area Polo Archivistico e Gestione documentale:

Responsabile del Servizio di Conservazione: dirigente con responsabilità dei procedimenti / processi / progetti di ParER. È il dirigente responsabile dell'Area Polo archivistico e gestione documentale. Rientrano tra le sue mansioni e responsabilità, come da specifica indicazione dell'appendice all'allegato A del Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici pubblicato da AgID:

- definizione e attuazione delle politiche complessive del sistema di conservazione nonché del governo della gestione del sistema di conservazione;

- definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente;
- corretta erogazione del servizio di conservazione all'ente produttore;
- gestione degli accordi, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.

In assenza del dirigente d'Area la figura di Responsabile del Servizio di Conservazione è svolta dal dirigente responsabile del Settore Innovazione digitale, dati, tecnologia e polo archivistico

Responsabile della funzione archivistica di conservazione: è il funzionario titolare della posizione di Elevata Qualificazione responsabile del presidio della funzione archivistica di conservazione ed opera a stretto contatto con il Responsabile del Servizio di Conservazione. Rientrano tra le sue mansioni e responsabilità, quanto indicato nell'appendice all'allegato A del Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici pubblicato da AgID:

- definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato;
- definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici;
- monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione;
- collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali (ora Ministero della Cultura) per quanto di competenza.

Responsabile dei Servizi di Conservazione Digitale: è il funzionario titolare della posizione di Elevata Qualificazione responsabile della gestione operativa dei servizi di conservazione ed opera a stretto contatto con il Responsabile del Servizio di Conservazione. Rientrano tra le sue mansioni e responsabilità:

- coordinamento delle attività operative a supporto del processo di conservazione;
- coordinamento delle attività delle risorse della funzione, in modo tale da garantire adeguati livelli di servizio agli Enti che conservano presso ParER;
- gestione il ciclo di pianificazione, esecuzione e controllo delle attività,
- definizione dei processi e delle procedure operative del servizio, in coerenza con le linee guida emesse dalla Funzione Archivistica di Conservazione;
- nel caso di nuovi sviluppi applicativi, definizione dei requisiti di massima del servizio e verifica dei documenti prodotti dall'Area Sviluppo Applicazioni;

Inoltre, come Referente per la Qualità:

- si occupa della gestione delle relazioni con gli Enti Produttori, Fornitori per ciò che attiene alle problematiche della Qualità;
- monitora e misura il livello di soddisfazione degli Enti Produttori;
- controlla i livelli di Qualità nell'ambito dei processi di conservazione;
- si occupa dell'analisi dei reclami degli Enti Produttori per la gestione di azioni correttive opportune da parte del responsabile competente.

All'interno della funzione operano diversi archivisti, che si occupano di analizzare le problematiche specifiche delle diverse tipologie documentarie, e in particolare la modellizzazione dei *pacchetti informativi*, di avviare in conservazione nuovi Enti e di estenderne l'uso del servizio

a nuove strutture e a nuove tipologie documentarie, di formare gli utenti all'utilizzo del servizio, di verificare l'andamento dei versamenti, di supportare gli utenti nella pratica quotidiana del servizio. A questo scopo parte del personale a turno opera come help desk per gli utenti, sia nelle attività preliminari all'avvio del servizio, che nelle attività di esercizio del servizio stesso; va sottolineato che l'help desk non è una struttura separata, ma un insieme di attività svolte da archivisti a supporto degli utenti, utilizzando procedure e strumenti standardizzati, formalizzati e condivisi con gli altri operatori dell'help desk. Gli archivisti infine contribuiscono allo sviluppo delle nuove applicazioni partecipando quando necessario all'analisi funzionale e ai test preliminari al passaggio in produzione.

All'interno delle Area di Infrastrutture e Sicurezza:

In questa area sono presenti le figure di **Responsabile Sicurezza Informatica e Responsabile Infrastruttura Tecnologica e Architetture Applicative** che includono tutti gli elementi relativi ai servizi di conservazione, come la sicurezza e la gestione delle infrastrutture a sostegno dell'erogazione, all'interno delle loro responsabilità come dichiarato nella Declaratoria.

All'interno dell'Area di Sviluppo Applicativo:

In questa area è presente la figura di **Responsabile Sistemi di conservazione**, come **Responsabile dello Sviluppo del Sistema di Conservazione**, che gestisce tutti gli aspetti di sviluppo e manutenzione del Sistema di Conservazione.

Il Responsabile del trattamento dei dati personali e il Responsabile della Protezione dei Dati (DPO) sono identificati nel capitolo 10 del presente Manuale.

Nella tabella successiva è riportata la mappatura tra le attività principali del Servizio e le strutture interessate. Per la rappresentazione grafica è stato utilizzato lo schema RACI:

- **R**, Responsible: ha il compito di svolgere una particolare attività;
- **A**, Accountable: è responsabile dei risultati dell'attività o ha un ruolo di approvatore;
- **C**, Consulted: è coinvolto attivamente nel processo indirizzando le azioni da compiere o le decisioni da prendere;
- **I**, Informed: è mantenuto informato sulle azioni da compiere o sulle decisioni prese. Il soggetto informato non può influenzare il risultato.

Attività	Resp. Servizio di conservazione	Ref. Sicurezza dei Sistemi	Resp. Funzione Archivistica Conservazione	Resp. Servizi di conservazione Digitale	Ref. Servizi Tecnologici Infrastrutture	Resp. Sistemi di conservazione e	Resp. Tratt. Dati Personali
Gestione degli Accordi	A		C	R			
Attivazione del servizio di conservazione	A		C	R			

Attività	Resp. Servizio di conservazione	Ref. Sicurezza dei Sistemi	Resp. Funzione Archivistica Conservazione	Resp. Servizi di conservazione Digitale	Ref. Servizi Tecnologici Infrastrutture	Resp. Sistemi di conservazione e	Resp. Tratt. Dati Personali
Gestione e monitoraggio del processo di conservazione	A		R	I		C	
Gestione e monitoraggio Infrastruttura	I, C		I	I	A, R	I, C	
Sviluppo, manutenzione e monitoraggio del sistema	I, C		I, C	I	I, C	A, R	
Monitoraggio dei Servizi di conservazione	I		C	R		C	
Verifica di conformità a norme e std di conservazione			A, R		I	I	C
Gestione Sicurezza del sistema	I	A, R			I	I	
Gestione degli incidenti di sicurezza	I	A, R	I	I	C	C	I
Gestione del Cambiamento	A	C	C	C	C	R	
Gestione mal-funzionamenti	A		R	R	R	R	
Rapporti con le Autorità di vigilanza	I		A,R				
Amministrazione Processi di Certificazione	I	I	I	A,R	I	I	
Trattamento dei dati personali	I	I	R	R			A

[\[Torna al Sommario\]](#)

6 OGGETTI SOTTOPOSTI A CONSERVAZIONE

6.1 Oggetti conservati

Il *Sistema di conservazione* gestito da ParER (Sistema), conserva *Documenti informatici*, in particolare documenti amministrativi informatici, con i *metadati* ad essi associati e le loro *Aggregazioni documentali informatiche*, che includono i Fascicoli informatici (Fascicoli). Inoltre, il Sistema gestisce l'organizzazione e la descrizione dei *Documenti informatici* e delle *Aggregazioni documentali informatiche* in **Serie**.

Tale modello riprende quello gerarchico di ordinamento di un *archivio*, illustrato in figura, derivata dallo schema dello standard **ISAD**.

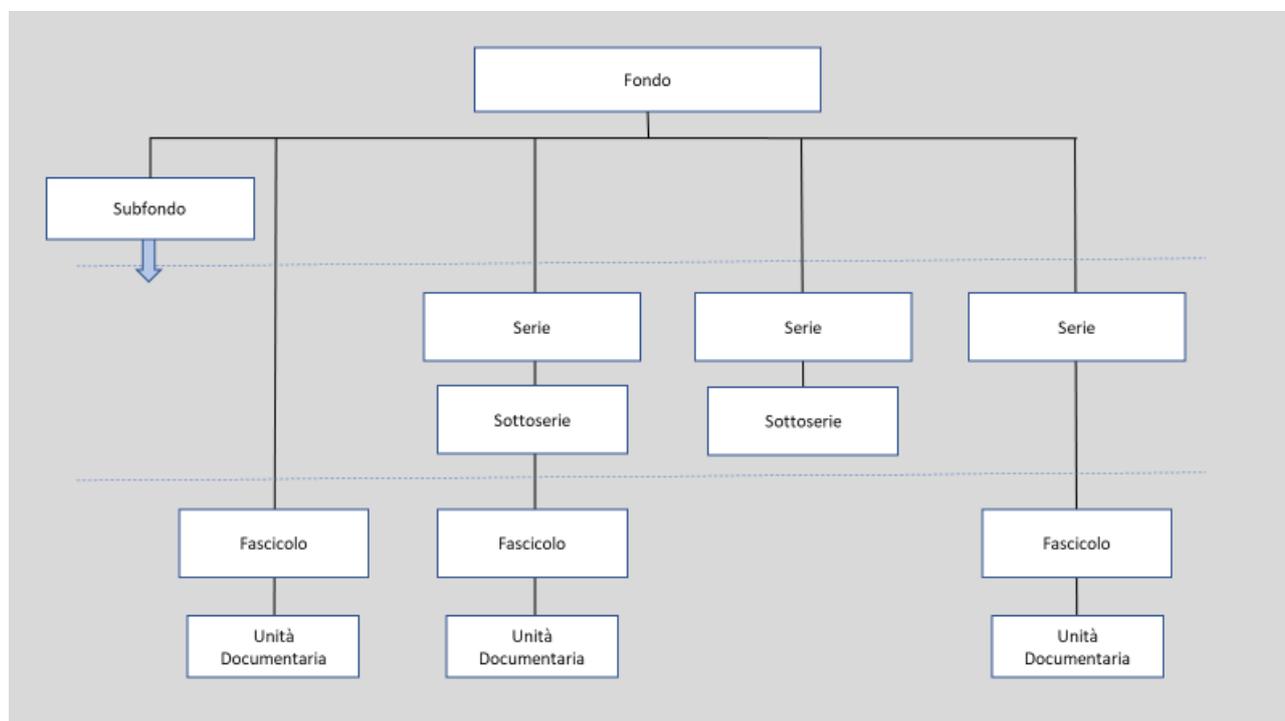


Figura 3 - Modello di ordinamento di archivio derivato da ISAD

I *Documenti informatici* e le loro *Aggregazioni documentali informatiche* (fascicoli) sono trattati nel sistema nella forma di **Unità documentarie** e **Unità archivistiche**, specificamente descritte nel paragrafo 6.1.1, e sono inviati in conservazione sotto forma di *Pacchetti di versamento* (SIP), che contengono sia i documenti che i relativi *metadati*.

Il Sistema gestisce gli oggetti sottoposti a conservazione in *archivi*, articolati in **Strutture** (generalmente, ma non necessariamente, corrispondenti alle Aree Organizzative Omogenee delle Pubbliche Amministrazioni) e distinti per ogni singolo *Produttore*.

Per mantenere anche nel Sistema le informazioni relative alla struttura dell'*archivio* e dei relativi vincoli archivistici, le **Unità documentarie** sono versate corredate di un set di *metadati* di Profilo archivistico che include gli elementi identificativi e descrittivi del Fascicolo, con riferimento alla voce di *classificazione* e l'eventuale articolazione in sottofascicoli. Inoltre, è gestita la presenza

di classificazioni, fascicoli e sotto-fascicoli secondari e collegamenti tra le diverse **Unità archivistiche** e documentarie presenti nel sistema.

Le **Unità archivistiche** e le **Serie** sono versate nel Sistema quando sono complete e dichiarate chiuse, descritte da un set di *metadati* che include obbligatoriamente, oltre alle informazioni di identificazione, *classificazione* e descrizione, anche il tempo di conservazione previsto. Nel caso delle **Serie** la chiusura avviene normalmente a cadenza annuale (o comunque secondo una definizione temporale definita dal *Produttore*) ed è da intendersi come chiusura della partizione periodica della Serie stessa (ad esempio, la partizione annuale della serie delle Determinazioni corrisponde alle determinazioni prodotte in un determinato anno e tale partizione va ad alimentare la relativa serie).

I *Documenti informatici* (**Unità documentarie**), e, in certi casi, i Fascicoli (**Unità archivistiche**) sono suddivisi in **tipologie documentarie** (definite nel sistema "Tipi unità documentarie" e "Tipi fascicolo"), che identificano gruppi documentali omogenei per natura e funzione giuridica, modalità di registrazione o di produzione. Tale suddivisione è funzionale all'individuazione, per ogni singola **tipologia documentaria**, di set di *metadati* standard e di articolazioni o strutture di composizione omogenee. Inoltre, le **tipologie documentarie** in molti casi individuano le **Serie** in cui si articola e organizza la produzione documentale del *Produttore*.

Per le principali **tipologie documentarie**, la Funzione archivistica elabora e pubblica documenti di studio ed analisi (modelli degli AIP e dei SIP), che definiscono per ogni **tipologia documentaria**:

- il set dei *metadati* descrittivi che le caratterizzano, ritenuti essenziali per la corretta conservazione dei documenti e delle aggregazioni documentali informatiche (vedi più avanti paragrafo 6.1.3), in coerenza con quanto stabilito nell'Allegato 5 delle **Linee Guida**;
- la struttura in base a cui sono articolate (vedi più avanti paragrafo 6.1.1).

A titolo esemplificativo, si riportano le principali macrocategorie di **tipologie documentarie** gestite e conservate:

- **Documentazione amministrativa:** documenti inerenti all'attività degli organi consiliari, contratti e accordi, decreti e ordinanze, deliberazioni, determinazioni, documentazione contabile, documenti protocollati, registri, strumenti urbanistici, ecc.;
- **Documentazione sanitaria:** referti e immagini diagnostiche;
- **Documentazione scolastica:** pagelle e registri didattici
- **Documentazione universitaria:** verbali di esame e altri documenti inerenti all'attività didattica;
- **Documenti di conservazione:** Evidenze informatiche prodotte da altri *sistemi di conservazione*.

Benché il Sistema operi primariamente su *Documenti informatici* originali e su Fascicoli informatici, al fine di mantenere la completezza e la consistenza dei fascicoli, e più in generale dell'*archivio* nel suo complesso, nel caso di Fascicoli ibridi è previsto l'invio al Sistema anche delle copie per immagini di originali analogici o dei soli *metadati* relativi a documenti in originale analogico.

Stante la natura eterogenea degli *archivi* conservati da ParER, diverse sono le attività svolte a garanzia non solo della integrità ma anche della fruibilità degli *archivi* stessi nel lungo periodo

per mantenere la loro leggibilità e reperibilità, anche nella prospettiva della futura fruizione come archivi storici.

A tal fine le strategie adottate per la conservazione a cura di ParER prevedono le seguenti azioni:

- definire con precisione la **Comunità di riferimento** di ogni *archivio*, in accordo con i *Produttori*;
- analizzare le caratteristiche archivistiche e tecnologiche dei documenti conservati;
- mantenere attivo un osservatorio tecnologico sulla conservazione ed effettuare sperimentazioni sulle tecnologie disponibili, con particolare riguardo alle tecnologie open source ed ai progetti nazionali e internazionali nell'area della conservazione;
- collaborare attivamente con le autorità istituzionalmente preposte alla definizione del quadro normativo e delle regole operative per la conservazione documentale e con le autorità di sorveglianza.

In ragione dei diversi fattori che influiscono sulla fruibilità degli *archivi* nel lungo periodo, ParER adotta diverse misure per garantire la reperibilità e la *leggibilità* dei documenti conservati negli *archivi*. In particolare per quanto riguarda la reperibilità dei documenti si prevedono appropriate procedure di natura archivistica (creazione di **Serie** e fascicoli, arricchimento di *metadati*, collegamento tra documenti interrelati, ecc.), mentre per quanto riguarda la *leggibilità* si prevedono procedure di manutenzione dei *formati*, che possono variare in ragione della **Comunità di riferimento** e delle caratteristiche archivistiche e tecnologiche dei documenti stessi; p.e. nel caso di studi in standard **DICOM**, che vengono restituiti solo a sistemi **PACS**, non vengono operate trasformazioni di *formato*, mentre nel caso di formati proprietari o deprecati di documenti amministrativi destinati ad avere ampia diffusione, si possono operare attività di trasformazione verso formati standard aperti (p.e. pdf/A); l'adozione di trasformazioni dipende dalla vita utile del documento (p.e. non vengono trasformati documenti che saranno sottoposti a *scarto* nel breve periodo), dagli accordi con il *Produttore* e da considerazioni più generali di natura tecnologica ed archivistica. Quando necessario ParER sviluppa e mantiene nel tempo appositi sistemi di accesso per specifiche **tipologie documentarie**, a garanzia della fruibilità nel lungo periodo.

Gli oggetti sottoposti a conservazione, siano essi *Aggregazioni documentali informatiche*, *Documenti informatici*, o *metadati*, sono trasmessi dal *Produttore*, memorizzati e conservati nel Sistema e distribuiti agli *Utenti* sotto forma di *pacchetti informativi*. Il *pacchetto informativo*, a seconda sia utilizzato per versare, conservare o distribuire gli oggetti sottoposti a conservazione, assume la forma, rispettivamente, di *Pacchetto di versamento* (SIP), *Pacchetto di archiviazione* (AIP) e *Pacchetto di distribuzione* (DIP), descritti rispettivamente nei paragrafi 6.2, 6.3 e 6.4.

Il *pacchetto informativo* è un contenitore astratto che contiene due tipi di informazione: il **Contenuto informativo** (o Content information) e le **Informazioni sulla conservazione** (PDI – Preservation Description Information), la cui correlazione è identificata dalle **Informazioni sull'impacchettamento** (PI – Packaging information). Il *pacchetto informativo*, inoltre, è descritto e può essere ricercato nel Sistema grazie alle **Informazioni descrittive** (Descriptive information).

Una rappresentazione grafica del *pacchetto informativo*, ripresa dal Modello **OAIS**, è riportata in figura.

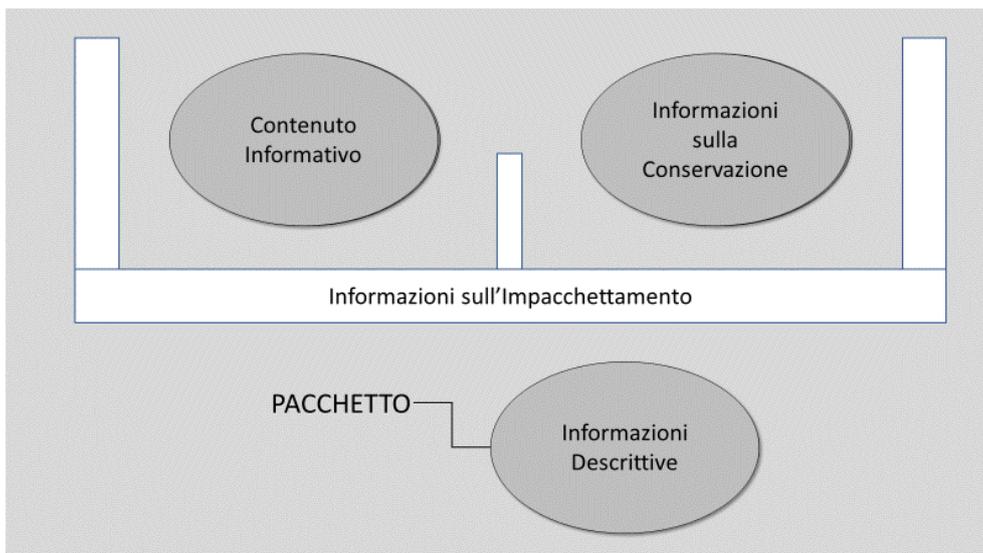


Figura 4 - Pacchetto informativo (da OAIS)

Il **Contenuto informativo** contiene le informazioni che costituiscono l'oggetto originario della conservazione ed è composto da due elementi:

- **Oggetto-dati:** può assumere la forma di sequenza di bit (tipicamente un file), qualora l'oggetto sia digitale, o solo da informazioni (*metadati*), qualora sia un oggetto materiale (ad esempio, un documento analogico);
- **Informazioni sulla rappresentazione:** costituiscono le informazioni necessarie a rendere comprensibile l'**Oggetto-dati** agli *Utenti*. Il caso tipico di **Informazioni sulla rappresentazione** è costituito dalle informazioni relative al *formato* con cui la sequenza di bit è codificata, informazioni che consentono al Sistema di decodificare opportunamente la sequenza di bit per essere correttamente rappresentata e resa intelligibile agli *Utenti* del Sistema.

Le **Informazioni sulla conservazione** sono le informazioni necessarie a conservare il **Contenuto informativo** e garantiscono che lo stesso sia chiaramente identificato e che sia chiarito il contesto in cui è stato creato. Sono costituite da *metadati* che definiscono la provenienza, il contesto, l'identificazione e l'*integrità* del **Contenuto informativo** oggetto della conservazione.

Le **Informazioni sull'impacchettamento** sono informazioni che consentono di mettere in relazione nel Sistema, in modo stabile e persistente, il **Contenuto informativo** con le relative **Informazioni sulla conservazione**.

Le **Informazioni descrittive**, infine, descrivono il *pacchetto informativo* e consentono di ricercarlo nel Sistema. In base alle caratteristiche della tipologia di oggetto contenuto nel Pacchetto, tali informazioni possono essere un sottoinsieme di quelle presenti nel *pacchetto informativo*, possono coincidere o possono anche essere diverse.

[\[Torna al Sommario\]](#)

6.1.1 Unità archivistiche e Unità documentarie

Le **Unità archivistiche** contengono una o più **Unità documentarie**, secondo le logiche di *classificazione* e fascicolazione utilizzate dal *Produttore* per organizzare i documenti prodotti nel proprio *archivio* (vedi figura 4).

L'**Unità documentaria** rappresenta l'unità minima elementare di riferimento di cui è composto un *archivio*, pertanto rappresenta il riferimento principale per la costruzione dei *pacchetti informativi* di cui ai paragrafi 6.2, 6.3 e 6.4.

Con riferimento a quanto indicato nello standard ISO 23081-2, l'**Unità documentaria**, rappresenta la più piccola "unit of records" individuabile e gestibile come una entità singola gestita nel Sistema, anche se al suo interno contiene elementi e **Componenti** come, ad esempio, un messaggio di posta elettronica con i suoi allegati.

All'**Unità documentaria** e agli elementi che la compongono sono associati set di *metadati* che li identificano e li descrivono, secondo le logiche e le articolazioni esposti al paragrafo 6.1.3.

Coerentemente con quanto sopra riportato l'Unità Documentaria è pertanto strutturata su tre livelli: Unità Documentaria, **Documento**, **Componente**, come rappresentato in figura.

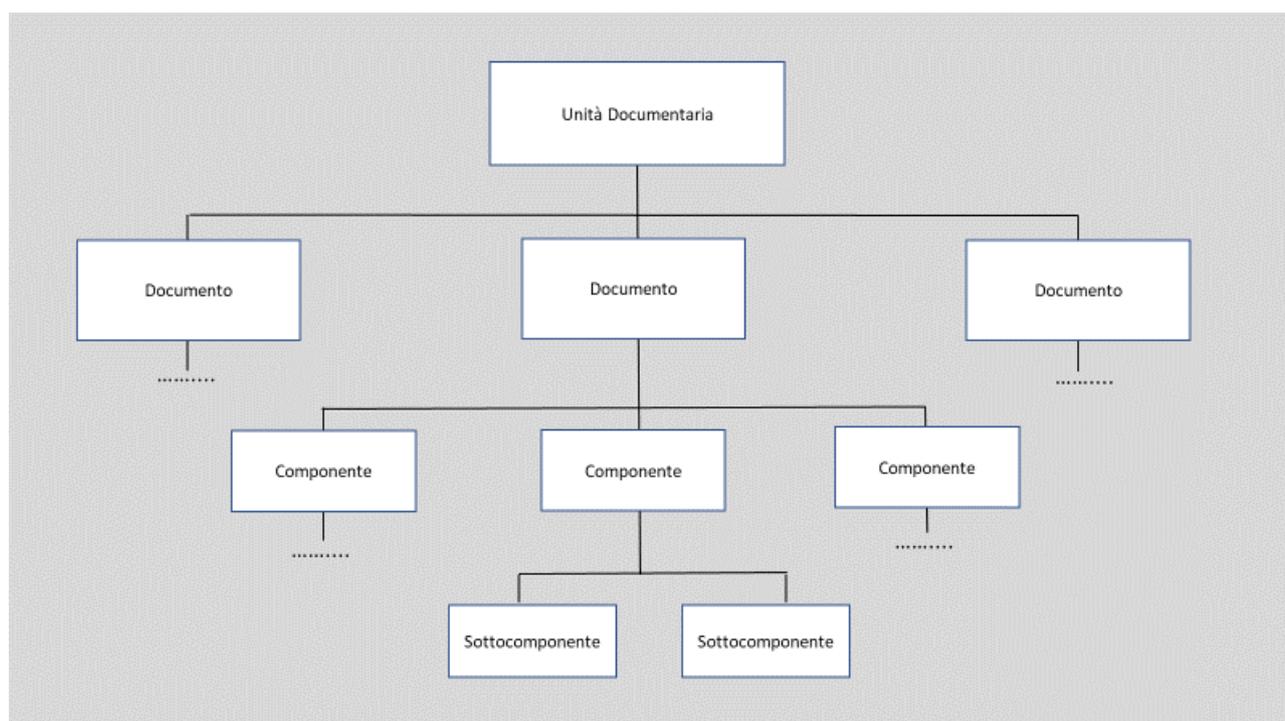


Figura 5 - Struttura dell'Unità documentaria

L'**Unità documentaria** fa sempre riferimento a una specifica **tipologia documentaria** che ne determina oltre ai *metadati* di riferimento anche la struttura, in termini di definizione ed articolazione in **Documenti** e **Componenti** in essa contenuti.

I **Documenti** sono gli elementi dell'**Unità documentaria** e sono identificati in base alla funzione che svolgono nel contesto dell'**Unità documentaria** stessa, ovvero:

- **Documento principale:** è il **Documento** che definisce il contenuto primario dell'**Unità documentaria**. È obbligatorio e quindi deve essere sempre presente;

- **Allegato:** è un **Documento** redatto contestualmente o precedentemente al **Documento principale** ed unito a questo, come parte integrante, per memoria, prova, chiarimento o integrazione di notizie. È facoltativo;
- **Annesso:** è un **Documento**, generalmente prodotto e inserito nell'**Unità documentaria** in un momento successivo rispetto a quello del **Documento principale**, per fornire ulteriori notizie e informazioni a corredo del **Documento principale**. È facoltativo;
- **Annotazione:** può essere costituita da quegli elementi che tradizionalmente in ambiente cartaceo venivano apposti sullo stesso supporto del **Documento principale** come elementi identificativi del **Documento** e del suo iter documentale e che in ambito informatico si sono mutati in **Documenti** associati al **Documento principale** (un tipico esempio di Annotazione è rappresentato dalla segnatura di protocollo). È facoltativa.

I **Componenti** individuano il contenuto del **Documento**, che normalmente è digitale, ovvero costituito da una sequenza di bit, generalmente sotto forma di file, e i relativi *metadati*, tra cui quelli che identificano il *formato*. È possibile, però, che in taluni casi, il **Componente** sia espresso solo da *metadati* e sia quindi privo della sequenza di bit. Tipicamente questo avviene quando l'oggetto della conservazione non è digitale (ad esempio, documenti presenti solo in originale analogico).

Inoltre, esiste una particolare categoria di **Componenti** definiti **Sotto componenti**, che contengono elementi integrativi del **Componente** rappresentati da sequenze di bit distinte da quelle del **Componente** (ad esempio, *marche temporali detached* o *firma detached*). Il **Sotto componente** ha una struttura del tutto simile al **Componente** ed è associato logicamente al **Componente** cui fa riferimento.

[\[Torna al Sommario\]](#)

6.1.2 Formati

Il *Sistema* tratta i formati descritti nell'Allegato 2 alle **Linee guida** e, inoltre, è in grado di trattare, su richiesta del *Produttore*, anche *formati* non compresi nel suddetto elenco, ma che il *Produttore* utilizza nei propri sistemi e che ritiene di dover conservare.

Tutti i formati trattati sono elencati e descritti in un registro interno al Sistema denominato "Registro dei formati" in cui ogni *formato* è corredato da informazioni relative a estensioni e **mimetype**. Inoltre, ogni *formato* è classificato in base alla sua idoneità a essere conservato a lungo termine in riferimento alle indicazioni fornite per la classificazione di formati dal citato Allegato 2 e all'indice di interoperabilità introdotto nel paragrafo 3.2 di detto Allegato. Sulla base di questa suddivisione i *formati* si dividono in:

- **Formati idonei:** sono i *formati* che per le loro caratteristiche di standardizzazione, di apertura, di sicurezza, di portabilità, di *immodificabilità*, di *staticità* e di diffusione sono reputati idonei alla conservazione a lungo termine;
- **Formati gestiti:** sono i *formati* leggibili e accessibili ma potenzialmente soggetti a obsolescenza tecnologica e che, in caso di necessità, possono essere opportunamente migrati in Formati idonei con apposite procedure;

- **Formati deprecati:** sono *formati* ritenuti non idonei per la conservazione a lungo termine e che al contempo non possono essere migrati in Formati idonei, per i quali, quindi, non è possibile assicurare la conservazione a lungo termine.

Con ogni *Produttore* è concordato un elenco di Formati ammessi, che individua i *formati* che il Sistema può accettare dal *Produttore* e che sono previsti per ogni **tipologia documentaria** gestita. L'elenco dei Formati ammessi è riportato (e gestito) nelle funzionalità "Amministrazione strutture versanti" del Sistema ed è aggiornato continuamente in base alle esigenze del *Produttore*

Il Sistema identifica i *formati* al momento della ricezione del SIP (vedi paragrafo 7.2) mediante l'analisi dei **magic number** o del contenuto del file, in modo tale da consentire l'individuazione dello specifico **mimetype**.

L'informazione sul *formato* è parte dei *metadati* dei **Componenti** dell'**Unità documentaria** e costituisce elemento dell'Informazione sulla rappresentazione (vedi paragrafo 6.1).

[\[Torna al Sommario\]](#)

6.1.3 Metadati

I *metadati* gestiti dal Sistema sono individuati in coerenza con la normativa italiana e con gli standard e i modelli internazionali di riferimento. Più in dettaglio sono descritti ed analizzati per specifici oggetti da conservare e specifiche **tipologie documentarie** tramite i modelli di SIP pubblicati sul sito del ParER. In generale il Sistema gestisce i metadati previsti delle **Linee Guida**, con la definizione di uno specifico profilo in relazione in particolare allo schema di metadati indicati nell'allegato 5 in riferimento al documento amministrativo informatico.

I *metadati* gestiti, in base alle funzioni cui assolvono, si dividono nelle seguenti macro classi:

- **Metadati di identificazione:** identificano in modo univoco le **Unità documentarie** e archivistiche. Includono i dati identificativi del *Produttore* e i dati di registrazione originari, nonché gli identificativi specifici di ogni elemento dell'**Unità documentaria (Documenti e Componenti)**;
- **Metadati di struttura:** descrivono la struttura dell'**Unità archivistica o documentaria**, indicando nell'ultimo caso il numero e la tipologia di **Allegati, Annessi e Annotazioni** che la compongono, nonché, per ognuno di essi, il numero e la tipologia dei **Componenti**;
- **Metadati di profilo archivistico:** descrivono il Fascicolo e più in generale la collocazione dell'**Unità documentaria** nel contesto dell'*archivio* del *Produttore*. Ricomprendono anche i *metadati* che collegano l'**Unità documentaria** ad altre **Unità documentarie** conservate nel sistema (Collegamenti);
- **Metadati di profilo generali:** individuano gli elementi descrittivi essenziali comuni alle diverse tipologie di **Unità archivistiche, Unità documentarie** e relativi elementi;
- **Metadati di profilo specifici:** individuano elementi descrittivi ulteriori rispetto a quelli previsti nel profilo generale. Sono definiti per ogni tipologia di **Unità archivistica e documentaria** e per ogni *Produttore*;
- **Metadati di conservazione:** sono tipicamente generati dal Sistema nel corso del *processo di conservazione* e attengono tanto all'analisi e alle verifiche effettuate sugli

oggetti conservati, che alla descrizione delle attività svolte dal Sistema. Tra i Metadati di conservazione rientrano anche i *metadati* associati alle **Unità archivistiche e documentarie** provenienti da altri *sistemi di conservazione* (Metadati specifici di migrazione) e che contengono le informazioni relative al *processo di conservazione* di cui le **Unità archivistiche e documentarie** sono state eventualmente oggetto prima di essere versate nel Sistema.

[\[Torna al Sommario\]](#)

6.2 Pacchetto di versamento (SIP)

I pacchetti di versamento (SIP) sono concordati per struttura e contenuto con il *Produttore* e contengono l'oggetto o gli oggetti da conservare. In base alle specifiche esigenze possono contenere una o più **Unità archivistiche**, una o più **Unità documentarie**, un **Documento** da aggiungere a un'**Unità documentaria** già versata o solo informazioni relative a un'**Unità documentaria** già conservata da aggiornare. Ogni SIP può generare uno o più *Pacchetti di archiviazione* così come più SIP possono costituire un unico *Pacchetto di archiviazione*.

I SIP sono composti dai file dei **Componenti** e dall'**Indice del SIP** (file XML che contiene i *metadati* e la struttura del pacchetto).

Per essere acquisiti e presi in carico dal Sistema, i SIP devono rispettare una determinata struttura dati, nell'ambito della quale viene concordato con il Produttore il contenuto informativo da portare in conservazione. La struttura dati è descritta nelle Specifiche tecniche dei servizi di versamento, mentre le procedure per la trasmissione e l'acquisizione dei SIP sono descritte nel capitolo 7.1.

I modelli di SIP gestiti dal Sistema, descritti in dettaglio nelle Specifiche dei Servizi di Versamento, sono:

- SIP di un'**Unità archivistica**: è il SIP utilizzato per versare le *Unità archivistiche* (Fascicoli). Contiene i *metadati* descrittivi dell'**Unità archivistica** e l'elenco delle **Unità documentarie** in esso contenute. Genera un corrispondente *Pacchetto di archiviazione* relativo all'**Unità archivistica**;
- SIP di un'**Unità documentaria**: contiene un'**Unità documentaria** completa in tutti gli elementi presenti nei sistemi del *Produttore* al momento del versamento. Il versamento di un pacchetto contenente un'**Unità documentaria** genera un corrispondente *Pacchetto di archiviazione*;
- SIP di un **Documento**: è utilizzato per aggiungere un singolo **Documento** e i relativi *metadati* a un'**Unità documentaria** già presente nel Sistema. Il versamento di tale pacchetto genera l'aggiornamento del *Pacchetto di archiviazione* dell'**Unità documentaria** cui il **Documento** viene aggiunto. La necessità di aggiungere un **Documento** a un'**Unità documentaria** già presente si presenta tipicamente in due casi:
 - quando, per numerosità e dimensioni, è preferibile suddividere il versamento di un'**Unità documentaria** in più parti;
 - qualora uno o più **Documenti** appartenenti a un'**Unità documentaria** siano disponibili sul sistema del *Produttore* solo in un momento successivo a quello in cui l'**Unità documentaria** di cui fanno parte è stata versata nel Sistema;

- SIP di Aggiornamento metadati: è utilizzato per versare nel Sistema esclusivamente informazioni, tipicamente *metadati*, per integrare, modificare o sostituire quelle già presenti in un'**Unità documentaria** già conservata nel Sistema. Il versamento di tale pacchetto genera l'aggiornamento del *Pacchetto di archiviazione* dell'**Unità documentaria** i cui i metadati vengono aggiornati.

Nel caso in cui, per motivi tecnici o organizzativi, il *Produttore* non sia in grado di produrre o versare SIP nella struttura dati richiesta, può trasmettere i documenti sotto forma di generici **Oggetti** il cui contenuto e struttura è concordato con l'Ente conservatore. Tali **Oggetti** sono sottoposti alla procedura di Preacquisizione (descritta nel paragrafo 7.1.1) per essere trasformati in SIP ed essere così accettati dal Sistema.

[\[Torna al Sommario\]](#)

6.3 Pacchetto di archiviazione (AIP)

Il *Pacchetto di archiviazione* viene generato dal Sistema a conclusione del processo di acquisizione e *presa in carico* dei SIP (vedi paragrafo 7.5). È composto dagli **Oggetti-dati** (file), dall'**Indice dell'AIP**, un file XML che contiene tutti gli elementi del *pacchetto informativo*, derivati sia dalle informazioni contenute nel SIP (o nei SIP) trasmessi dal *Produttore*, sia da quelle generate dal Sistema nel corso del *processo di conservazione*, e dai Documenti di conservazione, ovvero i documenti ricevuti o prodotti nel corso del processo di conservazione (Indici dei SIP, Esiti dei versamenti, ecc.).

L'**Indice dell'AIP** generato dal Sistema è conforme alle specifiche definite dalla norma UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali, in adesione a quanto previsto dalle **Linee Guida**.

La tabella seguente illustra come i vari elementi del *pacchetto informativo* sono presenti nell'AIP gestito dal Sistema.

Elemento del pacchetto informativo	Articolazione dell'elemento	Descrizione
Contenuto informativo	Oggetto-dati	È la sequenza di bit (tipicamente sotto forma di file) associata al Componente . Può coincidere con quella inviata nel SIP dal <i>Produttore</i> o essere stata generata, a partire da questa, dal Sistema nel caso di produzione di copie informatiche.
	Informazioni sulla rappresentazione	Sono contenute a livello di Componente nell' Indice dell'AIP e sono derivate sia da quelle contenute nel SIP di origine, sia da quelle generate dal Sistema. Includono i <i>metadati</i> relativi al <i>formato</i> .

Elemento del pacchetto informativo	Articolazione dell'elemento	Descrizione
Informazioni sulla conservazione	Metadati di provenienza, contesto, identificazione, integrità	Sono contenuti nell' Indice dell'AIP a livello di Unità archivistica, Unità documentaria, Documento e Componente e originano dai SIP ricevuti o dai documenti generati dal <i>processo di conservazione</i> .
Informazioni sull'impacchettamento	-	A livello di Unità archivistica sono contenute nell'Indice e includono i riferimenti alle Unità documentarie che la compongono. A livello di Unità documentaria sono contenute nei Metadati di struttura e a livello di Componente negli identificativi utilizzati per associare il Componente all' Oggetto-dati .

Il Sistema è in grado di gestire e produrre tre tipi di AIP, descritti in dettaglio nel documento Modelli di AIP:

- AIP di **Unità documentaria**: contiene gli **Oggetti-dati** e si configura come **Unità di archiviazione (AIU)** in quanto oggetto elementare conservato nel Sistema;
- AIP di Unità archivistica: il caso tipico è il Fascicolo e si configura come una collezione di AIP o Raccolta di archiviazione (AIC), il cui contenuto informativo è costituito dagli AIP delle singole unità documentarie appartenenti al fascicolo;
- AIP di Serie: si divide a sua volta in AIP di Serie di Unità documentarie e in AIP di Serie di Unità archivistiche (fascicoli). Si configura anch'esso come una collezione di AIP.

[\[Torna al Sommario\]](#)

6.4 Pacchetto di distribuzione (DIP)

Il *Pacchetto di distribuzione* viene generato dal Sistema a partire dai *Pacchetti di archiviazione* conservati ed è finalizzato a mettere a disposizione degli *Utenti*, in una forma idonea alle specifiche esigenze di utilizzo, gli oggetti sottoposti a conservazione.

Il Sistema mette a disposizione degli *Utenti*, per tutti gli oggetti sottoposti a conservazione, un DIP coincidente con l'AIP, ma può gestire la produzione di DIP specifici in relazione a particolari esigenze. In relazione alle sue caratteristiche e agli utilizzi a cui è destinato, il *Pacchetto di distribuzione* può essere generato al momento della richiesta da parte di un *Utente* e non conservato nel Sistema.

Le modalità di *esibizione* dei DIP sono descritte al paragrafo 7.6.

[\[Torna al Sommario\]](#)

7 PROCESSO DI CONSERVAZIONE

Il *processo di conservazione* si attiva a seguito di sottoscrizione dell'**Accordo** tra il *Produttore* e la Regione Emilia-Romagna con le modalità indicate nell'**Accordo** stesso e dettagliate nel **Disciplinare tecnico**. L'**Accordo** medesimo disciplina anche la chiusura del servizio in caso di recesso o scadenza dell'**Accordo**, con le modalità operative descritte nel paragrafo 7.9.

7.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico

Il *processo di conservazione* si basa sul **versamento** da parte dei *Produttori* degli oggetti da conservare (*Documenti informatici* e *Aggregazioni documentali informatiche*) in due fasi: **Versamento anticipato** e **Versamento in archivio**.

Con **Versamento anticipato** si intende il **versamento** nel *Sistema di conservazione* di singoli *Documenti informatici* che possono trovarsi ancora nella fase attiva del loro ciclo di vita. Tale versamento avviene in un momento il più possibile prossimo a quello di effettiva produzione del documento ed è definito anticipato perché interviene in un momento antecedente a quello previsto normalmente dalla pratica archivistica, ovvero il versamento del Fascicolo chiuso, o della **Serie** completa (o di partizioni di essa) in archivio di deposito.

Il **Versamento anticipato** è finalizzato a mettere in sicurezza l'oggetto, prevedendo una serie di controlli tesi a verificarne i metadati, il *formato* e le eventuali firme digitali apposte, al fine di mettere in atto le opportune misure necessarie alla sua conservazione a lungo termine, ovvero:

- la rilevazione dell'eventuale obsolescenza dei formati dei file, in modo da attivare per tempo le misure necessarie a mantenerne la leggibilità;
- l'apposizione di un riferimento temporale certo e opponibile a terzi;
- la rilevazione di eventuali anomalie o errori nella produzione dei documenti, anche al fine di segnalare al *Produttore* le opportune contromisure per la loro risoluzione.

In questa fase è prevista l'acquisizione nel Sistema anche di *Documenti informatici* per i quali la normativa stabilisce tempi precisi di versamento come, ad esempio, il registro giornaliero di protocollo che deve essere "trasMESSO entro la giornata lavorativa successiva al *Sistema di conservazione*, garantendo l'*immodificabilità* del contenuto"⁹.

Con **Versamento in archivio** si intende il **versamento** nel Sistema delle *Aggregazioni documentali informatiche* nella loro forma stabile e definitiva, principalmente Fascicoli chiusi e partizioni annuali di **Serie** documentarie ¹⁰.

Questa fase del *processo di conservazione*, assimilabile al versamento dall'archivio corrente all'archivio di deposito, assolve a un duplice obiettivo: da un lato portare nel Sistema le informazioni necessarie a costruire l'*archivio informatico* dell'ente; dall'altro aggiornare e fissare

⁹ Linee Guida AgID, par. 3.1.6.

¹⁰ In ottemperanza a quanto previsto dall'art. 67 del DPR 445/2000, che al comma 1 prevede che "Almeno una volta ogni anno il responsabile del servizio per la gestione dei flussi documentali e degli archivi provvede a trasferire fascicoli e serie documentarie relativi a procedimenti conclusi in un apposito archivio di deposito costituito presso ciascuna amministrazione".

definitivamente, qualora si rendesse necessario, le informazioni di corredo relative alle **Unità documentarie** versate anticipatamente nel Sistema.

Il versamento in archivio di un'aggregazione documentale informatica avviene dopo che i singoli elementi che compongono l'aggregazione sono stati versati nel Sistema. Nel SIP dell'aggregazione sono elencati tutti gli elementi che la compongono e il versamento avviene solo se nel Sistema questi sono tutti presenti.

A tal fine, prima di procedere con il loro versamento in archivio, è consigliabile effettuare l'aggiornamento dei metadati relativi alle Unità documentarie versate in Versamento anticipato, in modo da assicurare che i metadati conservati nel Sistema siano completi e definitivi.

In altri termini, si può dire che con il **Versamento in archivio** viene completato, da parte del *Produttore*, il *processo di conservazione* iniziato con il **Versamento anticipato**, assicurando che gli oggetti digitali siano correttamente conservati a partire dal momento della loro produzione e resi accessibili per gli usi previsti (esibizione, accesso amministrativo, studio e ricerca). Al tempo stesso, il Sistema è messo in condizioni di acquisire, man mano che sono disponibili, le informazioni di contesto archivistico degli oggetti conservati e di assicurare in questo modo la corretta formazione dell'*archivio* del *Produttore*.

Il Sistema inoltre gestisce altre due modalità di conservazione particolari:

- **Conservazione fiscale**, finalizzata alla conservazione a norma dei documenti rilevanti ai fini tributari, in conformità con quanto previsto dalla normativa di settore vigente (DM del 17 giugno 2014 del Ministero dell'economia e delle finanze);
- **Migrazione**, che ha per oggetto *Documenti informatici e/o Aggregazioni documentali informatiche* provenienti da altri *sistemi di conservazione*. La peculiarità di questa conservazione risiede nella necessità di garantire il mantenimento della catena di custodia e si sostanzia nell'acquisizione, oltre che degli oggetti da sottoporre a conservazione, anche dei documenti e dei *metadati* prodotti dal *Sistema di conservazione* di provenienza; qualora il sistema di provenienza sia un *Sistema di conservazione* conforme alle **Linee guida** ai fini dell'*interoperabilità*, il SIP avrà le caratteristiche definite nelle **Linee Guida** al paragrafo 4.7 sul processo di conservazione alla lettera h.

I SIP sono prodotti e versati nel Sistema sotto la responsabilità del *Produttore* con le modalità e le procedure descritte nei loro aspetti generali nel presente Manuale e, per gli aspetti operativi e specifici relativi a ogni *Produttore*, nei **Disciplinari tecnici**, dove sono illustrati i *Documenti informatici* e le *Aggregazioni documentali informatiche* oggetto di conservazione e le procedure operative per il loro **versamento** e acquisizione nel Sistema.

Al momento dell'acquisizione i SIP sono oggetto di verifiche automatiche. Nel caso in cui le verifiche abbiano successo, il **versamento** viene accettato, il SIP viene acquisito per la sua *presa in carico* e si genera in modo automatico il *Rapporto di versamento*, che viene inviato al sistema che ha effettuato il **versamento** in un documento in formato XML denominato "**Esito versamento**". Qualora il SIP non abbia superato i controlli, l'**Esito versamento** riporta il dettaglio degli errori che hanno causato il fallimento del **versamento**.

I SIP presi in carico dal Sistema sono inseriti in **Elenchi di versamento**, documenti in formato XML, che vengono validati dal Responsabile della funzione archivistica di conservazione o automaticamente dal Sistema. La validazione dell'Elenco innesca la generazione dei *Pacchetti di archiviazione* (AIP) relativi ai SIP in Elenco.

Va ricordato che il Sistema è in grado di acquisire e prendere in carico automaticamente solo SIP che rispettano la struttura dati indicata nei Modelli di SIP e nelle Specifiche tecniche dei servizi di versamento (vedi paragrafo 6.2). Qualora il Produttore non sia in grado di versare i documenti come SIP, può trasmetterli sotto forma di Oggetti (di formato e struttura concordati con l'Ente conservatore) per sottoporli a un'elaborazione preliminare (Preacquisizione), svolta dal Sistema e finalizzata alla loro trasformazione in SIP.

In base a quanto appena illustrato, il processo di acquisizione e *presa in carico* dei SIP prevede le seguenti fasi:

1. Preacquisizione;
2. Acquisizione;
3. Verifica;
4. Rifiuto o accettazione;
5. Presa in carico e generazione del Rapporto di versamento;
6. Generazione del Pacchetto di archiviazione.

Nei paragrafi seguenti sono illustrate nel dettaglio le varie fasi del processo.

[\[Torna al Sommario\]](#)

7.1.1 Preacquisizione

La fase di Preacquisizione ha in input un Oggetto e in output uno o più SIP e ha inizio con la trasmissione dell'Oggetto a cura del *Produttore* o di un *Versatore* esterno da lui incaricato (vedi paragrafo 4.2). L'Oggetto trasmesso deve essere conforme alle specifiche definite dall'Ente conservatore. Il *Produttore* / *Versatore* trasmette l'Oggetto interfacciando i propri sistemi o utilizzando il client di versamento manuale messo a disposizione dall'Ente conservatore. Non è prevista la trasmissione degli Oggetti su supporti fisici.

Qualora la trasmissione abbia esito positivo al *Produttore* viene attestata la corretta ricezione dell'Oggetto.

L'Oggetto ricevuto è sottoposto a controlli finalizzati a verificarne la conformità con le relative specifiche. Le eventuali non conformità rilevate durante i controlli possono essere bloccanti o non bloccanti. Nel primo caso il processo si interrompe; nel secondo caso, invece, si interviene sull'oggetto ricevuto in modo da eliminare le non conformità rilevate. L'oggetto così modificato, unitamente alla descrizione degli interventi che ha subito, viene versato nuovamente nel Sistema e sottoposto nuovamente ai controlli di cui sopra.

Nel caso in cui i controlli abbiano esito positivo, il Sistema procede alle elaborazioni necessarie a versare il SIP, ovvero:

- trasformazione dell'Oggetto in uno più SIP: ogni SIP generato contiene il riferimento all'Oggetto dal quale è stato generato;
- **versamento** dei SIP nel Sistema: i SIP vengono versati nel Sistema con le modalità descritte nel paragrafo 7.1.2.

Il *Produttore* può in ogni momento interrogare il Sistema per ottenere informazioni sullo stato di avanzamento del processo di preacquisizione e sugli esiti del versamento dei SIP così generati.

[\[Torna al Sommario\]](#)

7.1.2 Acquisizione

L'acquisizione avviene con il **versamento** di SIP nel Sistema esclusivamente mediante l'utilizzo dei servizi descritti nel paragrafo 8.2 ed in dettaglio nel documento "Specifiche tecniche dei servizi di versamento".

Per effettuare il **versamento** dei SIP il *Produttore* può interfacciare i propri sistemi o, in alternativa, utilizzare il client di versamento manuale messo a disposizione da ParER mediante il quale inserire i dati necessari a generare e versare il SIP nel Sistema.

Non è prevista la trasmissione di SIP su supporti fisici.

Al completamento della trasmissione, il Sistema avvia contestualmente il processo di verifica del pacchetto, descritto nel paragrafo seguente.

[\[Torna al Sommario\]](#)

7.2 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti

Il SIP acquisito viene sottoposto a verifiche automatiche da parte del Sistema, finalizzate ad evidenziare eventuali anomalie.

Le verifiche riguardano:

- l'identificazione del Versatore: queste verifiche, effettuate mediante il controllo delle credenziali comunicate dal sistema versante a ogni versamento, sono finalizzate a garantire l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione e/o dell'*area organizzativa omogenea* di riferimento ai sensi del art. 44, comma 1 lettera a) del CAD e a garantire il corretto inserimento nell'*archivio* del *Produttore* nella opportuna **Struttura** (vedi paragrafo 6.1.1);
- la conformità dell'**Indice del SIP** al modello dati stabilito (vedi paragrafo 6.2): queste verifiche sono finalizzate a controllare se l'**Indice del SIP** è conforme al modello concordato con il *Produttore* e configurato nel sistema;
- l'univocità degli identificativi degli oggetti contenuti nel SIP: il controllo è finalizzato a verificare che gli identificativi assegnati dal *Produttore* e contenuti nel SIP siano effettivamente univoci, verificando che gli stessi non siano già presenti nel Sistema;
- la consistenza dei Metadati di profilo e specifici (vedi paragrafo 6.1.3): questa verifica è finalizzata a controllare che i set di Metadati presenti nel pacchetto siano conformi (in termini di obbligatorietà, valori e formato) a quelli concordati tra il *Produttore* e l'Ente conservatore. Tali set sono configurati nel Sistema mediante le funzionalità di Amministrazione delle Strutture versanti;

- il controllo sulle eventuali firme digitali apposte sugli **Oggetti-dati** (file) contenuti nel pacchetto. Le verifiche sono finalizzate a controllare la regolarità della firma digitale apposta in ordine a: formato di firma utilizzato, *integrità* del documento firmato (controllo crittografico), catena trusted, validità del certificato (scadenza e formato), presenza di eventuali revoche. I controlli sono effettuati alla data indicata dal *Produttore* nel SIP (che può essere quella contenuta nella firma, in una marca temporale o un riferimento temporale dichiarato nell'Indice SIP) o, in assenza di questa, alla data del versamento;
- l'ammissibilità dei **formati** degli **Oggetti-dati** (file) presenti nel pacchetto in base a quanto concordato con il *Produttore*: le verifiche si esplicano nel calcolo del **mimetype** dell'**Oggetto-dati** e nel confronto del valore così ottenuto sia con quello eventualmente dichiarato dal *Produttore* nel SIP, sia con i Formati ammessi, documentati e conservati nel Sistema nelle funzionalità di Amministrazione delle strutture versanti;
- la coerenza e la consistenza delle *Aggregazioni documentali informatiche* versate: si tratta di controlli che vengono svolti in caso di **Versamento in archivio** di *Aggregazioni documentali informatiche* e sono finalizzati a verificare la coerenza e la completezza di quanto versato.

La descrizione analitica delle verifiche automatiche e dei controlli a cui sono sottoposti i SIP, nonché le logiche con cui il Sistema opera in quest'attività, sono illustrati nel documento "Specifiche tecniche dei servizi di versamento".

[\[Torna al Sommario\]](#)

7.3 Accettazione e presa in carico dei pacchetti di versamento e generazione del rapporto di versamento

Nel caso in cui tutte le verifiche abbiano avuto esito positivo, il SIP viene acquisito nel Sistema per la sua *presa in carico*, memorizzato nelle sue varie parti (**Indice del SIP** e **Oggetti-dati**), associato logicamente all'*archivio* del *Produttore* ed eliminato dall'area di lavoro temporanea. In particolare, l'**Indice del SIP** e gli **Oggetti-dati** vengono memorizzati nella loro *integrità* e mantenuti nel Sistema anche ai fini del loro successivo inserimento nell'AIP (vedi paragrafo 7.5). Le operazioni di acquisizione si concludono con la *presa in carico* dei SIP accettati e la generazione automatica del relativo *Rapporto di versamento* che viene memorizzato nel Sistema e associato al SIP cui si riferisce.

Il *Rapporto di versamento* contiene l'Identificativo univoco del Rapporto, il *Riferimento temporale* relativo alla sua creazione (specificato con riferimento al **tempo UTC**), l'*impronta* dell'**Indice del SIP** e le *impronte* degli **Oggetti-dati** che ne fanno parte, oltre alla descrizione sintetica del contenuto del SIP acquisito. La descrizione analitica del *Rapporto di versamento* e la relativa struttura dati è contenuta nel documento "Specifiche tecniche dei servizi di versamento".

Il *Riferimento temporale* contenuto nel *Rapporto di versamento* è generato dal Sistema con le modalità descritte nel capitolo 8 ed è quindi da considerarsi opponibile ai terzi in base a quanto previsto dal comma 4, lettera b) dell'art. 41 del DPR 22 febbraio 2013.

Il *Rapporto di versamento* è reso disponibile al *Produttore* in varie modalità:

- è trasmesso in risposta al **versamento** del SIP nell'**Esito versamento**, un documento in formato XML che contiene, oltre al *Rapporto di versamento*, l'elenco analitico dei controlli eseguiti e dei relativi esiti, i parametri di configurazione del Sistema al momento del versamento e la data di versamento del SIP, descritto in dettaglio nel documento "Specifiche tecniche dei servizi di versamento";
- può essere richiesto utilizzando un apposito servizio, secondo le modalità descritte nel documento "Specifiche tecniche dei servizi di recupero";
- può essere visualizzato e scaricato dall'interfaccia web del Sistema dagli operatori abilitati, utilizzando le apposite funzionalità del Sistema.

[\[Torna al Sommario\]](#)

7.4 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie

Nel caso in cui almeno una delle verifiche descritte al paragrafo 7.3 non vada a buon fine, il SIP viene rifiutato e il Sistema restituisce al *Produttore* gli errori riscontrati, inviando l'**Esito versamento**, un documento in formato XML, descritto in dettaglio nel documento Specifiche tecniche dei servizi di versamento, in cui sono contenute tutte le informazioni sui controlli effettuati e i relativi esiti, sia sintetici che analitici, nonché l'**Indice del SIP** rifiutato.

I Pacchetti rifiutati, ovvero l'**Indice dei SIP** e gli **Oggetti-dati** che ne fanno parte, unitamente ai relativi **Esiti versamento**, sono memorizzati in un'area temporanea del Sistema, logicamente esterna all'*archivio* vero e proprio, a cui sia il *Produttore* che ParER possono accedere utilizzando l'interfaccia web del Sistema, per eventuali ulteriori controlli e verifiche (vedi paragrafo 7.4.1).

I SIP rifiutati restano memorizzati nel Sistema per almeno sei mesi; trascorso questo periodo possono essere cancellati, interamente o per la sola parte di **Oggetti-dati**. La cancellazione è stabilita ed effettuata sulla base di valutazioni che tengono conto delle **tipologie documentarie** trattate, delle caratteristiche del *Produttore* e della quantità e qualità dei versamenti falliti. Eventuali specifiche modalità e tempistiche di cancellazione dei SIP rifiutati sono concordate con il *Produttore* e configurate nel Sistema.

[\[Torna al Sommario\]](#)

7.4.1 Monitoraggio

Il Sistema mette a disposizione specifiche funzionalità di monitoraggio relative alla gestione dei **versamenti** dei SIP e alla generazione e gestione degli AIP, oltre a statistiche e report su quanto presente nel Sistema.

Il monitoraggio consente di avere una vista complessiva, suddivisa per fasce temporali, sull'acquisizione dei SIP, sul rifiuto dei SIP, sui tentativi falliti di versamento e sulle eventuali anomalie, mettendo a disposizione degli operatori tutte le informazioni necessarie a verificare

tanto le anomalie che hanno impedito il **versamento** dei SIP nel Sistema, quanto tutti gli elementi relativi ai SIP versati e agli AIP generati o aggiornati a seguito di tali **versamenti**.

In particolare, sono evidenziati, in tabelle sintetiche complessive o per singola **Struttura**:

- i **versamenti** di SIP svolti con successo, cioè che hanno generato un *Rapporto di versamento*;
- l'inserimento o meno dei SIP in **Elenchi di versamento**;
- i versamenti rifiutati;
- i tentativi di versamento falliti, che non hanno attivato il processo di acquisizione.

Tali informazioni di monitoraggio sono a disposizione degli *Utenti* degli Enti che dispongono di un profilo adeguato.

Dalle tabelle sintetiche è possibile scendere fino al dettaglio dei singoli versamenti, evidenziando, nel caso dei versamenti rifiutati, opportuni codici d'errore, che consentono agli operatori di individuare le soluzioni necessarie alla risoluzione delle anomalie riscontrate. Le più comuni azioni di risoluzione delle anomalie prevedono:

- Utilizzo di parametri di forzatura dei **versamenti**: nel caso in cui i controlli sulle firme, sui *formati* o sui collegamenti presenti sul SIP non vadano a buon fine e il **versamento** del SIP fallisca, i SIP rifiutati possono essere versati nuovamente in conservazione forzando i controlli precedentemente falliti. Tali forzature, che sono operate dal *Produttore* valorizzando appositi parametri presenti nel SIP, consentono di portare in conservazione i SIP anche in presenza delle anomalie, che inizialmente ne avevano pregiudicato l'acquisizione. In questi casi, il Sistema segnala al *Produttore* nell'**Esito versamento** che il SIP è stato acquisito a seguito di forzatura;
- Modifica di dati non corretti presenti nel SIP: nel caso in cui il SIP non superi i controlli a causa di alcuni dati non corretti nel SIP stesso, il *Produttore* provvede alla correzione dei dati indicati ed effettua nuovamente il **versamento**;
- Modifica delle configurazioni del Sistema: nel caso in cui il **versamento** del SIP non vada a buon fine per la presenza nel SIP stesso di dati non corrispondenti con i valori configurati nel Sistema, ParER può procedere, d'accordo con il *Produttore*, a modificare di conseguenza le configurazioni. Di tale modifica viene data comunicazione al *Produttore*, che provvede a inviare nuovamente in conservazione il SIP;
- Versamenti rifiutati e non risolvibili: nel caso in cui un **versamento** sia stato rifiutato per la presenza di anomalie che il *Produttore* giudica non risolvibili, il **versamento** può essere marcato come non risolvibile ed escluso, di conseguenza, da futuri controlli;
- Annullamento di versamenti effettuati: nel caso in cui un **versamento** andato a buon fine sia stato effettuato per errore o contenga degli errori non correggibili altrimenti, il *Produttore* provvede ad annullarlo, utilizzando apposite funzionalità del Sistema. Il SIP, e il relativo AIP eventualmente generato, non sono cancellati dal Sistema, ma marcati come Annullati. I SIP e gli AIP annullati sono esclusi dai risultati delle ricerche effettuate sul Sistema, e sono richiamabili solo da utenti appositamente abilitati a farlo.

Il modulo di Monitoraggio, inoltre, fornisce accesso alle statistiche dei sistemi, del Data Base, dei versamenti, ecc., mettendo a disposizione degli operatori report sia sintetici che analitici.

[\[Torna al Sommario\]](#)

7.4.2 Gestione delle anomalie

Le anomalie che possono riscontrarsi nell'operatività del servizio in fase di **versamento** sono gestite in generale secondo lo schema indicato nella tabella seguente.

Tipo anomalia	Descrizione	Modalità di gestione
Mancata risposta al versamento	È il caso in cui l' Unità documentaria viene correttamente versata ma, per vari motivi, la risposta di avvenuta ricezione non perviene al <i>Produttore</i> , che pertanto, può ritenerla erroneamente non versata, oltre a non ricevere il rapporto di versamento.	Il <i>Produttore</i> trasmette nuovamente l' Unità documentaria e il <i>Sistema di conservazione</i> restituisce una risposta di esito negativo che contiene l'indicazione che l' Unità documentaria risulta già versata e il relativo <i>Rapporto di versamento</i> . Tale risposta deve essere usata dal <i>Produttore</i> come attestazione di avvenuto versamento e l' Unità documentaria deve risultare come versata.
Errori temporanei	È il caso di errori dovuti a problemi temporanei che pregiudicano il versamento , ma si presume non si ripresentino a un successivo tentativo di versamento . Il caso più frequente è l'impossibilità temporanea di accedere alle CRL degli enti certificatori. In questi casi il <i>Sistema di conservazione</i> restituisce un messaggio di errore perché non riesce a completare le verifiche previste sulla validità della firma e il versamento viene quindi rifiutato.	Il <i>Produttore</i> deve provvedere a rinviare l' Unità documentaria in un momento successivo. L'operazione potrebbe dover essere ripetuta più volte qualora il problema, seppur temporaneo, dovesse protrarsi nel tempo.
Versamenti non conformi alle regole concordate	È il caso in cui il versamento non viene accettato perché non conforme alle regole concordate (formato file non previsto, mancanza di <i>metadati</i> obbligatori, ecc.).	<i>Produttore</i> e ParER concordano una soluzione al problema.
Errori interni o dovuti a casistiche non previste o non gestite	In alcuni casi è possibile che il <i>Sistema di conservazione</i> risponda con un messaggio di errore generico che non indica le cause dell'anomalia riscontrata in quanto dovuta a un errore interno o perché legata a una casistica non prevista, non gestita o non	Il <i>Produttore</i> segnala il problema a ParER, che si attiverà per la sua risoluzione.

Tipo anomalia	Descrizione	Modalità di gestione
	gestibile dal <i>Sistema di conservazione</i> .	
Errori nel contenuto dei dati conservati	È il caso eccezionale in cui per ragioni tecniche il <i>Sistema di conservazione</i> abbia effettuato un errore, che non può essere corretto con le procedure standard, oppure siano stati versati dati errati da parte del <i>Produttore</i> , che, in accordo con il <i>Produttore</i> stesso, si ritiene più semplice correggere per via tecnica, piuttosto che annullare e versare nuovamente	Il <i>Produttore</i> richiede formalmente al personale archivistico di ParER di effettuare una correzione tecnica dei dati; il gruppo di sviluppo e manutenzione viene quindi incaricato di intervenire manualmente sul database per effettuare la correzione: l'intervento effettuato viene annotato nell'AIP e l'azione manuale effettuata sul database viene tracciata nel log del database; la richiesta di intervento tecnico e la relativa soluzione rimangono tracciate all'interno del sistema di gestione delle attività di sviluppo e manutenzione.

[\[Torna al Sommario\]](#)

7.5 Preparazione e gestione del Pacchetto di archiviazione

Come elemento ulteriore di controllo dei versamenti effettuati, i SIP accettati e presi in carico sono inseriti in appositi **Elenchi di versamento**¹¹ generati secondo criteri, definiti "criteri di raggruppamento", predefiniti per **tipologia documentaria** e anno di produzione. Normalmente il criterio standard prevede che l'elenco si chiuda al raggiungimento di un numero massimo di componenti (5000) o dopo 30 giorni dall'apertura, ma tali parametri possono essere variati in base a specifiche esigenze conservative.

L'**Elenco di versamento** è un documento in formato XML, generato alla chiusura dell'elenco e fornito di un *Riferimento temporale* opponibile ai terzi. Riporta per ogni documento o aggregazione versata l'Identificativo univoco, un set di *metadati* descrittivi, le *impronte* degli **Oggetti-dati** che lo compongono e una serie di informazioni sintetiche relative alle verifiche a cui è il SIP è stato sottoposto durante il processo di acquisizione.

L'Elenco è recuperabile dal *Produttore* utilizzando apposite funzionalità dell'interfaccia web del Sistema.

Gli elementi inseriti nell'Elenco possono essere sottoposti a ulteriori controlli, anche a campione, finalizzati a verificare la corrispondenza degli oggetti versati con quanto concordato con il *Produttore* e a evidenziare eventuali anomalie non rilevabili dalle verifiche automatiche al **versamento**.

Una volta chiuso l'Elenco di versamento e completati i controlli, l'Elenco viene validato, automaticamente o manualmente dal Responsabile della funzione archivistica di conservazione, eventualmente anche con propria firma digitale.

¹¹Tali elementi vengono a sostituire le precedenti azioni di creazione volumi effettuate nel rispetto della Delibera CNIPA 11/2004. Gli **Elenchi di versamento** sono prodotti a partire dal 2015 a seguito dell'abbandono definitivo della creazione di volumi precedentemente prevista. Il sistema continua a gestire anche le informazioni relative ai volumi costituiti fino al 2014.

Tale validazione avvia il processo di creazione dei Pacchetti di Archiviazione (AIP) e dei relativi indici in formato conforme allo standard UNI SinCRO.

I SIP accettati e presi in carico dal Sistema, dopo la validazione dell'**Elenco di versamento** in cui sono stati inseriti, sono soggetti a una fase di elaborazione finalizzata alla creazione dell'AIP (o all'aggiornamento di un AIP esistente).

A seguito di queste elaborazioni, nel caso di **Versamento anticipato**, viene generato (o aggiornato) l'AIP dell'**Unità documentaria**.

L'AIP dell'**Unità documentaria** è composto da:

- l'**Indice dell'AIP**: è un documento in formato XML prodotto in conformità alle specifiche contenute nella norma UNI 11386 - Standard SinCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali e descritto in dettaglio nel documento "Modelli dei pacchetti di archiviazione", che contiene tutti i *metadati* dell'**Unità documentaria** presenti sul Sistema e i riferimenti agli altri file presenti nel pacchetto. Tra i dati contenuti nell'Indice vi sono:
 - la data di generazione dell'AIP (espressa con un *Riferimento temporale* opponibile ai terzi con le caratteristiche descritte al paragrafo 7.3), che costituisce il *Riferimento temporale* opponibile a terzi di tutti i file elencati nell'Indice stesso;
 - i *metadati* descrittivi dell'**Unità documentaria**;
 - i *metadati* generati dal Sistema nel corso delle verifiche e delle elaborazioni operate sul SIP;
 - le *impronte* dei singoli file (**Oggetti-dati**) dell'AIP stesso;
 - le *impronte* delle eventuali precedenti versioni dell'**Indice dell'AIP** (in caso di aggiornamento);
 - le *impronte* degli altri documenti generati dal Sistema nel *processo di conservazione*;
 - il riferimento agli **Elenchi di versamento** relativi ai SIP da cui è stato generato o aggiornato l'AIP;
- I file (**Oggetti-dati**) dell'**Unità documentaria** ricevuti nel SIP e le eventuali copie informatiche generate dal Sistema;
- I file con le eventuali precedenti versioni dell'**Indice dell'AIP**;
- I file degli **Indici dei SIP** da cui è stato generato o aggiornato l'AIP;
- I file degli **Esiti versamento** relativi ai SIP da cui è stato generato o aggiornato l'AIP;
- I file dei **Rapporti di versamento** relativi ai SIP da cui è stato generato o aggiornato l'AIP.

La sottoscrizione dell'AIP dell'**Unità documentaria** può essere effettuata con l'apposizione del sigillo elettronico del conservatore Regione Emilia-Romagna o tramite firma digitale del Responsabile del Servizio di Conservazione o del Responsabile della Funzione Archivistica di Conservazione.

La sottoscrizione degli AIP delle **Unità documentarie** può avvenire in due modi, a seconda che il processo di conservazione si svolga in regime di **versamento anticipato** o in regime di **versamento in archivio**.

Nel primo caso, la sottoscrizione viene apposta su un'evidenza informatica, denominata Elenco Indici AIP, prodotta a partire dagli **Elenchi di versamento** e contenente gli identificativi e l'impronta degli Indici degli AIP di ogni **Unità documentarie** contenuta negli elenchi stessi. Tale

evidenza informatica, una volta sottoscritta, è inserita negli AIP delle singole **Unità documentarie**.

Nel caso di **Versamento in archivio**, invece, la sottoscrizione degli AIP delle **Unità documentarie** avviene attraverso la sottoscrizione degli AIP delle aggregazioni (**Unità archivistiche** e **Serie**) in cui le **Unità documentarie** sono comprese. Gli Indici di tali AIP contengono, infatti, oltre ai *metadati* descrittivi dell'*Aggregazione documentale informatica*, le *impronte* degli Indici degli AIP delle **Unità documentarie** e/o delle **Unità archivistiche** che li compongono.

Gli **Indici dell'AIP** delle **Unità archivistiche** e delle **Serie** sono sottoscritti ad attestare il corretto svolgimento del processo di **Versamento in archivio** che completa il processo di trasferimento al Sistema dal punto di vista del *Produttore*. La sottoscrizione può essere effettuata con l'apposizione del sigillo elettronico del conservatore Regione Emilia-Romagna o tramite firma digitale del Responsabile del Servizio di Conservazione o del Responsabile della Funzione Archivistica di Conservazione.

Con la sottoscrizione dell'AIP dell'*Aggregazione documentale informatica* si determina anche l'accettazione della custodia da parte di ParER dei *Documenti informatici* e delle *Aggregazioni documentali informatiche* versate, cioè la dichiarazione che tutte le **Unità documentarie** relative all'*Aggregazione documentale informatica* sono correttamente acquisite e conservate dal Sistema nell'*archivio*.

Contestualmente alla generazione degli AIP, il Sistema memorizza le **Informazioni descrittive** sul *Pacchetto di archiviazione*, ovvero un set di *metadati* derivato da quello presente nell'**Indice dell'AIP** ed eventualmente da altri documenti contenuti nell'AIP stesso, finalizzato a ricercare gli AIP conservati nel Sistema.

Gli AIP sono conservati nel Sistema per il tempo di conservazione previsto dalle norme; allo scadere del tempo di conservazione possono essere scartati con le procedure descritte nel paragrafo 7.8.

Il *Produttore* può accedere agli AIP conservati utilizzando le funzionalità dell'interfaccia web del Sistema o chiamando l'apposito servizio con le modalità descritte nel documento "Specifiche tecniche dei servizi di recupero".

L'aggiornamento degli AIP può essere originato da due eventi: versamento di un SIP da parte del *Produttore* e attivazione di procedure di conservazione da parte del Sistema.

Nel primo caso l'aggiornamento dell'AIP viene innescato dal *Produttore* che può inviare ulteriori SIP per integrare o aggiornare le informazioni e/o altri elementi presenti nell'AIP secondo le modalità descritte nel documento "Specifiche tecniche dei servizi di versamento". Nel secondo caso, invece, gli aggiornamenti derivanti dalle procedure di conservazione sono innescati dal Sistema al verificarsi di determinati eventi e sono finalizzati a mantenere la *leggibilità* e la reperibilità nel tempo degli AIP.

Infine, gli AIP in casi eccezionali possono essere sottoposti a procedure di sequestro e di eventuale annullamento. Le procedure da applicare in questi casi sono descritte operativamente in specifici documenti tecnici.

Le politiche di conservazione dei pacchetti di archiviazione (AIP), per assicurare sia il contenuto dell'informazione all'ente produttore sia l'integrità nel tempo dei pacchetti conservati sono descritte al capitolo 9.2. Inoltre periodicamente viene verificato che il totale dei componenti versati con i SIP corrisponda alla somma dei componenti presenti negli AIP, di quelli in lavorazione e di quelli in attesa di lavorazione, al netto dei componenti contenuti in versamenti annullati.

[\[Torna al Sommario\]](#)

7.6 Preparazione e gestione del Pacchetto di distribuzione (DIP) ai fini dell'esibizione

I DIP sono prodotti di norma a partire dagli AIP presenti sul Sistema. Nel caso in cui non sia stato ancora generato l'AIP, è comunque possibile produrre DIP, riferiti agli oggetti versati e ai documenti di conservazione già prodotti.

Esistono varie tipologie di DIP, ognuna corrispondente alle specifiche esigenze di utilizzo da parte degli *Utenti (Comunità di riferimento)*.

In base alla tipologia di DIP e alle sue specifiche esigenze di utilizzo, il Sistema mette a disposizione funzionalità per la sua produzione e distribuzione, sia automatiche che manuali.

Il Sistema fornisce le seguenti tipologie di DIP:

- DIP coincidente con l'AIP: contiene tutti gli elementi presenti nell'AIP (vedi anche paragrafo 7.9) ed è scaricabile dall'interfaccia web del Sistema o tramite appositi servizi descritti nel documento "Specifiche tecniche dei servizi di recupero";
- DIP coincidente con il SIP: contiene gli Oggetti-dati presenti, l'**Indice del SIP** e l'**Esito versamento** ed è scaricabile dall'interfaccia web del Sistema;
- DIP del *Rapporto di versamento*: contiene i *Rapporti di versamento* relativi all'**Unità documentaria** ed è scaricabile dall'interfaccia web del Sistema o tramite appositi servizi descritti nel documento "Specifiche tecniche dei servizi di recupero";
- DIP dei documenti di conservazione: contiene i documenti di conservazione prodotti nel corso del processo di conservazione (**Indice del SIP**, Informazioni sull'impacchettamento, **Esito versamento**, *Rapporto di versamento*) ed è scaricabile dall'interfaccia del Sistema;
- DIP dell'**Unità documentaria**: contiene esclusivamente gli **Oggetti-dati** che la compongono ed è scaricabile dall'interfaccia web del Sistema;
- DIP del **Documento**: contiene esclusivamente gli **Oggetti-dati** del **Documento** ed è scaricabile dall'interfaccia web del Sistema;
- DIP del **Componente**: contiene il singolo file del **Componente** ed è scaricabile dall'interfaccia web del Sistema;
- DIP dell'**Elenco di versamento**: contiene l'**Elenco di versamento** in cui è contenuta l'**Unità documentaria** ed è scaricabile dall'interfaccia web del Sistema;
- DIP per l'esibizione: contiene i file dell'**Unità documentaria** e una dichiarazione, sotto forma di file in formato testo, che illustra il contenuto del DIP e fornisce informazioni utili ad agevolarne l'esibizione.

La distribuzione dei pacchetti a fine di *esibizione* avviene utilizzando le funzionalità dell'interfaccia web del Sistema, oppure chiamando l'apposito servizio descritto nel documento "Specifiche tecniche dei servizi di recupero".

Normalmente i DIP sono trasmessi o resi disponibili al *Produttore*, che poi provvede a consegnarli agli interessati. La consegna o la messa a disposizione dei DIP direttamente agli interessati è possibile solo con specifico accordo tra *Produttore* e ParER.

Il *Produttore* può consultare quanto versato in ParER tramite interfaccia web, collegandosi all'indirizzo comunicato da ParER e autenticandosi tramite username e password preventivamente forniti da ParER.

Gli operatori da abilitare per l'accesso tramite interfaccia web al *Sistema di conservazione* sono comunicati formalmente dal *Produttore* a ParER, che provvede a fornire le credenziali di accesso ai diretti interessati.

L'accesso web consente al *Produttore* di ricercare i documenti e le aggregazioni versati, di effettuarne il download e di acquisire le evidenze delle attività di conservazione.

[\[Torna al Sommario\]](#)

7.7 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti

La produzione di duplicati informatici o copie informatiche dei *Documenti informatici* conservati nel Sistema avviene mediante la messa a disposizione del *Produttore* di DIP comprensivi degli **Oggetti-dati** che li compongono.

Tali pacchetti sono acquisibili dagli *Utenti* utilizzando le funzionalità dell'interfaccia web del Sistema o gli appositi servizi descritti nel documento "Specifiche tecniche dei servizi di recupero".

Non è previsto da parte di ParER né il rilascio di copie cartacee conformi agli originali digitali conservati, né l'accesso diretto alla documentazione da parte di colui che, dovendo tutelare situazioni giuridicamente rilevanti, abbia presentato istanza di consultazione.

Pertanto, in merito all'esercizio del diritto d'accesso ai documenti conservati da ParER, questo si limita a fornire al *Produttore*, su precisa richiesta di quest'ultimo e senza che su di esso debba gravare alcun particolare onere, il documento informatico conservato, qualora per un qualsiasi motivo il *Produttore* stesso abbia deciso di non acquisirlo direttamente mediante le modalità descritte nel paragrafo 7.6.

Permane in carico al *Produttore* sia la responsabilità di valutare la fondatezza giuridica della domanda di accesso, sia l'onere di far pervenire il documento (o sua eventuale copia cartacea conforme) al soggetto richiedente.

ParER provvederà a consegnare direttamente la documentazione richiesta solo nel caso di visite ispettive presso ParER o provvedimenti di esibizione o sequestro da parte dell'autorità giudiziaria o di altra autorità ispettiva espressamente indirizzati al soggetto conservatore.

Nei casi previsti dalla normativa, il ruolo di pubblico ufficiale è svolto dal Responsabile del servizio ParER in qualità di dirigente dell'ufficio responsabile della conservazione dei documenti, o da altri dallo stesso formalmente designati, quale il Responsabile della Funzione archivistica di

conservazione per l'attestazione di conformità all'originale di copie di *Documenti informatici* conservati.

Il ruolo di pubblico ufficiale, per i casi in cui è previsto l'intervento di soggetto diverso della stessa amministrazione, sarà svolto da altro dirigente all'uopo individuato o da altro soggetto da quest'ultimo designato.

[\[Torna al Sommario\]](#)

7.8 Scarto dei pacchetti di archiviazione

Il Produttore, in base ai tempi di conservazione risultanti dai propri **Massimari di scarto** invia a ParER un Elenco di scarto, in cui sono indicate le **Unità archivistiche** o le **Unità documentarie** da sottoporre a procedura di *scarto*.

Tale Elenco di scarto viene verificato da parte di ParER ed eventualmente adeguato in modo da poter essere utilizzato nel Sistema. L'elenco, se modificato, viene trasmesso al *Produttore* che può rifiutarlo indicandone i motivi (innescando in tal modo una nuova verifica da parte di ParER) o accettarlo. L'elenco finale viene trasmesso dal *Produttore* all'Autorità di vigilanza che, in base alle norme vigenti, deve fornire l'autorizzazione per lo *scarto*.

Il *Produttore*, una volta ricevuto il nulla-osta (che può essere concesso anche solo su una parte dell'Elenco proposto), provvede ad adeguare, se necessario, l'*Elenco di scarto* presente sul Sistema alle decisioni dell'Autorità. Una volta che l'*Elenco di scarto* definitivo viene predisposto, il *Produttore* lo valida e trasmette a ParER la richiesta di procedere allo *scarto*.

ParER effettua un ulteriore controllo sulla congruenza dell'*Elenco di scarto* definitivo con quello autorizzato dall'autorità e, in caso riscontri anomalie, provvede alla correzione e sottopone nuovamente l'Elenco alla validazione del *Produttore*.

Nel caso in cui il controllo sull'*Elenco di scarto* dia esito positivo, ParER procede alla cancellazione degli AIP contenuti nell'Elenco. Al termine delle operazioni viene data comunicazione al Produttore dell'avvenuto scarto, fornendo nella stessa tutti gli elementi utili a ricostruire l'intero processo.

[\[Torna al Sommario\]](#)

7.9 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori

L'**Accordo** prevede che, in caso di recesso o a scadenza di contratto, la Regione Emilia-Romagna, tramite il ParER, è tenuta a riversare i *Documenti informatici* e le *Aggregazioni documentali informatiche* conservate, i *metadati* a essi associati e le *evidenze informatiche* generate nel corso

del *processo di conservazione* nel sistema indicato dal *Produttore*, secondo modalità e tempi indicati nel **Disciplinare Tecnico** o nella specifica procedura.

ParER garantisce comunque il mantenimento nel proprio *Sistema di conservazione* dei *Documenti informatici* e delle *Aggregazioni documentali informatiche* conservati, con i *metadati* a essi associati e le *evidenze informatiche* generate nel corso del *processo di conservazione* fino alla comunicazione da parte del *Produttore* dell'effettiva messa a disposizione del *Sistema di conservazione* in cui effettuare il riversamento.

ParER provvederà all'eliminazione dal proprio *Sistema di conservazione* di tutti gli oggetti riversati e di tutti gli elementi riferiti al *Produttore* solo al termine del riversamento e solo dopo le opportune verifiche - effettuate da entrambe le Parti e svolte di concerto tra le stesse - di corretto svolgimento del riversamento stesso.

In tal caso viene garantita la cancellazione e non leggibilità dei dati entro 90 giorni, a partire dal termine del versamento e delle relative verifiche, sia dal sistema primario (compresi i backup), sia dal sito di **business continuity**, sia dal sito di **Disaster recovery**.

L'intera operazione dovrà comunque avvenire con l'autorizzazione e la vigilanza delle competenti autorità, in particolare delle strutture del MiC.

In caso di chiusura del servizio da parte della Regione Emilia-Romagna, con interventi di modifica alla normativa regionale, si provvederà a trasferire quanto conservato ai *Sistemi di conservazione* individuati per proseguire le attività svolte dalla Regione Emilia-Romagna e a cancellarlo da tutti i sistemi compresi quelli di backup, fornendo evidenze del trasferimento all'Ente Produttore.

Per quanto riguarda gli aspetti operativi per il trasferimento di *archivi* ad altri *sistemi di conservazione*, ParER adotta lo standard Uni Sincro, e provvede a mettere a disposizione l'*archivio* del *Produttore* in un'area a lui dedicata, da cui potrà prelevarlo utilizzando un canale sicuro di trasferimento (**FTPS**). Analogamente il Sistema è predisposto per la ricezione di *archivi* in formato Uni Sincro; qualora il precedente Conservatore non sia in grado di produrre l'*archivio* in formato Uni Sincro, ParER, a seguito di specifici accordi, può mettere a disposizione del *Produttore* consulenza e strumenti per facilitarne il trasferimento.

[\[Torna al Sommario\]](#)

8 IL SISTEMA DI CONSERVAZIONE

8.1 Componenti logiche

Il diagramma in figura, realizzato sul modello della rappresentazione delle entità funzionali di **OAIS**, schematizza dal punto di vista logico le principali componenti del *Sistema di conservazione* di ParER e le principali relazioni con i soggetti interessati dal *processo di conservazione* descritto nei capitoli precedenti del presente Manuale.

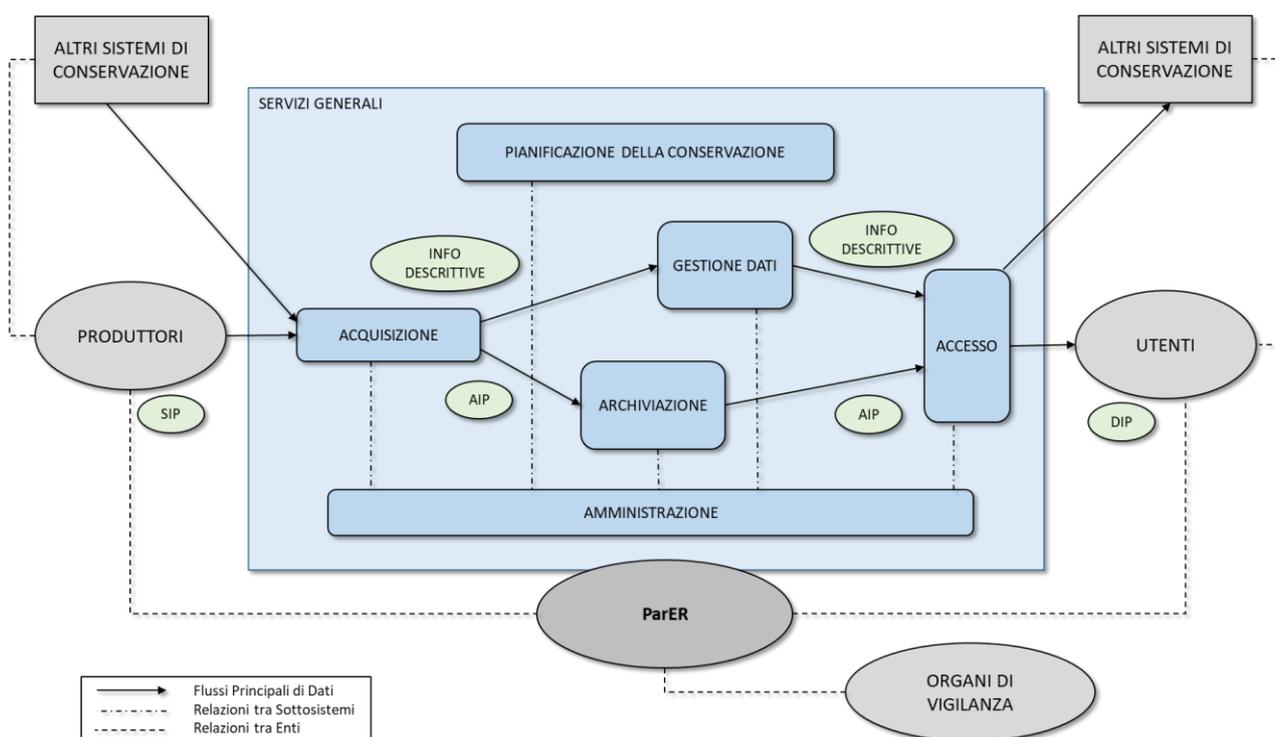


Figura 6 - Schema logico del Sistema di conservazione

Per la descrizione dei ruoli di *Produttori*, *Utenti*, Regione Emilia-Romagna/ParER, come soggetto Conservatore e Amministratore del Sistema, e Organi di vigilanza si rimanda al capitolo 4 del presente Manuale.

In ottica di *interoperabilità* ParER è in grado di ricevere da altri *sistemi di conservazione* documenti già sottoposti a conservazione, e di versarli ad altri Sistemi secondo gli accordi intercorsi con il *Produttore*.

Le funzionalità di *Acquisizione* gestiscono la fase di *Acquisizione* e *presa in carico* del *processo di conservazione* (vedi paragrafi 7.1 – 7.4), ovvero, attraverso i **Web Service** di versamento esposti dal Sistema, consentono la ricezione dei SIP dei *Produttori*, la loro verifica e la generazione, a partire dai SIP, dei relativi AIP e delle **Informazioni descrittive** per la loro ricerca.

Le funzionalità di *Gestione Dati* gestiscono le **Informazioni descrittive** generate al termine della fase di *acquisizione* e *presa in carico* del *processo di conservazione*. Tali funzionalità garantiscono: *memorizzazione*, *manutenzione* e *aggiornamento* all'interno del Sistema sia delle

Informazioni descrittive necessarie a ricercare gli AIP, ricevute dall'Acquisizione, che dei dati necessari per gestire i pacchetti.

Le funzionalità di Archiviazione gestiscono la fase di gestione degli AIP del *processo di conservazione* (vedi paragrafo 7.5): *memorizzazione*, **migrazione** dei supporti, backup, **Disaster recovery** ed eliminazione (*scarto*) degli AIP conservati nel Sistema.

Le funzionalità di Amministrazione gestiscono il governo dell'intero *processo di conservazione*, permettendo di definire e aggiornare nel Sistema politiche, standard e configurazioni che regolano tutte le altre funzionalità, incluse la gestione degli accordi con i *Produttori*, il monitoraggio del Sistema, la produzione di copie informatiche per la conservazione (**migrazione** dei *formati*) e la selezione degli AIP per lo *scarto*.

Le funzionalità di Pianificazione della conservazione gestiscono il monitoraggio dell'ambiente in cui il Sistema è inserito e forniscono le indicazioni necessarie per fare in modo che le informazioni conservate restino fruibili nel lungo periodo, tenendo conto dell'evoluzione tecnologica dei sistemi e del cambiamento della **Comunità di riferimento** (*Utenti*). Intervengono nella progettazione dei *Pacchetti Informativi* e nella pianificazione dello sviluppo e dei test del software necessario per la **migrazione** degli AIP. Tale funzione non è svolta da uno specifico applicativo, né segue procedure meccaniche, ma si configura invece come una serie di attività svolte utilizzando un insieme di strumenti, non solo informatici, finalizzati a raccogliere informazioni, confrontarsi con la **Comunità di riferimento**, effettuare test e verifiche sugli oggetti conservati, il tutto finalizzato a fornire indicazioni utili a mantenere il *processo di conservazione* aggiornato in relazione sia all'evoluzione tecnologica, che alle esigenze della **Comunità di riferimento**. I risultati di questa analisi si concretizzano, tipicamente ma non esclusivamente, in aggiornamenti nei modelli di *pacchetti informativi* gestiti dal Sistema, in implementazione di nuove librerie o altri strumenti software utilizzati dal Sistema, nella definizione e nell'aggiornamento delle politiche di conservazione e nei test su nuovi componenti hardware. Questi elementi sono inseriti nel Sistema utilizzando principalmente le funzionalità di Amministrazione di SacER e, secondariamente, quelle analoghe presenti negli altri moduli del Sistema, garantendo che il *processo di conservazione* sia sempre in grado tanto di contrastare efficacemente l'obsolescenza tecnologica, quanto di rispondere adeguatamente alle esigenze della **Comunità di riferimento** di ParER.

Le funzionalità di *accesso* gestiscono la fase di gestione del DIP del *processo di conservazione* (vedi paragrafo 7.6), fornendo supporto agli operatori per la ricerca e la restituzione degli oggetti conservati. Le funzioni di *interoperabilità* consentono inoltre la restituzione da parte del Sistema di DIP coincidenti con gli AIP conformi a quanto previsto dalle **Linee guida**.

Il diagramma in figura schematizza i principali flussi di dati che intercorrono tra le componenti logiche del sistema descritte nei paragrafi precedenti; per completezza nello schema è stata inserita anche la componente '**Disaster recovery**', in quanto, pur non avendo un ruolo rilevante nella gestione ordinaria, riveste un ruolo significativo nello scambio di flussi informativi e svolge funzionalità elaborative autonome, seppur limitate, ai fini della produzione delle copie di salvataggio dei file su cassetta.

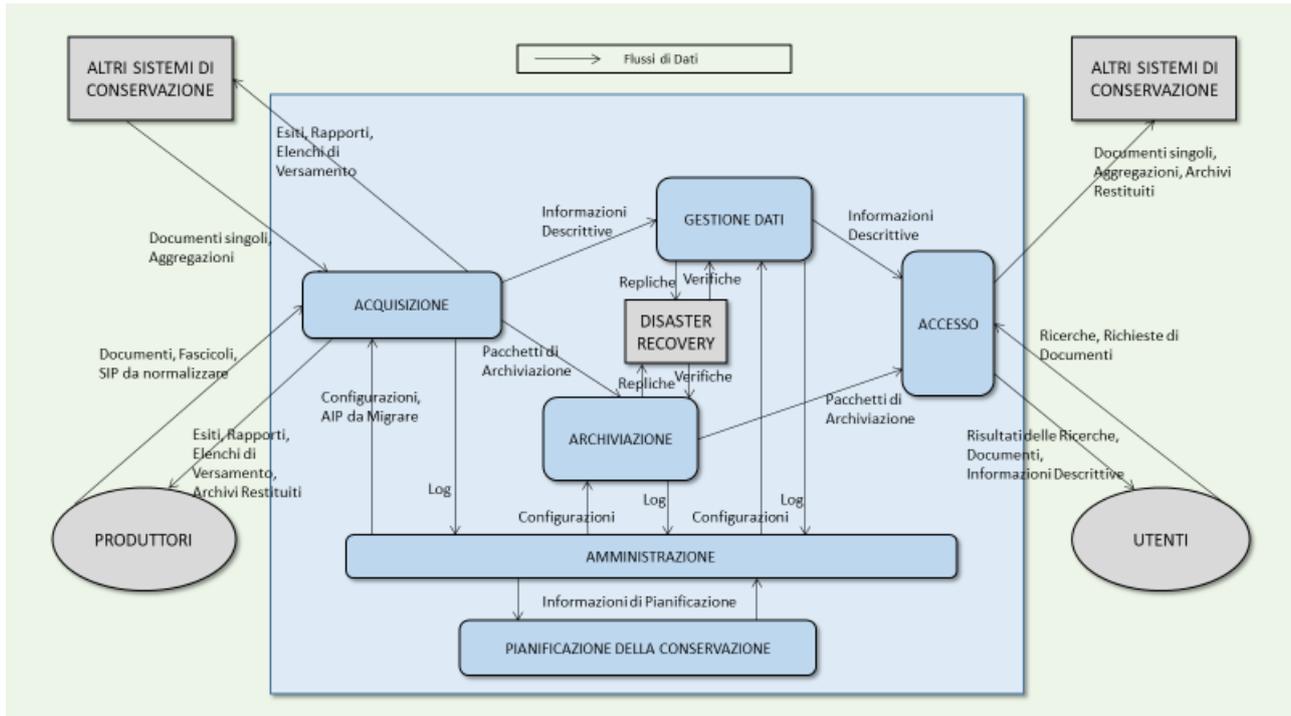


Figura 7 - Flussi di dati nel Sistema di conservazione

Il Servizio di conservazione è supportato da un unico Sistema integrato, suddiviso logicamente in sistemi dedicati agli specifici conservatori (ambienti). Nell'ambito del Sistema gli archivi di ogni Ente *Produttore* sono allocati in aree logicamente separate (strutture). Gli accessi degli utenti sono limitati alle strutture per i quali sono stati profilati in modo tale che gli archivi di ogni Ente risultano adeguatamente protetti.

In aggiunta alle componenti logiche delineate nei paragrafi precedenti, che ne costituiscono il nucleo centrale, il Sistema mette a disposizione diversi Servizi generali a supporto delle altre funzionalità. Oltre ai servizi di gestione e monitoraggio dei sistemi, della rete, e della sicurezza dei sistemi, mette a disposizione in particolare:

- il servizio di **Identity Management**, che, via *IDP*, garantisce i corretti accessi al Sistema da parte dei diversi utilizzatori;
- il servizio di Firma tramite dispositivo **HSM**, che consente di apporre le firme digitali necessarie nel processo di conservazione senza utilizzare **applet** di firma all'interno del browser;
- il servizio di **Audit e Log**, che mantiene e manda in conservazione la storia degli accessi effettuati al Sistema e ai dati;
- il **Sito Web** di ParER, che fornisce informazioni e documentazioni relative al processo e al *Sistema di conservazione*;
- il Sistema di e-Learning della Regione Emilia-Romagna, che nell'area dedicata a ParER mette a disposizione degli utenti corsi sul processo di Conservazione.

[\[Torna al Sommario\]](#)

8.2 Componenti tecnologiche

Il *Sistema di conservazione* è costituito da diversi moduli software che interagiscono tra loro per la gestione dell'intero *processo di conservazione*. Il Sistema, inoltre, si avvale di ulteriori componenti applicative esterne con funzioni di supporto al processo.

Il diagramma in figura schematizza dal punto di vista tecnologico le principali componenti del *Sistema di conservazione* di ParER e le principali relazioni con altri sistemi interessati dal *processo di conservazione* descritto nei capitoli precedenti del presente Manuale.

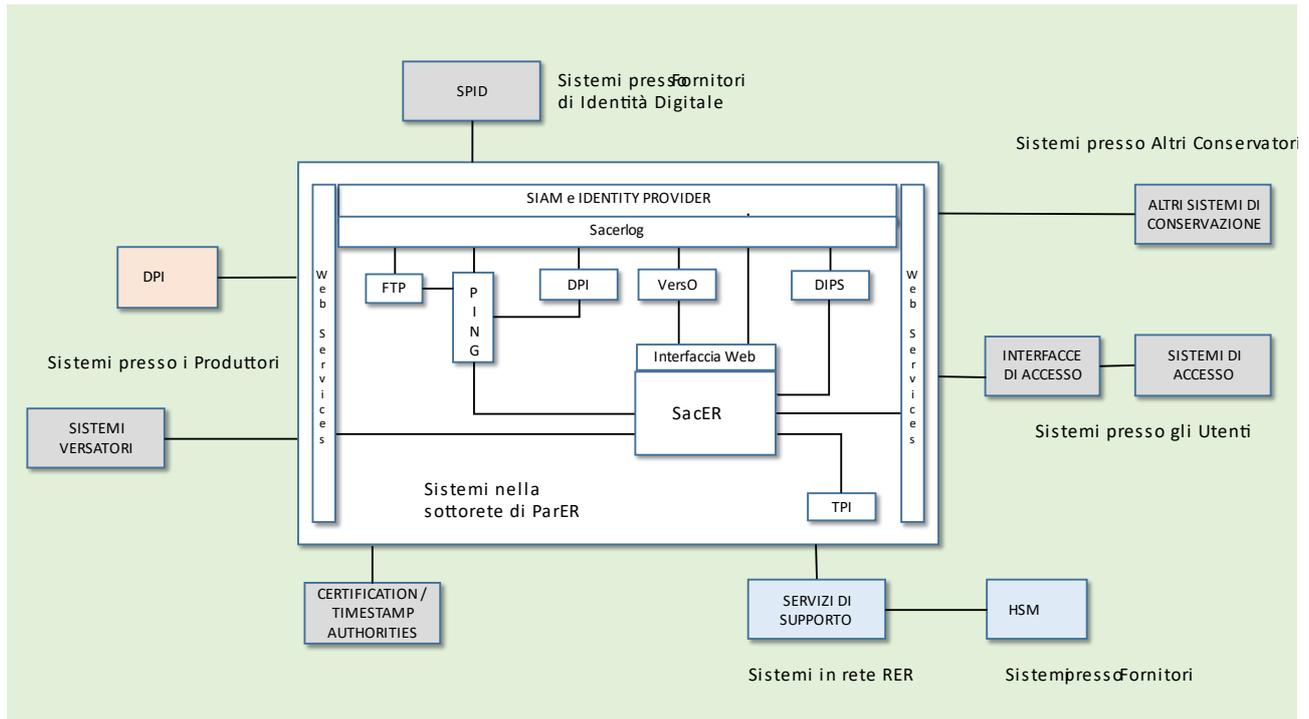


Figura 8 - Schema Tecnologico del Sistema di conservazione

Nella figura sono riportate:

- in bianco le componenti del *Sistema di conservazione* interne al perimetro di sicurezza del data center di ParER;
- in rosa le componenti del *Sistema di conservazione* sviluppate da ParER, ma esterne al perimetro di sicurezza del data center di ParER, in quanto installate nelle reti dei *Produttori*;
- in azzurro le componenti a supporto del Sistema gestite dalla Regione Emilia-Romagna;
- in grigio le componenti che fanno riferimento ai soggetti esterni (*Produttori, Utenti e Authorities*).

Qui di seguito sono illustrati i singoli moduli software del Sistema e le componenti di supporto.

[\[Torna al Sommario\]](#)

8.2.1 SacER

Il modulo software SacER costituisce il nucleo centrale del Sistema e implementa le funzionalità principali del *processo di conservazione*, quali:

- Acquisizione SIP;
- Archiviazione;
- Gestione dati;
- Amministrazione;
- Accesso.

Le funzionalità di Acquisizione SIP di SacER consentono la gestione delle varie fasi del processo di Acquisizione e *presa in carico* (vedi paragrafi 7.1 – 7.4). Operativamente si compongono delle seguenti attività:

- acquisizione del SIP trasmesso attraverso i Servizi di versamento;
- **memorizzazione** del SIP in un'area temporanea logicamente distinta dall'*archivio* vero e proprio per effettuare le verifiche previste;
- verifica del SIP in relazione alla struttura dati, ai *metadati* degli oggetti sottoposti a conservazione, alle eventuali firme apposte sui file (**Oggetti-dati**) associati ai **Componenti**, ai *formati* dei file stessi e generazione del *Rapporto di versamento* in caso di verifica positiva;
- restituzione dell'**Esito versamento**, comprensivo, in caso di esito positivo, del *Rapporto di versamento*;
- creazione degli **Elenchi di versamento**: un primo job provvede all'individuazione dei SIP da inserire negli Elenchi secondo i criteri di raggruppamento definiti da ParER; un secondo job genera gli Elenchi e vi appone un *Riferimento temporale* opponibile a terzi; un terzo job esegue i controlli finali e chiude l'Elenco per la sottoscrizione a cura del Responsabile della funzione archivistica di conservazione. Tutti i job sono eseguiti sugli Application server automaticamente ed in modo ricorrente secondo intervalli di tempo stabiliti nel modulo Amministrazione;
- eventuale migrazione di **formato** degli **Oggetti-dati** contenuti nei SIP sia per contrastarne l'obsolescenza tecnologica, sia per esigenze di miglioramento della fruibilità degli oggetti conservati;
- estrazione dei metadati dal SIP (ed eventuale loro normalizzazione) e dal Sistema da utilizzare per completare le informazioni necessarie a generare l'AIP (**Informazioni sulla rappresentazione, Informazioni sulla conservazione, Informazioni sull'impacchettamento, Informazioni descrittive**);
- generazione dell'**Indice dell'AIP**, utilizzando i metadati estratti dal SIP e quelli generati dal Sistema nel corso del processo di conservazione. SacER produce report di eccezioni a fronte di situazioni anomale nella creazione dell'**Indice dell'AIP**. Tutte le azioni vengono registrate sul sistema in apposite tabelle di log;
- generazione dell'AIP, che avviene impacchettando in un oggetto auto-consistente l'**Indice dell'AIP**, le evidenze informatiche prodotte nel corso del processo di conservazione e gli **Oggetti-dati**.

Le funzionalità di Archiviazione di SacER gestiscono la parte del processo di Gestione dell'AIP relativa alla *memorizzazione* e verifica degli **Oggetti-dati** su Data Base Oracle e **file system** (vedi paragrafo 7.5) e comprendono:

- la **memorizzazione** degli AIP e l'organizzazione gerarchica dei supporti di memorizzazione. In particolare, gli **Oggetti-dati** degli AIP, costituiti dagli **Indici degli**

AIP e dei SIP, dagli **Esiti versamento**, dai *Rapporti di versamento* e dai file associati ai **Componenti**, sono memorizzati su supporti di diverso tipo in ragione della loro dimensione e della frequenza con cui vengono ricercati:

- gli **Oggetti-dati** di piccole dimensioni e ad accesso più frequente vengono salvati temporaneamente all'interno del Data Base in opportune tabelle sotto forma di **BLOb**, per poi essere memorizzati in modo permanente nell'**object storage**, utilizzando a questo scopo appositi job periodici, descritti più avanti
- gli **Oggetti-dati** di grande dimensione e di accesso meno frequente vengono salvati temporaneamente su **file system** in cartelle opportunamente strutturate, per poi essere memorizzati in modo permanente su supporti a cassette, utilizzando a questo scopo un apposito componente software chiamato TPI, descritto più avanti;
- il controllo dell'integrità degli oggetti conservati, comprensivo della copia degli archivi, del controllo degli errori e delle procedure di refreshing dei supporti, come descritto nel paragrafo 9.2 e in conformità con il Piano della Sicurezza di ParER;
- la restituzione dei pacchetti alle funzioni di Accesso, mediante opportune funzionalità dell'interfaccia web del Sistema o mediante l'utilizzo di Servizi di recupero;
- la cancellazione degli AIP sottoposti a scarto a seguito della procedura descritta nel paragrafo 7.8.

Le funzionalità di Gestione Dati di SacER sono finalizzate principalmente a gestire le **Informazioni descrittive** degli AIP generate durante il processo di acquisizione (vedi paragrafo 7.5) e includono:

- la **memorizzazione** dei *metadati* estratti dal SIP o generati dal Sistema nel corso del processo di Acquisizione dei SIP;
- la gestione degli aggiornamenti dei dati generati dalle funzionalità di Amministrazione e nel corso del *processo di conservazione*;
- l'esecuzione delle ricerche e la sua restituzione alle funzionalità di Accesso, che avvengono mediante l'utilizzo di funzionalità da interfaccia web del Sistema o mediante chiamata a Servizi specifici.

Le funzionalità di Amministrazione di SacER consentono di gestire configurazioni e parametrizzazioni in grado di determinare il funzionamento del Sistema in funzione degli specifici accordi intercorsi con i *Produttori*, definite nel **Disciplinare tecnico** e in funzione delle policy stabilite nell'ambito della Pianificazione della conservazione (come descritto più avanti). Inoltre, consentono di monitorare tutta l'attività svolta da SacER, così come descritto nel paragrafo 7.4.1. In particolare, in SacER è possibile configurare tutte le entità significative: Enti, **Strutture**, operatori e relativi profili, **tipologie documentarie**, **formati** accettati, logiche di controllo dei versamenti, logiche di creazione delle **Serie**, regole di *accesso* e di esibizione, politiche di monitoraggio del sistema. Anche l'interfaccia web di SacER è configurata automaticamente in ragione del profilo dei singoli operatori che vi accedono.

Le funzionalità di Amministrazione sono costituite da transazioni eseguibili tramite l'interfaccia web del sistema e riservate agli operatori di ParER, ma visibili negli esiti anche agli operatori dei *Produttori*.

Le funzionalità di Accesso di SacER consentono di restituire in forma di DIP gli oggetti conservati. A tal fine SacER mette a disposizione un'interfaccia web per le ricerche e per l'estrazione manuale dei documenti e dei Servizi di recupero per l'estrazione automatica.

Gli AIP forniti sono trasformati in DIP sulla base delle caratteristiche dell'oggetto e degli utilizzi cui è destinato. In molti casi la trasformazione dell'AIP in DIP può richiedere specifici passi

elaborativi e trasformazioni complesse, che, necessitando di elaborazioni onerose, vengono normalmente eseguite da opportuni job batch e mantenute in modo permanente sul Data Base. Secondo la natura dei DIP, l'*esibizione* può avvenire on-line con un download, oppure tramite il trasferimento in un'area di transito, da cui il successivo recupero viene effettuato dal sistema richiedente con chiamata FTP. In molti casi, per comodità di trasferimento e recupero, i vari elementi che costituiscono il DIP vengono compressi in un archivio di tipo ZIP.

Il modulo di Accesso, oltre a verificare tramite i servizi di Autenticazione l'abilitazione dell'*Utente* al recupero del documento, traccia in apposite tabelle di log tutte le richieste prevenute, qualunque ne sia stato l'esito.

[\[Torna al Sommario\]](#)

8.2.2 VersO

Il client di versamento manuale VersO (Versamento Online) è un modulo che ParER mette a disposizione degli Enti produttori per svolgere operazioni routinarie sul sistema. Poiché utilizza un'interfaccia web, non richiede l'installazione di alcun software sulla stazione di lavoro dell'*Utente*.

Il suo utilizzo tipico è il **versamento di Unità documentarie** per le quali non esiste un sistema interfacciato con Sacer. VersO viene richiamato tramite interfaccia web, si autentica sull'**IdP** di ParER o su **SPID**, utilizzando in ogni caso logiche di profilazione del Sistema, ed effettua il **versamento** dei SIP tramite interazione guidata con l'operatore del *Produttore*.

Tale modulo semplifica le operazioni di **versamento** manuale da parte del *Produttore*, automatizzando la generazione dell'**Indice del SIP** ed effettuando un test completo della correttezza del versamento prima di eseguire il versamento stesso. Inoltre, mantiene il log dei versamenti effettuati e consente di interrompere temporaneamente l'operazione (p.e per raccogliere informazioni necessarie per completarlo), riprendendola successivamente, indipendentemente dalla scadenza della sessione web.

[\[Torna al Sommario\]](#)

8.2.3 PING

Il modulo software PING (PreINGest) gestisce il processo di preacquisizione nel caso di **versamento** di Oggetti da trasformare in SIP (vedi paragrafo 7.1.1).

La trasmissione dei pacchetti, solitamente compressi, avviene tramite protocollo **FTPS**; l'**FTP server** provvede a memorizzare i file ricevuti sullo **storage** dedicato allo spazio FTP di input.

Una volta ricevuti gli Oggetti, un job schedulato provvede alla loro elaborazione per la produzione dei SIP da versare. Un ulteriore job schedulato si occupa di effettuare il **versamento** a SacER, che avviene utilizzando un apposito servizio di versamento. Tale servizio accetta in chiamata due file XML, uno con l'**Indice del SIP** e un altro con le **Informazioni sull'impacchettamento**, relative alla posizione dei file del SIP memorizzati sullo spazio FTP di input.

SacER utilizza le **Informazioni sull'impacchettamento** per recuperare i file dal **file system** di PING e depositarli nel proprio per le successive elaborazioni.

Le successive elaborazioni vengono eseguite da PING direttamente, nel caso in cui la normalizzazione possa basarsi su regole precodificate (come p.e. nel caso delle immagini diagnostiche in formato Dicom), oppure utilizzando un motore ETL di esecuzione delle trasformazioni nel caso in cui si debbano applicare regole di trasformazioni specifiche dell'oggetto in questione. In questo caso le regole vengono definite durante la fase di avvio del servizio, tramite uno strumento visuale ed eventuali integrazioni di codice sviluppato ad hoc.

PING traccia e memorizza nel proprio Data Base gli esiti dei versamenti a SacER e può essere interrogato da un operatore tramite interfaccia web o dal sistema versante tramite opportuno **Web Service**, per conoscere a quale punto del processo è giunto il SIP.

PING mette inoltre a disposizione del *Produttore* un client di versamento di Oggetti da trasformare, sia on line, sia tramite l'utilizzo di un client **FTP** installato sulla postazione di lavoro dell'utente o su un server della rete del *Produttore*.

[\[Torna al Sommario\]](#)

8.2.4 DPI

Il modulo software DPI (Digital Preservation Interface), sviluppato e mantenuto da ParER, consiste in un sistema di interfaccia tra i sistemi dell'Ente produttore e PING; DPI può essere installato all'interno della rete dell'Ente stesso e gestito secondo le politiche di sicurezza dell'Ente, potendo tra l'altro autenticarsi sul suo **IdP**.

DPI implementa funzionalità di **versamento** per specifiche tipologie di SIP. In particolare, qualificandosi come nodo **DICOM**, DPI riceve dai **PACS** studi diagnostici, che poi trasmette a PING per la trasformazione e il **versamento** a SacER.

DPI può operare con logiche sia push che pull, ricevendo o estraendo dati e documenti dai sistemi del *Produttore* per poi versarli nel Sistema, richiamando gli opportuni servizi di PING.

Inoltre, DPI fornisce strumenti di monitoraggio dei versamenti effettuati a disposizione dell'Ente produttore.

[\[Torna al Sommario\]](#)

8.2.5 Interfacce di Acquisizione e di Recupero (Web Service)

I sistemi che debbono versare a SacER documenti o aggregazioni e ottenerne l'esibizione colloquiano con SacER tramite opportuni **Web Service**, che sono definiti nei documenti "Specifiche tecniche dei servizi di versamento" e "Specifiche tecniche dei servizi di recupero". Tali servizi sono invocati anche dai componenti di versamento sviluppati da ParER (DPI, VersO), oltre che dai sistemi di versamento dei *Produttori*.

Nel processo di preacquisizione il client versante (p.e. DPI) utilizza **Web Service** per coordinare il processo con il modulo PING, ma trasmette gli oggetti da conservare tramite protocollo **FTPS**, su un'opportuna area FTP, gestita dal server FTP di ParER. Fa eccezione il client interno a PING, che può versare anche on line, senza appoggiarsi su protocollo **FTP**.

[\[Torna al Sommario\]](#)

8.2.6 TPI

Il modulo software TPI (Tivoli Preservation Interface) gestisce la *memorizzazione* degli **Oggetti-dati** su supporti a cassette, operata utilizzando come sistema di gestione della **tape library** il software Tivoli.

TPI opera nel seguente modo:

- un job schedulato sul file server invia al sistema di gestione della **tape library** il comando di archiviazione delle cartelle in cui SacER ha depositato gli oggetti da archiviare, selezionate tramite opportuni criteri definiti in sede di amministrazione di sistema;
- il sistema di gestione della **tape library** provvede a leggere i file dalle cartelle e ad archivarli tramite le sue funzionalità di archiving nella **tape library**, dove rimangono in situazione **near-line**, cioè disponibili e raggiungibili nella **tape library**, senza necessità di reperire cassette da un magazzino;
- una volta che li ha archiviati, TPI provvede a cancellare i file dal **file system** su disco;
- l'allineamento tra sito primario e sito di **Disaster recovery** viene garantito da un job periodico schedulato sul file server del sito primario, che aggiorna automaticamente il **file system** del sito secondario. Il job invia al sito secondario i nuovi file pervenuti nel **file system**, senza replicare le cancellazioni effettuate in seguito all'archiviazione su cassetta;
- sul sito di **Disaster recovery**, in maniera indipendente da quanto avviene sul sito primario, ma con politiche analoghe, viene eseguito un job di archiviazione analogo a quello del sito primario, mantenendo così l'indipendenza tra i due siti per quanto riguarda l'archiviazione.

Le funzionalità di Archiviazione di SacER verificano lo stato degli Oggetti-dati nei due siti e lo registrano sul Data Base Oracle.

Presso il sito di **Disaster recovery** viene prodotta una seconda copia per ogni cassetta.

Le attività di gestione del sito di **Disaster recovery** sono tracciate in uno specifico Data Base del sistema di gestione della **tape library**.

[\[Torna al Sommario\]](#)

8.2.7 DIPS

Il modulo software DIPS (DIPSpenser), previo controllo dei diritti di accesso alle informazioni, consente di attivare ricerche sul Sistema e di soddisfare richieste relative agli oggetti conservati, anche quando le funzionalità di ricerca messe a disposizione dall'interfaccia web di SacER non riescono a soddisfare le particolari esigenze dell'*Utente*.

DIPS consente ricerche complesse sugli oggetti conservati sulla base delle **Informazioni descrittive** memorizzate dalle funzionalità di Gestione dati, e di ottenere l'*esibizione* dei documenti individuati dalla ricerca, sfruttando le funzionalità di Accesso di SacER. DIPS opera ricercando gli AIP da esibire, attraverso le **Informazioni descrittive** fornite dalle funzionalità di Gestione dati, e richiedendo gli AIP alle funzionalità di Archiviazione.

Il modulo DIPS consiste di un sistema generalizzato in grado di configurare tramite opportuna parametrizzazione i criteri da utilizzare nella ricerca e la presentazione dei risultati in ragione delle necessità e delle preferenze dei diversi utenti.

[\[Torna al Sommario\]](#)

8.2.8 SIAM

Il modulo software SIAM (SacER Identity and Access Management) consente di gestire l'autenticazione e la profilatura degli operatori. Tale profilatura viene utilizzata da SacER e dagli altri moduli software del Sistema per valutare a quali viste specifiche di dati e a quali attività ogni operatore abbia accesso, sulla base dei ruoli assegnati.

Per le funzionalità di autenticazione SIAM utilizza sistemi di **IdP** (Identity Provider); ParER mette a disposizione un proprio **IdP**, ma accetta anche l'autenticazione effettuata tramite SPID.

SIAM mantiene il Data Base degli operatori dell'**IdP** di ParER, nonché il Data Base dei profili di tutti gli operatori abilitati al Sistema, qualunque sia l'**IdP** su cui si sono autenticati, gestendo quindi in modo centralizzato la profilatura per tutti i moduli del Sistema.

La profilatura si spinge fino al livello delle singole attività previste dal Sistema (p.e. pressione di uno specifico bottone di una specifica videata) ed al livello elementare dei dati gestiti (**Struttura**, **Unità documentaria**, Registro, ecc.) tramite la definizione e la combinazione di opportuni ruoli.

L'**IdP** implementato da ParER colloquia con gli altri moduli del Sistema tramite standard SAML (Security Assertion Markup Language); l'utilizzo di SAML consente al *Sistema di conservazione* di accettare operatori autenticati su **SPID**.

[\[Torna al Sommario\]](#)

8.2.9 Sacerlog

Il modulo Sacerlog raccoglie e conserva nel sistema informazioni essenziali sul processo di conservazione in base al paradigma proposto da PREMIS, basato sui concetti di Agente (in generale l'utente collegato al sistema), Evento (p.e. "Inserimento" o "Cancellazione") e Oggetto (p.e. "Parametro di configurazione della **Struttura**").

In pratica, ogniqualvolta un agente scatena un evento che modifica un oggetto (inclusa la creazione dell'oggetto stesso), il sistema di log registra la fotografia dell'oggetto modificato e le informazioni essenziali sulla modifica (agente, evento, timestamp, ecc.).

Sacerlog è utilizzato anche per registrare nel log eventi di sola consultazione (ad es. "Visualizzazione dettaglio **Unità documentaria**"), di cui è necessario tenere traccia per ragioni di sicurezza.

Il sistema di log è completamente parametrabile tramite funzioni di amministrazione, che consentono di stabilire quali combinazioni di agenti / eventi / oggetti / debbano essere registrati nel log.

Il log può essere consultato da un utente che possiede le dovute abilitazioni per determinare la storia di quanto accaduto su un oggetto. Il log può essere anche consultato per esporre il contenuto dell'oggetto ad un qualunque istante di riferimento, determinando la fotografia dell'oggetto più recente rispetto all'istante di riferimento.

[\[Torna al Sommario\]](#)

8.2.10 Componenti di supporto

Completano il Sistema i vari moduli di supporto, ovvero le componenti che non implementano specifiche logiche applicative, ma mettono a disposizione funzionalità trasversali agli altri moduli. Più nello specifico:

- il time server della rete regionale tramite protocollo **NTP** distribuisce il *Riferimento temporale* all'interno dei **Data Center** con fuso orario Europe/Rome (GMT+1) e configurazione della variazione automatica dell'ora solare, allineandolo costantemente con l'orario dell'Istituto Elettrotecnico Nazionale Galileo Ferraris di Torino (ntp.ien.it), che è a disposizione di qualsiasi altro sistema che voglia mantenere l'orario allineato con i sistemi di ParER.
- il modulo di Audit e Log di sistema è costituito da un insieme eterogeneo di componenti che si occupano di raccogliere tutte le informazioni rilevanti sugli eventi accaduti durante la vita del sistema. Si tratta di informazioni sistemistiche (*log di sistema* operativo, del data base e degli application server), di sicurezza (accessi andati a buon fine e rifiutati), che vengono raccolte dai diversi strati tecnologici del Sistema con il supporto di componenti specifici, ivi incluso Sacerlog. Il modulo di Log si basa su un sistema **SIEM** (HP ArcSight) opportunamente configurato e alimentato, che si occupa di raccogliere i *log* e memorizzarli in conformità con le politiche definite da ParER sulla base della normativa vigente, con i disciplinari regionali in materia di sicurezza informatica e con la necessità di mantenere nel Sistema tutte le informazioni necessarie a documentare le attività svolte, anche per funzionalità di audit. Le informazioni memorizzate in ArcSight vengono analizzate continuamente in remoto dal Centro Operativo per la Sicurezza (**SOC**), utilizzando opportuni strumenti atti a individuare tempestivamente eventuali minacce per la sicurezza del servizio. Componenti di audit e log sono presenti anche nel sito di **Disaster recovery**;
- il modulo di Monitoraggio Tecnico è costituito da un insieme eterogeneo di componenti che si occupano di raccogliere in tempo reale le segnalazioni di possibili malfunzionamenti dell'infrastruttura e di segnalarle alla struttura della Regione Emilia-Romagna preposta alla gestione; allo scopo vengono utilizzati diversi software open source tra cui Zabbix, che viene alimentato da opportuni agenti software, e Graylog, che raccoglie temporaneamente i log dei sistemi e li indicizza, per agevolare la diagnostica delle problematiche applicative. Le informazioni di monitoraggio sono raccolte per analisi di periodo nel cruscotto realizzato tramite un'applicazione di **business intelligence** costruita con lo strumento open source SpagoBI. Componenti di monitoraggio tecnico sono presenti anche nel sito di **Disaster recovery**;
- il modulo di Request Tracking viene utilizzato per automatizzare e mantenere traccia dei processi fondamentali del servizio di conservazione: tra questi la gestione delle richieste di rilascio in produzione delle nuove versioni dell'applicativo e le richieste di manutenzione dell'infrastruttura; allo scopo viene utilizzato il software di **trouble ticket** della Regione Emilia-Romagna;

- i componenti di supporto allo sviluppo vengono utilizzati per garantire la corretta gestione degli sviluppi del software, per quanto riguarda sia l'evoluzione che la manutenzione correttiva del sistema; in generale si tratta di componenti open source normalmente utilizzati dai gruppi di sviluppo della Regione Emilia-Romagna sulla base di metodologie consolidate; tali componenti, oltre a facilitare lo sviluppo del software e a supportare la gestione dei progetti e delle risorse, consentono di tenere traccia di tutte le attività significative nell'ambito dello sviluppo, dal momento della definizione dei requisiti fino al momento della richiesta di rilascio, e delle relative evidenze documentali. La tracciatura del processo di sviluppo è supportata da un opportuno strumento open source (Redmine), su cui sono definiti diversi workflow in ragione della problematica di sviluppo da affrontare;
- il sito web di ParER espone in modo strutturato informazioni e documentazione utili sia ai *Produttori* che agli *Utenti* (**Comunità di riferimento**). Tali informazioni riguardano, ad esempio, le procedure amministrative di attivazione dei servizi di conservazione e le specifiche per effettuare i **versamenti** dei SIP. Inoltre, rende disponibili informazioni aggiornate sulla quantità dei Documenti conservati e sulle tematiche legate agli *archivi*, alla gestione documentale e alla conservazione degli oggetti digitali. Dal sito è possibile, inoltre, iscriversi alla newsletter settimanale con cui ParER tiene aggiornata la **Comunità di riferimento** sulle novità in materia di Conservazione;
- il sito interno di ParER gestisce in modo strutturato informazioni e documentazione a supporto del Sistema di Gestione Integrato (SGI) della Qualità e della Sicurezza, necessario per il conseguimento e il mantenimento delle certificazioni ISO sulla Sicurezza e sulla Qualità del servizio e delle iscrizioni al Cloud Market Place di AgID;
- SELF, sistema di e-Learning della Regione Emilia-Romagna, è il sistema che la Regione ha adottato per la diffusione dell'e-learning nelle proprie pratiche formative e in quelle di altri enti pubblici, cui SELF offre tecnologie, servizi, risorse didattiche e competenze nella gestione di corsi in e-learning. In particolare, per quanto riguarda ParER, SELF mette a disposizione corsi introduttivi e intermedi sul processo di Conservazione e risorse formative sulla gestione della privacy.

[\[Torna al Sommario\]](#)

8.3 Componenti fisiche

8.3.1 Schema generale

Dal punto di vista tecnico il sistema è progettato e realizzato in maniera da fornire un'elevata continuità di servizio, garantire l'*integrità* degli oggetti conservati, gestire grandi volumi di dati, mantenere performance stabili indipendentemente dai volumi di attività e assicurare la riservatezza degli accessi.

Il Sistema è sviluppato con tecnologie di larga diffusione open source o comunque di libero utilizzo, a parte i sistemi di memorizzazione di dati, per i quali si utilizzano prodotti proprietari, che dispongono però di interfacce standard de facto o de jure; in particolare il Data Base per ragioni di sicurezza e di performance è proprietario (Oracle), ma standard SQL, l'**Object Storage** (NetApp) è proprietario, ma adotta le specifiche pubbliche **S3**, mentre il sistema di gestione dello **storage** su cassetta (TSM) è fornito da IBM, fornitore della **tape library**.

Il diagramma in figura schematizza le principali componenti infrastrutturali del *Sistema di conservazione* di ParER e le principali relazioni con altri sistemi interessati dal *processo di conservazione* descritto nei capitoli precedenti del presente Manuale.

Il Sistema è realizzato su due siti che distano circa 100 chilometri l'uno dall'altro: un sito primario con caratteristiche di continuità operativa, installato presso il **Data Center** della Regione Emilia-Romagna a Bologna, che svolge funzioni di normale operatività, ed un sito secondario, installato presso il **Data Center** di Lepida s.c.p.a. a Parma, ma gestito per i sistemi di conservazione direttamente dalla Regione Emilia-Romagna che ha lo scopo di subentrare come sito di **Disaster recovery** nel caso di caduta irreparabile del sito primario.

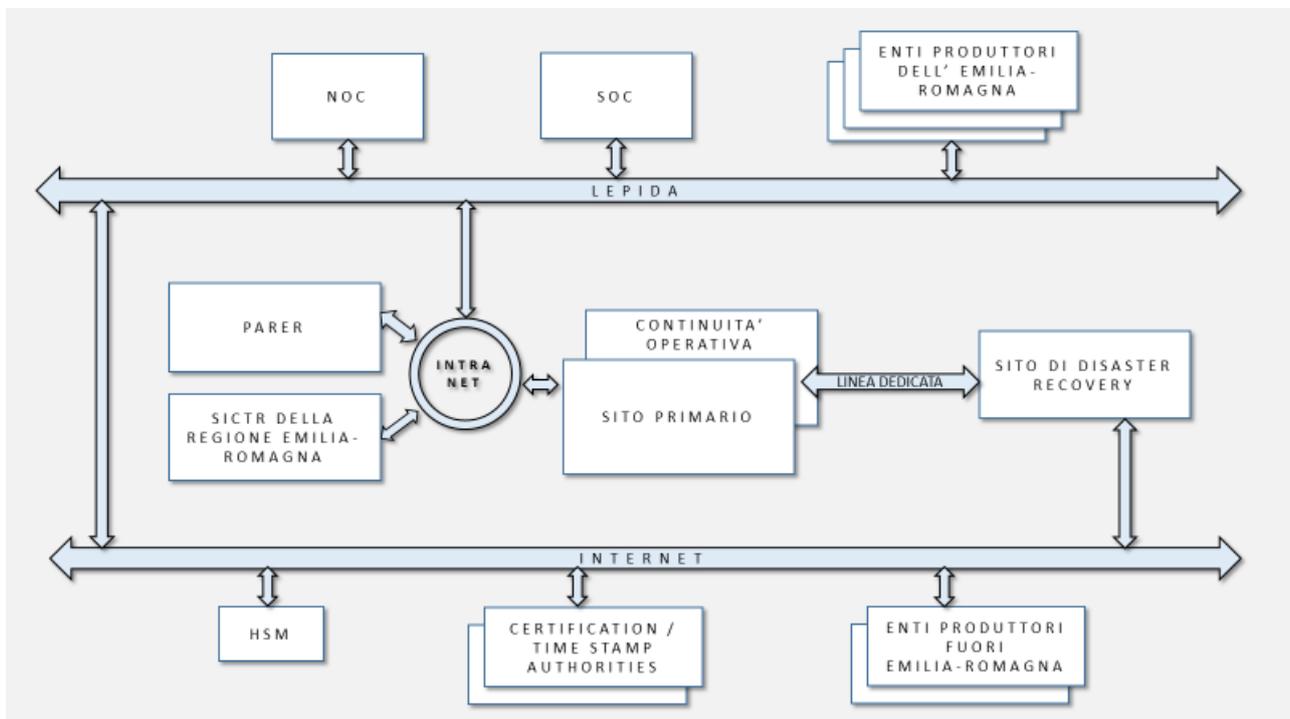


Figura 9 - Schema Infrastrutturale del Sistema di conservazione

Il sito primario e il sito di Parma sono gestiti dalla Regione Emilia-Romagna all'interno di una sottorete dell'Intranet regionale dedicata al *Sistema di conservazione*. Il collegamento tra i due siti è garantito da una linea dedicata in banda larga fornita da Lepida s.c.p.a.. Il sito di **Disaster recovery** viene reso accessibile via Internet solo nel momento in cui, a seguito di disastro, dovesse essere promosso a sito primario.

Il Sistema di conservazione, benché sia ospitato in data center di terzi, dispone di sotto reti proprie isolate dalle altre sotto reti.

Alcuni sistemi di supporto sono installati in una sotto rete del **data center** della Regione Emilia-Romagna; nello specifico si tratta dei log server, dei time server, dei server di monitoraggio, dei server che ospitano il sito web di ParER e dei **proxy** che gestiscono gli scambi con gli **HSM**. La comunicazione tra la sotto rete del *Sistema di conservazione* e la sotto rete generale della Regione Emilia-Romagna è limitata a protocolli e porte ben specifiche, in modo tale da garantire l'isolamento della porzione di rete del *Sistema di conservazione* dai rimanenti sistemi regionali. Gli **HSM** sono installati presso un fornitore esterno, aggiudicatario di gara per la gestione del servizio per la Regione Emilia-Romagna.

Presso un fornitore esterno aggiudicatario di apposita gara è allocato il Centro di Monitoraggio dell'Infrastruttura (**NOC**), che effettua il controllo continuo delle apparecchiature informatiche e dei server per tutti i sistemi della Regione Emilia-Romagna, e quindi anche di ParER (escluso il sito di DR).

Presso un altro fornitore esterno aggiudicatario di apposita gara è allocato il Centro Operativo per la Sicurezza (**SOC**), che fornisce i servizi di sicurezza per tutti i sistemi della Regione Emilia-Romagna, e quindi anche di ParER (escluso il sito di DR).

Il sito primario è costituito da due sotto-siti collegati in rete locale in due diversi edifici della Regione, che operano per garantire la **continuità operativa** del servizio.

Tutti i componenti del sito primario e del sito di continuità operativa e i componenti esterni sviluppati da ParER, nonché gli **HSM**, sono ridondati, mentre non lo sono i componenti del sito di **Disaster recovery**.

Il sistema interagisce con i *Produttori* dell'Emilia-Romagna tramite la rete regionale in banda larga **Lepida**, che è completamente ridondata; **Lepida** è a sua volta attestata su Internet con collegamenti in banda larga. In questo modo viene garantita tramite Internet una connessione ad alta velocità con i sistemi delle Certification / Time Stamp Authorities, con gli **HSM**, con i **provider di identità SPID** e con i *Produttori* che non appartengono all'Emilia-Romagna e che quindi non sono connessi a **Lepida**.

In situazione di normale funzionamento il Sistema è attivo solo sul sito primario con garanzia di **continuità operativa** anche nel caso di caduta di uno dei due sotto-siti; il sito di **Disaster recovery** si limita a replicare le informazioni del sito primario in maniera asincrona man mano che vengono generate e a compiere funzioni di **backup** gestite autonomamente e di **archiving** sotto il controllo del sito primario.

Nel sito primario in situazione di normale funzionamento il carico della maggior parte delle applicazioni è distribuito tra i due sotto-siti; nel caso di caduta di uno dei due sotto-siti, l'altro ancora attivo provvede a garantire la continuità del servizio, sia pure con performance ridotte, fino al ripristino della situazione normale. Nel caso di caduta irreparabile di ambedue i sotto-siti del sito primario non recuperabile nel breve periodo (disastro) il sito di **Disaster recovery** viene posto in stato di attività e attivato come destinatario del traffico di rete, con funzionalità ridotte fino al ripristino del sito primario.

Sia nel sito primario che nel sito di **Disaster recovery** sono presenti diverse istanze del Sistema:

- un'**istanza** di Produzione, cui è riservata la maggior parte delle risorse;
- un'**istanza** di Test, riservata al personale di ParER per il test delle nuove versioni rilasciate dai laboratori di sviluppo;
- un'**istanza** di Preproduzione, allineata all'**istanza** di produzione, per i test dei *Produttori*.

I sistemi di sviluppo risiedono presso il **Data Center** della Regione Emilia-Romagna.

La separazione delle istanze viene assicurata attraverso l'utilizzo di domini di rete distinti, che non sono visibili l'uno all'altro.

Nell'ambito di ciascuna istanza, il sistema utilizza una logica multi-Ente, assimilabile ad un sistema **multi-tenant**, intendendo con ciò un insieme di "aree" che, pur condividendo una medesima istanza applicativa, sono logicamente separate tra loro. Tale separazione è realizzata sia per quanto concerne gli accessi, sia per quanto concerne la conservazione dei dati.

[\[Torna al Sommario\]](#)

8.3.2 Caratteristiche tecniche dei Sistemi

Il diagramma in figura schematizza le principali componenti tecniche dei sistemi di ParER. I due sotto-siti del sito primario sono tra loro identici, tranne che per la presenza di una **tape library** di dimensioni ridotte in uno dei due siti, che svolge solamente funzioni di **Backup**; i sistemi del sito di **Disaster recovery** sono analoghi a quelli di un sotto-sito del sito primario, a parte la mancata ridondanza dei componenti e l'assenza del **proxy** per **HSM**.

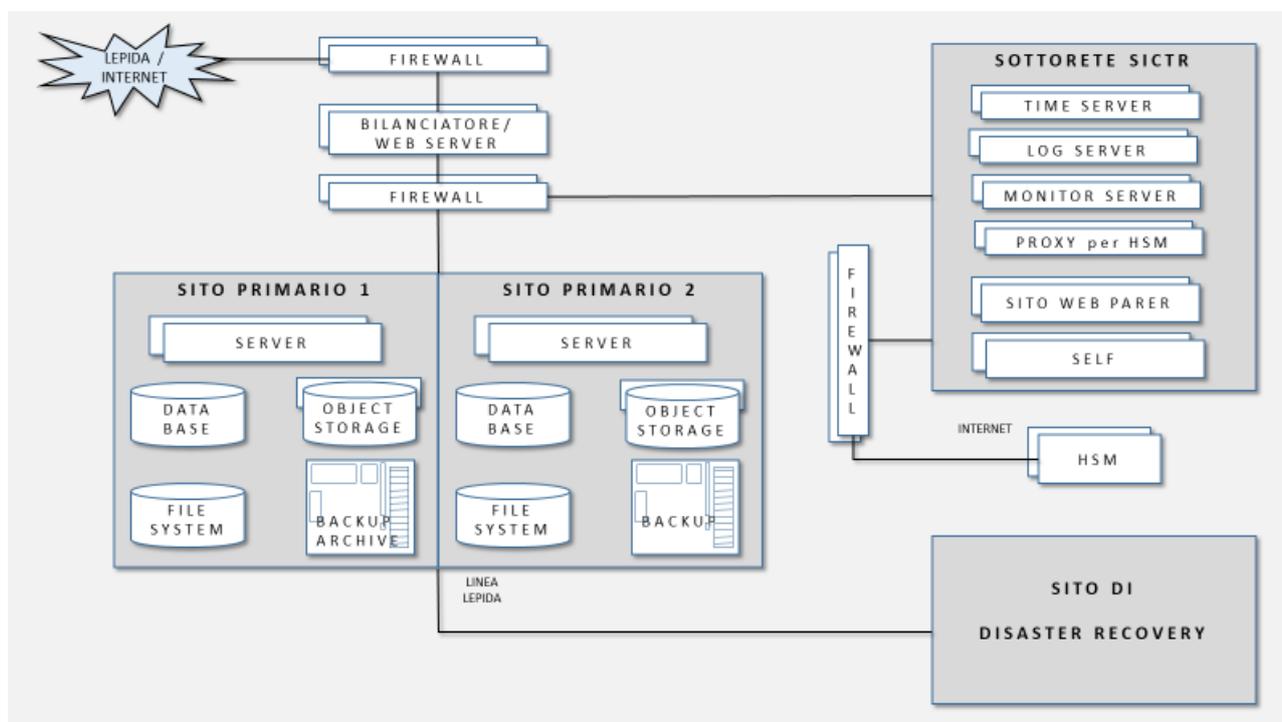


Figura 10 - Schema dei Sistemi di ParER

I servizi ausiliari, in quanto di interesse di tutta l'infrastruttura regionale, sono ospitati su server della sottorete della Regione Emilia-Romagna; tra questi fondamentale per il processo di conservazione è il time server della rete regionale tramite protocollo **NTP** distribuisce il *Riferimento temporale* all'interno dei **Data Center** con fuso orario Europe/Rome (GMT+1) e configurazione della variazione automatica dell'ora solare, allineandolo costantemente con l'orario dell'Istituto Elettrotecnico Nazionale Galileo Ferraris di Torino (ntp.ien.it).

Nell'ambito del sito primario i sistemi sono aggregati in **cluster**, mentre nel sito di **Disaster recovery**, in quanto non ridondato, non sono presenti cluster fisici di sistemi; sono però presenti cluster logici di Application server, in numero ridotto rispetto al sito primario, con lo scopo di distribuire il carico applicativo tra diversi sistemi.

Gli accessi al sistema avvengono esclusivamente passando da **firewall** tramite protocolli sicuri (**HTTPS** e **FTPS**).

Lo **storage** utilizza come supporti di memorizzazione sia dischi che nastri magnetici su cassetta.

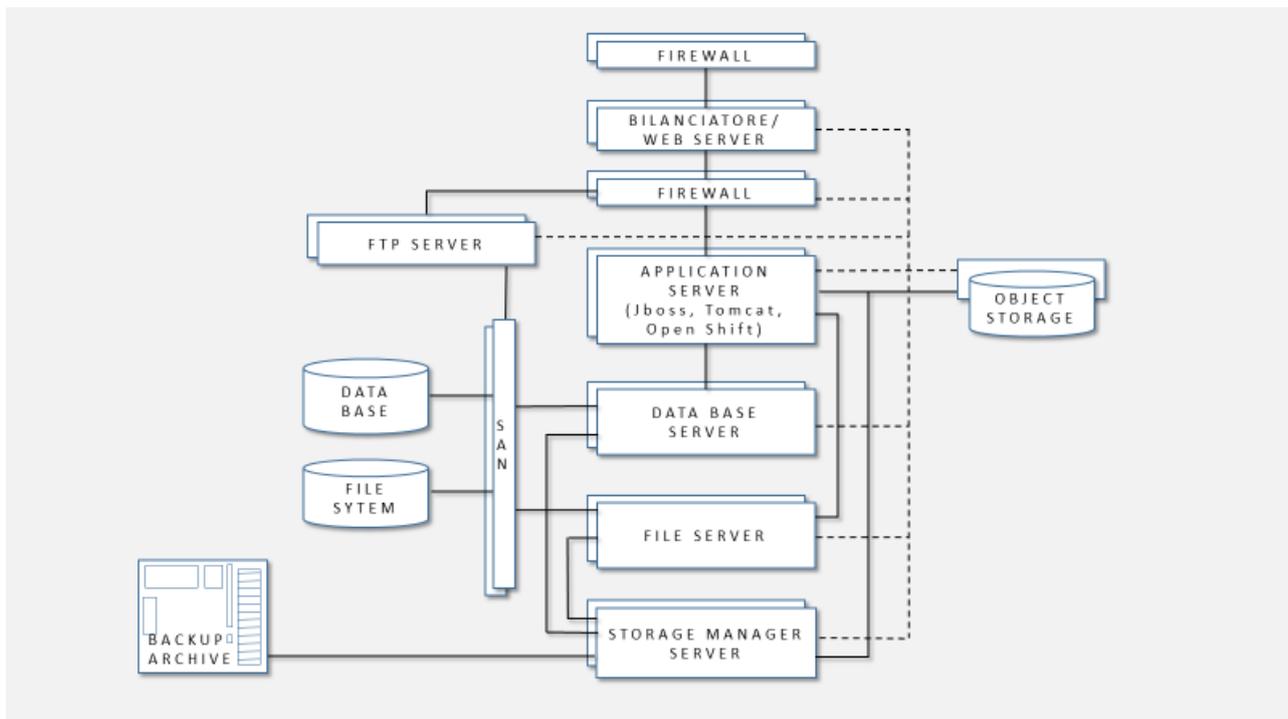


Figura 11 - Schema del Sito Primario

Lo **storage** su disco è suddiviso tra:

- **Data Base Oracle** per la *memorizzazione* dei metadati delle informazioni tipiche del processo di conservazione; viene utilizzato anche per memorizzare temporaneamente in forma di **BLOB** una parte degli **Oggetti-dati** dal momento del loro ingresso nel sistema fino al momento della loro conservazione definitiva nell'**Object storage**;
- **File system** per la *memorizzazione* temporanea degli **Oggetti-dati** che, in base alle politiche configurate nel sistema, verranno archiviati su cassette; il **file system** contiene inoltre tutti i file di servizio (log, configurazioni, ecc.) e un'Area **FTP** per il trasferimento ed il recupero asincrono degli **Oggetti-dati** da parte dei *Produttori*. Le aree temporanee vengono cancellate normalmente entro una settimana dopo l'utilizzo da opportune procedure applicative. Le aree utilizzate vengono sovrascritte continuamente e quindi i dati temporanei dopo un breve tempo non sono più accessibili.

Lo **storage** su disco è ospitato su uno storage array ed è costituito da un'area di storage primario con dischi ad alta velocità e da un'area di storage secondario con dischi a media velocità; in questo modo è possibile ottimizzare la distribuzione dei dati sui dischi in ragione delle necessità applicative.

La maggior parte degli **Oggetti-dati** conservati nel sistema risiede permanentemente all'interno di **appliance** dedicate alla gestione dell'**Object storage**, su cui vengono trasferite da un processo di elaborazione che li sposta dall'originaria posizione temporanea nel data base.

Lo **storage** su nastri magnetici si basa su un sistema a cassette (**tape library**), completamente governato da Tivoli Storage Manager (TSM), che gestisce cassette in standard **LTO6** su cui vengono mantenuti:

- in modalità **archiving**, in situazione **near-line** gli **Oggetti-dati** che non vengono mantenuti nell'**Object storage** (tipicamente quelli molto voluminosi e di accesso non frequente);

- in modalità di **backup**, i backup full ed incrementali e gli archive log del Data Base, immediatamente disponibili per qualsiasi attività di restore che si rendesse necessaria;
- in modalità di **backup** i file presenti nel **File system**.

Il Sistema è sviluppato in **Java** su sistemi operativi Linux (Red Hat) utilizzando i seguenti componenti principali:

- **Bilanciatore di carico LBL** (Oplon), che svolge anche il ruolo di Web server;
- **File Server** GlusterFS per la gestione del file system condiviso tra diversi server e delle aree **FTP**;
- **FTP server** in cluster;
- **Application server** JBoss Enterprise (Red Hat) in cluster logico gestito dai componenti di clustering di JBoss;
- **Servlet container** Tomcat (Apache) per i componenti che non richiedono l'utilizzo di un application server (p.e. TPI, DPI, Kettle server);
- Open Shift (Red Hat) come orchestratore dei container in cui vengono eseguiti i **Microservizi**;
- Data Base Oracle con utilizzo delle funzionalità di **RAC, di Data Guard** e di **partitioning**;
- **Object Storage** NetApp distribuito in replica su tre siti;
- Tivoli Storage Manager (IBM) con funzionalità di **Backup** e **Archiving** su **tape library**.

I moduli applicativi del Sistema, essendo sviluppati in **Java** secondo le specifiche **Java Platform Enterprise Edition (J2EE)**, sono raggruppati in diversi contesti applicativi caricati su JBoss. I moduli principali sono ognuno connesso ad un proprio schema di Data Base, in modo da garantire una buona modularità dell'applicativo. I componenti che non dispongono di proprio schema di Data Base utilizzano gli altri schemi, accedendo tramite **Web Service** appositamente ottimizzati per l'accesso ai dati, oppure tramite opportuni **grant**. I componenti applicativi che richiedono un'esecuzione fortemente dinamica sono invece sviluppati tramite **Microservizi** caricati in opportuni contenitori la cui gestione viene orchestrata da Open Shift.

Il colloquio tra il Sistema e gli applicativi esterni è effettuato tramite **Web Service**.

Il trasferimento dei dati sincrono è realizzato in **HTTPS** tramite tecnologie **ReST**, mentre il trasferimento asincrono utilizza tecnologie **FTPS**.

Il Sistema è Web-based e testato per diversi browser (Firefox, Explorer, Chrome). Non richiede l'installazione di alcun componente sul client.

Il **framework di sviluppo** utilizzato è stato derivato dal framework open source Spring, migliorandone gli aspetti di accessibilità; la **persistenza** è gestita tramite **EJB**, generati con la piattaforma Hibernate e solo in pochissimi casi particolari ben identificati e documentati tramite chiamate dirette JDBC, in modo da garantire portabilità verso altri Data Base relazionali e quindi facilitare il riuso dell'applicativo. Il sistema ingloba diverse librerie applicative open source, molte delle quali sviluppate nell'ambito di progetti internazionali, in particolare per la verifica delle firme e dei **formati**.

La replica dei dati sul sito di **Disaster recovery** è garantita da diverse tecnologie:

- il Data Base viene sincronizzato da Oracle tramite Data Guard con modalità di physical standby e maximum availability (il sito primario non attende la fine della scrittura del sito di **Disaster recovery** per considerare chiusa la transazione);
- l'**Object storage** viene replicato nei diversi siti dalle tecnologie intrinseche di NetApp;

- il file system su disco viene allineato tramite **SCP**;
- l'archivio su cassette viene mantenuto aggiornato da TSM in maniera indipendente tra i due siti tramite opportune politiche di schedulazione; l'applicativo controlla periodicamente la corretta sincronizzazione dei file system e degli archivi su cassette tra i due siti.

Nel caso di dismissione di dispositivi elettronici di memorizzazione dei dati l'Area Infrastrutture e sicurezza regionale si occupa di garantire la cancellazione sicura delle informazioni presenti nel sistema, in base alle politiche e alle procedure di sicurezza della Regione Emilia-Romagna.

[\[Torna al Sommario\]](#)

8.4 Procedure di gestione e di evoluzione

La gestione del *Sistema di conservazione* è affidata a diversi gruppi di operatori, secondo la natura delle attività da svolgere; tali attività includono la gestione operativa del sistema in esercizio, l'avviamento di nuovi enti e di nuovi servizi di conservazione e le eventuali successive modifiche, l'evoluzione dell'infrastruttura e dell'applicativo, e infine la gestione dei malfunzionamenti e degli incidenti di sicurezza.

[\[Torna al Sommario\]](#)

8.4.1 Gestione dell'Esercizio

Per quanto attiene alla gestione operativa del sistema in esercizio, l'Unità Servizi di Conservazione Digitale di ParER presidia le attività descritte nello specifico punto del paragrafo 5.2.

L'Area Infrastrutture e sicurezza presidia parallelamente l'operatività quotidiana dell'infrastruttura hardware e software sottostante il *Sistema di conservazione*, nonché la pianificazione ed il controllo delle attività straordinarie che possono avere impatto sull'esercizio, come descritto allo specifico punto del paragrafo 5.2, oltre a quelle dettagliate nel paragrafo 9.2; l'attività dell'Area citata copre sia il sito primario, incluso il sito di **Continuità Operativa**, sia l'infrastruttura di **Disaster Recovery**.

[\[Torna al Sommario\]](#)

8.4.2 Gestione delle utenze

La procedura riportata nel documento "Gestione utenze" descrive le modalità con cui viene garantita la corretta gestione dei soggetti che hanno accesso al sistema di conservazione tramite i suoi moduli applicativi (vedi il paragrafo 8.2), con particolare riguardo alla sicurezza dei dati e delle informazioni conservate, nel rispetto della politica generale di controllo degli accessi di SID.

La procedura descrive inoltre il metodo seguito per la gestione delle password in coerenza con quanto descritto nella *Politica sulla sicurezza SID*.

La richiesta dell'attivazione, della modifica del profilo o della cessazione di un'utenza è effettuata per vie formali dall'Ente di appartenenza dell'*Utente*.

Se l'autenticazione avviene tramite **SPID**, la gestione della password è affidata al provider dell'identità SPID; se invece avviene tramite l'**IDP** di ParER, è affidata a personale di ParER specificamente formato al rispetto delle procedure di sicurezza, in particolare a quelle definite per la gestione delle utenze.

Le password gestite dall'**IDP** di ParER sono conservate nel Sistema crittografate e non sono accessibili al personale, nemmeno se dotato di privilegi amministrativi.

Periodicamente ParER effettua un controllo delle utenze attive nel *sistema di Conservazione* e delle relative profilature, con il coinvolgimento degli Enti che ne hanno richiesto l'attivazione, al fine di mantenere pulito l'archivio gestito da SIAM (vedi paragrafo 8.2.8).

Il sistema di gestione delle autenticazioni viene costantemente aggiornato in base alle direttive regionali in termini di sicurezza informatica e alle risultanze dei processi di certificazione per la sicurezza e di qualificazione nel Cloud Market Place di AgID.

[\[Torna al Sommario\]](#)

8.4.3 Gestione dei Malfunzionamenti

La procedura riportata nel documento "Gestione delle Richieste di Informazioni, Reclami e Segnalazioni" descrive la maniera in cui ParER tratta le richieste di informazioni, i malfunzionamenti e gli eventuali reclami da parte degli *Utenti* del sistema.

La gestione dei malfunzionamenti può coinvolgere diverse strutture di SID, secondo la natura del malfunzionamento stesso, che può essere rilevato da diverse fonti: malfunzionamenti di natura applicativa possono essere segnalati dagli Enti *Produttori, dagli Enti Conservatori e dagli Enti Gestori*, dall'Unità Servizi di Conservazione Digitale, dalla Funzione Archivistica di Conservazione di ParER o dall'Unità Sistemi di Conservazione, mentre malfunzionamenti di natura tecnica possono essere segnalati dal dall'Area Infrastrutture e sicurezza.

Allo stesso modo diverse possono essere le strutture che intervengono nella soluzione del malfunzionamento: l'Unità Servizi di Conservazione Digitale è normalmente in grado di risolvere i malfunzionamenti che non sono dovuti a problemi tecnici, eventualmente coinvolgendo l'Ente che ha rilevato il malfunzionamento e per suo tramite i suoi fornitori di servizi; i malfunzionamenti di natura infrastrutturale vengono risolti dall'Area Infrastrutture, e sicurezza; l'Unità sistemi di conservazione viene coinvolta nel caso in cui si sia verificato un malfunzionamento del software applicativo; in questo caso si attivano le procedure di manutenzione, che sono descritte nei successivi paragrafi.

[\[Torna al Sommario\]](#)

8.4.4 Gestione degli Incidenti di Sicurezza

Tutte le aree organizzative coinvolte nel sistema di conservazione, con il supporto del **SOC**, sono sistematicamente coinvolte nelle attività di prevenzione e di risoluzione degli incidenti di sicurezza, secondo le politiche definite nella *Politica sulla sicurezza SID*.

La procedura riportata nel documento "Gestione incidenti" descrive le modalità con cui vengono gestiti gli eventi che possono avere un impatto sui requisiti di *integrità, disponibilità e riservatezza* dei dati conservati o del Servizio di conservazione.

L'obiettivo della procedura viene raggiunto attraverso le seguenti attività:

- Preparazione;
- Rilevazione e Analisi;
- Contenimento, Rimozione e Ripristino;
- Attività post-incidente.

ParER ha definito le responsabilità nell'ambito della gestione degli incidenti di sicurezza.

In particolare,

- gli Enti in accordo hanno l'obbligo di notificare tempestivamente a ParER (alla casella helpdeskParER@Regione.Emilia-Romagna.it) gli **Incidenti di sicurezza (compresi i Data Breach)** di qualsiasi natura, che coinvolgono il Sistema di conservazione, al fine di garantire l'applicazione delle contromisure adeguate. Le notifiche devono essere effettuate sulla base delle regole definite di seguito.
- ParER ha l'obbligo di
 - gestire gli incidenti di sicurezza, garantendone la tracciatura e l'applicazione di soluzioni adeguate alla riduzione degli impatti con il supporto dell'Area Infrastrutture e sicurezza;
 - notificare tempestivamente agli Enti in accordo un'incidente di sicurezza di qualsiasi natura, che coinvolga l'ambito di titolarità dell'Ente. Le notifiche devono essere effettuate sulla base delle regole definite di seguito.

Le notifiche devono essere effettuate via e-mail e contenere almeno le seguenti informazioni:

- data/ora e modalità attraverso le quali si è venuti a conoscenza dell'evento.
- causa, sistemi coinvolti, eventuali disservizi causati, utenti coinvolti, dettagli tecnici rilevanti.
- data/ora e azioni intraprese per contenere i danni causati dall'incidente e per ripristinare i sistemi
- considerazioni sull'incidente, suggerimenti, adeguamenti da effettuare.

Nel caso in cui tutte le informazioni sopraindicate non siano immediatamente disponibili, queste saranno comunicate nel corso della gestione dell'incidente.

A fronte della richiesta da parte dell'Ente impattato da un eventuale incidente, ParER può condividere eventuali evidenze digitali o altre informazioni dopo la chiusura dell'incidente stesso attraverso opportuni canali di comunicazione.

[\[Torna al Sommario\]](#)

8.4.5 Evoluzione pianificata

L'evoluzione pianificata del Servizio di Conservazione segue le linee guida formulate dal Responsabile del Servizio di Conservazione, che ne stabilisce politiche, priorità e tempistiche; l'evoluzione è inquadrata nell'ambito di un piano annuale, rivisto semestralmente e articolato in progetti, ed è monitorata tramite Stati di Avanzamento Lavori (SAL) periodici, cui partecipano diversi soggetti in ragione dei diversi argomenti trattati. In particolare, si tengono SAL per l'evoluzione degli aspetti operativi del servizio, cui partecipano gli addetti alla Unità Servizi di Conservazione Digitale, SAL per l'evoluzione degli applicativi, cui partecipano, oltre ai responsabili di ParER, i responsabili dei fornitori dello sviluppo. I progetti sono gestiti tramite una pianificazione di dettaglio, che fissa tempi di realizzazione ed impiego delle risorse, con il supporto, ove applicabile, di un opportuno strumento di gestione (Redmine).

L'evoluzione dell'infrastruttura è gestita dall'Area Infrastrutture e sicurezza, in accordo con il Responsabile del Servizio di Conservazione, secondo le politiche e le procedure della Regione Emilia-Romagna.

[\[Torna al Sommario\]](#)

8.4.6 Richieste di Cambiamento

All'evoluzione pianificata si affiancano evoluzioni derivanti dalle necessità di migliorare l'operatività dell'esercizio, e, soprattutto per quanto riguarda il software applicativo, dalla necessità di correggere eventuali errori o imperfezioni del sistema; tali necessità vengono formalizzate come Richieste di Cambiamento, la cui gestione è descritta in dettaglio nel documento "Gestione richieste di cambiamento del Servizio di conservazione".

Le richieste di cambiamento riguardano sia cambiamenti di tipo applicativo, che infrastrutturale e di configurazione. Per ogni ambito esiste un responsabile di riferimento, che costituisce il punto di raccolta delle richieste / esigenze che emergono nelle funzioni di competenza. Le richieste di cambiamento vengono valutate prima di essere autorizzate; se autorizzate, ottengono una priorità di realizzazione e vengono pianificate nell'ambito della pianificazione generale dei lavori, qualora non abbiano alta criticità; se invece rivestono carattere d'urgenza, ottengono priorità massima e risorse dedicate, fino alla soluzione; la pianificazione generale riserva normalmente una quota delle risorse per le attività correttive urgenti.

Il monitoraggio della realizzazione dei cambiamenti di una certa entità e la valutazione degli esiti è normalmente discusso nei SAL; i cambiamenti realizzati sono comunicati dai Responsabili al personale del ParER ed eventualmente agli altri soggetti coinvolti nel servizio di conservazione.

Se la richiesta di cambiamento riguarda le componenti applicative del sistema, viene attivato il processo di sviluppo del software, dalla definizione dei requisiti fino al rilascio in produzione, come descritto nei prossimi paragrafi.

La procedura di evoluzione è più snella nel caso di interventi evolutivi di minore rilevanza, quali correzioni di errori e piccole migliorie, che non richiedono la definizione di requisiti e la verifica di compatibilità tecnica; anche il test di accettazione in generale in questi casi risulta notevolmente semplificato.

ParER comunica tempestivamente agli Enti i cambiamenti che hanno impatto sul Servizio.

In particolare:

- modifiche all'infrastruttura di erogazione,
- modifiche dei referenti del Servizio,
- modifiche al processo di conservazione,

sono comunicate tramite pubblicazione sul sito web di ParER e sulla pagina dei conservatori accreditati di AgID, mentre il rilascio di nuove funzionalità viene comunicato tramite la pubblicazione delle informazioni sulle nuove **release** sul sistema di conservazione.

[\[Torna al Sommario\]](#)

8.4.7 Progettazione e Realizzazione di Software Applicativo

La procedura riportata nel documento "Progettazione e realizzazione di software applicativo del Servizio di Conservazione" descrive le modalità con cui vengono garantiti lo sviluppo del software e l'esecuzione dei test preliminari al rilascio in produzione, in accordo con tempi, risorse e modalità attuative concordate nel piano delle attività, assicurando l'allineamento con le esigenze espresse e coordinandosi con i fornitori coinvolti.

La procedura inizia con la definizione dei requisiti in accordo con l'Unità Sistemi di Conservazione, e procede poi con il test di integrazione effettuato dagli analisti funzionali e dagli analisti informatici della soluzione realizzata. Il superamento del test di integrazione produce una nuova **release**, che viene deployata in ambiente di Test.

I test della nuova **release** vengono condotti nell'ambiente di Test sulla base del piano di test sotto responsabilità dell'Unità Sistemi di Conservazione con il supporto dell'Unità Servizi di Conservazione Digitale. Questi test analizzano i comportamenti globali del sistema che non è possibile osservare in riferimento al singolo modulo o componente e coprono l'intera gamma delle caratteristiche da testare (test funzionali, test di performance, test di interfaccia, test di affidabilità, test di stress, test di sicurezza).

Le diverse attività prevedono un continuo scambio di informazioni tra le diverse aree e i diversi ambiti di ParER, in particolare tra gli addetti allo sviluppo del sistema di conservazione e il personale che esercita l'Unità Servizi di Conservazione Digitale, coinvolgendo, se necessario, l'Area Infrastrutture e sicurezza, al fine di garantire la coerenza tra i requisiti (funzionali, di sicurezza e di esercibilità) e quanto sviluppato.

Lo sviluppo del software applicativo segue le linee guida fissate dalla Regione Emilia-Romagna per lo sviluppo sicuro e le raccomandazioni degli standard di riferimento internazionali; i dettagli in merito sono riportati nel *Piano della Sicurezza* di ParER.

Lo sviluppo è supportato da strumenti di gestione dello sviluppo e di versioning del codice secondo gli standard definiti dai Sistemi Informativi della Regione Emilia-Romagna.

La tracciatura del processo di sviluppo è supportata da un opportuno strumento (Redmine), su cui sono definiti diversi workflow in ragione della problematica di sviluppo da affrontare.

Al termine del processo di sviluppo il software applicativo viene rilasciato come nuova **release** eventualmente deployabile in pre-produzione e produzione; il contenuto della nuova release è documentato all'interno delle Release Notes, ricavabili da Redmine.

[\[Torna al Sommario\]](#)

8.4.8 Gestione dei Rilasci

Prima di effettuare il rilascio in riproduzione e produzione, l'Unità Sistemi di Conservazione verifica tramite sistemi automatici e controlli manuali l'eventuale obsolescenza delle librerie di componenti utilizzate nella produzione della nuova **release**; qualora si rilevino criticità nell'ambito della sicurezza o rischi di malfunzionamenti, la nuova release non viene rilasciata, ma rimandata agli sviluppatori per l'aggiornamento dei componenti obsoleti e un nuovo system test. Se non si rilevano problemi bloccanti, l'Unità Sistemi di Conservazione concorda con l'Area Infrastrutture e sicurezza e con l'Unità Servizi di Conservazione Digitale il piano di rilascio della nuova **release** nell'ambiente di riproduzione e successivamente nell'ambiente di produzione, e richiede all'Area Infrastrutture e sicurezza di effettuare il rilascio.

La procedura di rilascio di una nuova **release** è illustrata in figura e descritta in dettaglio nel documento "Gestione dei Rilasci del Servizio di conservazione".

L'obiettivo del processo di Gestione dei rilasci viene raggiunto attraverso le seguenti attività:

- pianificare i rilasci relativi a nuove soluzioni nei diversi ambienti precedenti al passaggio in esercizio, in accordo con tempi, finestre temporali predefinite, risorse e modalità attuative concordate;
- definire e pianificare le eventuali attività formative (per utenti, personale interno) che devono accompagnare il rilascio in esercizio;
- verificare che il rilascio non abbia avuto impatti negativi sull'esercizio, e nel caso risolverli;
- coordinare i rilasci in esercizio delle nuove funzionalità, mantenendo il coordinamento e la verifica delle attività in carico all'Area Infrastrutture e sicurezza e garantendo il rispetto dei tempi pianificati.

L'Area Infrastrutture e sicurezza regionale tramite una procedura automatica provvede inoltre a installare nel sito di **Disaster recovery** la nuova **release**, da attivare nel caso di dichiarazione di disastro.

[\[Torna al Sommario\]](#)

8.4.9 Gestione e conservazione dei Log

Tutti i log di sistema, qualunque sia lo strumento che li genera, vengono raccolti nel **SIEM** (ArcSight) della Regione Emilia-Romagna, dove possono essere analizzati da personale dotato delle opportune autorizzazioni, secondo quanto definito nei disciplinari regionali in materia; inoltre sono continuamente verificati dal Centro Operativo per la Sicurezza (**SOC**) nell'ambito delle attività di prevenzione e controllo delle minacce informatiche.

In base alle politiche regionali, periodicamente i log più vecchi di un anno vengono cancellati automaticamente dal sistema, sotto controllo del personale dell'Area Infrastrutture e sicurezza, in quanto si ritiene che dopo tale periodo di tempo abbiano esaurito la loro utilità.

I log sono accessibili secondo necessità solo a personale tecnico esplicitamente incaricato a tale scopo dal Responsabile del Servizio.

Su richiesta motivata dell'Ente, i Log sono resi disponibili per la consultazione, limitatamente alle informazioni di pertinenza dell'Ente.

[\[Torna al Sommario\]](#)

8.5 Asset

Ai fini dell'erogazione del Servizio di conservazione sono state classificate le seguenti **tipologie di asset**:

Tipo di asset	Descrizione	Responsabile	Tipologia di dati
ASSET INFORMATIVI	pacchetti informativi versati in conservazione (SIP)	Ente produttore proprietari degli Archivi	Dati dei Produttore
	pacchetti informativi generati dal processo di conservazione (AIP e DIP)	Ente Conservatore	Dati Derivati
	evidenze di funzionamento del sistema di conservazione (log)	RER (SID)	Dati Derivati
	dati del SGI, dati di progettazione	RER (SID)	Dati di RER SID
	codice software e dati di configurazione sistemi	RER (SID)	N.A.
ASSET INFRASTRUTTURALI	asset relativi all'infrastruttura principale	RER (SID)	N.A.
	asset relativi al Servizio di DR	RER (SID)	N.A.
PERSONALE	personale archivistico, personale tecnico	RER	Dipendenti di RER /Fornitori esterni

9 MONITORAGGIO E CONTROLLI

9.1 Procedure di monitoraggio

Oltre alle funzionalità di monitoraggio applicativo gestite dal personale di ParER, che sono state illustrate al paragrafo 7.4.1, sono attive procedure di monitoraggio tecnico gestite dal personale dell'Area Infrastrutture e sicurezza, coerentemente con quanto definito nelle politiche e nei disciplinari regionali.

[\[Torna al Sommario\]](#)

9.2 Funzionalità per la verifica e il mantenimento dell'integrità e della consistenza degli archivi

Le procedure di monitoraggio citate nel paragrafo precedente, le politiche di conservazione dei **backup** e le caratteristiche delle tecnologie utilizzate garantiscono la completa *integrità* di quanto archiviato in SacER, ovvero di quanto depositato nel Data Base, nell'object storage e negli archivi su cassetta, una volta che sia stato duplicato nel sito di **Disaster recovery** e salvato tramite opportuno **backup** sia nel sito primario che nel sito di **Disaster recovery**.

Le funzionalità messe a disposizione per realizzare le componenti logiche di Archiviazione e di Gestione dei dati consentono:

- la manutenzione e l'amministrazione del Data Base, che contiene tutti i metadati trattati nel Sistema. La gestione sistemistica del Data Base è effettuata dall'Area Infrastrutture e sicurezza tramite prodotti certificati da Oracle, ed è tracciata nel *log di sistema*. Il Data Base fornisce periodicamente informazioni statistiche utili a valutarne il dimensionamento e le performance, e quindi a pianificare attività di manutenzione del Data Base stesso e degli applicativi che lo utilizzano;
- il controllo dell'*integrità* del Data Base, che avviene utilizzando funzionalità native del Data Base stesso. Le funzionalità di **Data Guard** del Data Base assicurano la replica del Data Base nel sito di **Continuità operativa** (in maximum security) e di **Disaster recovery** (in maximum availability), mentre le funzionalità di Recovery Management consentono **backup** del Data Base completi e incrementali, a caldo e a freddo, secondo le politiche di sicurezza descritte nel Piano della Sicurezza
- la manutenzione e l'amministrazione dell'**object storage**, che contiene tutti i **Componenti** (files) conservati nel Sistema, a parte i file memorizzati temporaneamente nel **file system** e definitivamente nello storage a cassette. Tale attività è effettuata dall'Area Infrastrutture e sicurezza tramite prodotti certificati da NetApp, ed è tracciata nel *log di sistema*. L'object storage fornisce periodicamente informazioni statistiche utili a valutarne il dimensionamento e le performance, e quindi a pianificarne le attività di manutenzione del Data Base stesso e degli applicativi che lo utilizzano;
- la congruenza delle copie dei file nei diversi siti in cui è installato l'**object storage**. La congruenza è garantita dalle caratteristiche intrinseche dell'object storage, che vengono opportunamente utilizzate dagli applicativi. Allo stesso modo è garantita dalle specifiche

dell'object storage la possibilità di aggiungere ulteriori nodi anche in altri siti, per aumentare il numero delle copie dei documenti;

- la manutenzione e l'amministrazione ai **Componenti** memorizzati su storage a cassette, che è effettuata dall'Area Infrastrutture e sicurezza tramite prodotti certificati da IBM, ed è tracciata nel *log di sistema*;
- l'integrità dei **Componenti** memorizzati su storage a cassette, L'integrità nel singolo sito è garantita dalle funzionalità intrinseche del modulo di archiving di TSM per tutti i dati archiviati su cassetta; queste funzionalità includono tra l'altro il controllo ed il riversamento periodico dei dati archiviati su nuove cassette; la congruenza tra il sito primario e il sito di **Disaster recovery** è invece garantita dalle logiche applicative implementate nel modulo TPI.

Per quanto riguarda l'integrità del contenuto informativo delle **Unità Documentarie** e in particolare dei **Componenti**, essa è garantita dal mantenimento delle impronte dei file per tutta la vita dei pacchetti informativi.

Esistono nel sistema diversi momenti in cui le impronte vengono verificate dopo il versamento, come ad esempio la creazione dell'AIP e lo copia del file dal **Blob** del Data Base all'**object storage**.

Inoltre, il Sistema implementa specifica funzionalità per verificare periodicamente la consistenza degli archivi conservati, controllando che tutti gli oggetti trasmessi nel Sistema nei pacchetti di versamento siano correttamente conservati negli AIP o in elaborazione per essere inseriti in nuovi AIP o negli aggiornamenti degli AIP esistenti.

Qualora, nonostante le garanzie fornite dalle tecnologie impiegate, si verificassero anomalie nell'*integrità* degli archivi, sono previste le opportune procedure applicative di ripristino illustrate nel paragrafo seguente; tali procedure sono rese possibili dalle politiche di gestione dei **backup**, che garantiscono la manutenzione di copie integre degli archivi fino a superamento delle verifiche di *integrità* a ad adozione di procedure di ripristino.

Non sono considerati facenti parte del Sistema, e quindi non fruiscono della stessa garanzia di *integrità*, i dati in ingresso presenti su aree temporanee (spazi FTP, **file system** del DPI, ecc.), per i quali le procedure di soluzione di cui al paragrafo seguente prevedono la ritrasmissione nel caso di anomalie.

Il *Piano della Sicurezza* di ParER descrive le modalità con cui ParER assicura gli obiettivi di sicurezza richiesti per la conservazione a lungo termine degli archivi, dettagliando i controlli di sicurezza delle diverse componenti del sistema (organizzazione, accessi, infrastruttura, gestione dell'esercizio, gestione dello sviluppo) e le procedure adottate per garantire i back up degli archivi e il **Disaster recovery**.

[\[Torna al Sommario\]](#)

9.3 Soluzioni adottate in caso di anomalie

Le anomalie vengono affrontate con diverse metodologie, secondo la natura dell'anomalia stessa e la collocazione dell'evento che le ha generate nel *processo di conservazione*; quindi, oltre alle procedure atte a garantire l'*integrità* e la consistenza degli archivi, nel senso indicato al paragrafo

precedente, esistono anche procedure atte a risolvere anomalie in altre componenti del sistema che registrano dati in SacER. Qui di seguito si trattano esclusivamente le anomalie di origine tecnica, in quanto il trattamento delle anomalie verificatesi nel processo di versamento è già stato descritto precedentemente nel paragrafo 7.4.2

Le caratteristiche comuni e le specificità delle procedure di risoluzione delle anomalie dipendono da diversi fattori organizzativi e tecnologici; in particolare:

- tutte le funzionalità del sistema che inseriscono o modificano dati nel Data Base e file nell'area FTP o nel **File System** operano in modalità transazionale;
- il **backup** del Data Base assicura il restore all'ultima transazione completata correttamente;
- la distribuzione delle copie dell'**object storage** sui diversi nodi ove necessario è verificata per via applicativa;
- del **File System** del DPI non viene effettuato backup;
- dell'Area **FTP** non viene effettuato backup;
- il **File System** di SacER è sottoposto a **backup** full a caldo con frequenza settimanale.

Non è quindi possibile far fronte a tutte le possibili anomalie con le stesse procedure, ma sono necessarie procedure specifiche secondo la natura dell'anomalia stessa.

La tabella seguente illustra le misure adottate per risolvere eventuali anomalie, classificate in ragione della collocazione delle informazioni nell'ambito del sistema nel momento in cui si è verificata l'anomalia:

Ambito del sistema	Misure adottate
File System del DPI	Si richiede la ritrasmissione dei SIP, sulla base dell'elenco fornito dalla funzione 'Recupero Studi' del DPI
Area FTP	Si eseguono opportune procedure di quadratura sia in DPI che in PING, guidati da informazioni ottenute tramite un'opportuna interrogazione del Data Base di PING; in caso si evidenzino perdite, i file perduti debbono essere ritrasmessi dal <i>Produttore</i>
Data Base	Si effettua la restore tramite le funzioni standard di Oracle dal sito primario o dal sito di Disaster recovery (nel caso di indisponibilità del DB primario)
Object Storage	Si effettua un controllo di congruenza tra Data Base e Object Storage per via applicativa, e si procede poi al recupero dei Componenti ancora presenti nei Blob temporanei del Data Base
File System di SacER	Si effettua la restore tramite le funzioni standard del file server per tutti i file inseriti nel file system fino all'ultimo back up; per i file inseriti successivamente all'ultimo back up si eseguono opportune procedure di quadratura tra Data Base e file system , che provvedono a riportare il sistema in stato di congruenza. Le procedure di recupero vengono eseguite sia sul sito primario che sul secondario.
Data Base del TSM	Si effettua la restore tramite le funzioni standard di DB2 (Data Base di TSM)

[\[Torna al Sommario\]](#)

9.4 Verifica periodica di conformità a normativa e standard di riferimento

Il Responsabile della Funzione Archivistica di Conservazione partecipa attivamente e regolarmente alle iniziative locali e nazionali sulla conservazione digitale e in particolare ai tavoli promossi in materia da AgID e dal MiC.

Qualora siano emerse problematiche significative, provvede a diffonderle all'interno di ParER e, se lo ritiene necessario, con il supporto dell'Unità Servizi di Conservazione Digitale, anche tra gli altri attori della procedura di conservazione.

Le notizie di maggior interesse vengono anche pubblicate sul sito web di ParER.

[\[Torna al Sommario\]](#)

9.5 Audit e gestione delle Non Conformità

ParER effettua periodicamente audit interni sul suo Sistema di Gestione Integrato (SGI), per verificare l'efficacia di policy, procedure e documenti nel rispetto dei requisiti di:

- ISO9001
- ISO27001 con le estensioni ISO27017 e ISO27018
- ISO 37001
- Qualificazione nel Cloud Market Place di AgID.

Gli audit interni costituiscono momento fondamentale per il conseguimento e il mantenimento delle certificazioni ISO e della qualificazione.

ParER si impegna a fornire su richiesta dei propri Enti in accordo (Produttori, Conservatori, Gestori) copia aggiornata delle certificazioni conseguite e della relativa documentazione.

Inoltre, ParER garantisce la disponibilità agli audit sia da parte di Organi di vigilanza sia da parte degli Enti in accordo.

La procedura riportata nel documento "Gestione Audit" e schematizzata in figura descrive l'insieme di attività e responsabilità legate alla pianificazione, conduzione e documentazione degli Audit del SGI.

Le eventuali non conformità rilevate nei processi di audit vengono gestite seguendo la procedura descritto nel documento "Gestione delle Non Conformità".

Lo scopo della procedura è fornire indicazioni operative per la gestione delle non conformità effettive o potenziali che, verificandosi, inficiano il buon andamento operativo del Servizio di conservazione e per l'attuazione di azioni volte a eliminare le cause delle non conformità stesse.

[\[Torna al Sommario\]](#)

9.6 Controlli di sicurezza

ParER dedica particolare attenzione alla sicurezza del sistema informativo utilizzato nell'ambito del *servizio di conservazione*. Le politiche e gli strumenti adottati a protezione del sistema in esercizio sono descritte nei documenti "Politica della sicurezza SID" e "Piano della Sicurezza".

La Politica sulla sicurezza è pubblicata e costantemente aggiornata da ParER sul sito web a disposizione di tutti i soggetti interessati e in particolare degli utilizzatori del Sistema di conservazione.

Il rispetto delle regole di sicurezza stabilite da ParER viene periodicamente controllato tramite opportuni test, che vengono svolti da personale esterno specializzato con cadenza periodica prestabilita o anche in maniera estemporanea, qualora il Responsabile della Sicurezza lo richieda.

Le attività relative alle verifiche tecniche e VA/PT (Vulnerability Assessment / Penetration Test) sono descritte all'interno della procedura "Gestione delle vulnerabilità", che viene implementata nell'ambito dei sistemi e degli applicativi in esercizio.

I Vulnerability Assessment sono eseguiti da laboratori (aziende esterne) in possesso di Certificato ISO 17025.

I principali obiettivi della procedura sono:

- verificare l'efficacia dei controlli e delle misure di sicurezza implementate dal ParER;
- valutare l'efficacia delle metodologie e delle soluzioni tecniche/tecnologiche adottate;
- avviare le procedure di soluzione delle vulnerabilità che sono state rilevate durante i test.

[\[Torna al Sommario\]](#)

10 TRATTAMENTO DEI DATI PERSONALI

Il nuovo Regolamento europeo sulla protezione dei dati personali (Regolamento (UE) 2016/679 – cd. "GDPR"), ha definito le seguenti figure:

- Titolare del Trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4, par. 1, n. 7 GDPR);
- Responsabile del trattamento: la persona fisica, giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (art. 4, par. 1, n. 8 GDPR);
- Responsabile della Protezione dei Dati (c.d. Data Protection Officer o D.P.O.): figura prevista dagli artt. 37 e seguenti del GDPR che ne disciplinano compiti, funzioni e responsabilità.

Al Titolare del Trattamento, ai sensi dell'art. 24 del GDPR, spetta l'adozione di misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento effettuato è conforme al Regolamento ed in particolare:

- gli interventi normativi necessari per l'adeguamento al GDPR;
- l'attribuzione di funzioni e compiti ai "soggetti attuatori" per gli adempimenti previsti dal GDPR.

Il Responsabile del Trattamento, ai sensi dell'art. 28 del GDPR, è soggetto esterno, con esperienza, capacità e conoscenza necessarie per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del Regolamento comunitario, anche relativamente al profilo della sicurezza, il quale effettua trattamenti di dati personali per conto del Titolare sulla base di un contratto o da altro atto giuridico che determini la materia del trattamento, la durata, la finalità, le categorie di dati personali trattati, le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento.

Il DPO, ai sensi dell'art. 28 del GDPR, ha il compito di sovrintendere alla gestione dei trattamenti di dati personali effettuati nell'ambito del Servizio di conservazione, affinché i dati siano trattati nel rispetto delle normative privacy europee e nazionali. Tale ruolo è ricoperto dal **Data Protection Officer (DPO) della Regione Emilia – Romagna**.

Inoltre, il DPO funge da punto di contatto, in riferimento alla casella e-mail dpo@regione.emilia-romagna.it, per l'autorità di controllo per questioni connesse al trattamento dei dati personali.

Nell'atto deliberativo di Giunta regionale n. 1123 del 16 luglio 2018 sono state individuate, nell'assetto organizzativo dell'Ente, le seguenti figure che intervengono nei trattamenti di dati personali con competenze e responsabilità specifiche:

- "Titolare dei trattamenti di dati personali" è stata individuata la Giunta regionale;
- "Soggetti attuatori" sono stati indicati, tra gli altri, i Direttori Generali della Regione Emilia-Romagna, ciascuno per il proprio ambito di competenza, con attribuzione di funzioni e compiti volti agli adempimenti necessari per la conformità dei trattamenti di dati personali effettuati dall'Ente in esecuzione del regolamento;
- "Responsabili del trattamento" sono designati soggetti esterni dell'Amministrazione che siano tenuti ad effettuare trattamenti di dati personali per conto del Titolare; detta

deliberazione n. 1123/2018 dispone che, attesa la natura negoziale della designazione del responsabile del trattamento, questa deve essere effettuata all'interno di contratti od accordi e, in ogni caso, in costanza di formazione del rapporto contrattuale, anche in aderenza ai facsimili messi a disposizione dalla struttura della Giunta regionale competente in materia di privacy.

I Direttori Generali possono delegare ai dirigenti assegnati alla Direzione relativamente ai trattamenti di diretta responsabilità della stessa, le funzioni e compiti attribuiti in materia di privacy, come specificato al punto 3 dell'allegato A della soprarichiamata deliberazione.

La Regione Emilia-Romagna, in attuazione di quanto previsto dalla legislazione regionale in materia di riordino istituzionale e delle funzioni regionali nel settore del patrimonio culturale, subentra ad IBACN negli atti giuridici (accordi) per la conservazione digitale già sottoscritti dal Responsabile del Servizio Polo Archivistico regionale, comprensivi degli accordi di cui all'art. 28 GDPR, parti integranti e sostanziali, con i quali le parti regolano i trattamenti di dati personali necessari e conseguenti alla sottoscrizione dei medesimi.

Dal quadro organizzativo sopra esposto risulta che il Responsabile del Polo Archivistico svolge le funzioni ed i compiti di responsabile del trattamento dati personali previsti in materia di privacy correlati alla conservazione digitale.

Con riferimento alla tematica del trattamento dei dati personali, occorre distinguere preliminarmente la categoria più ampia dei dati personali contenuti nei documenti oggetto di conservazione e la categoria dei dati personali degli *Utenti* del servizio di conservazione, trattati per consentire l'accesso al *Sistema di conservazione*.

L'impostazione adottata negli schemi di accordo con i *Produttori* consiste pertanto nel riconoscimento della titolarità del trattamento di dati personali contenuti nei documenti oggetto di conservazione in capo allo stesso *Produttore* e nella contestuale designazione della Regione Emilia-Romagna quale "Responsabile del trattamento" dei dati personali necessari all'esecuzione dell'**Accordo** e al compimento degli atti conseguenti.

Di conseguenza, la Regione Emilia-Romagna si impegna, nel trattamento dei suddetti dati, ad attenersi alle istruzioni e a svolgere i compiti indicati dall'Ente Produttore, così come meglio definiti nell'Allegato ex art. 28 del GDPR "Accordo Trattamento dati personali", da considerarsi parte sostanziale e integrante di ogni **Accordo** sottoscritto con i *Produttori*.

Coerentemente a quanto espresso, il Responsabile del Polo Archivistico regionale individuato dagli Enti Produttori, Titolari del trattamento, sulla base di Accordi ex art. 28 del GDPR quale *Responsabile del trattamento*, assume la responsabilità sulla garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali e sulla garanzia che il trattamento dei dati affidati dai *Produttori* avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.

Nel caso siano stipulati contratti con altri responsabili del trattamento (denominati anche "sub-responsabili"), in sede contrattuale, vengono imposte agli stessi condizioni vincolanti in materia di trattamento dei dati personali non meno onerose di quelle contenute negli Accordi sottoscritti con i *Produttori*. I contratti con le nomine del responsabile del trattamento degli eventuali sub-responsabili del ParER sono accessibili ai *Produttori* su richiesta, mentre i riferimenti degli atti

relativi risultano disponibili nel sito della Regione Emilia-Romagna, nell'area Amministrazione trasparente, nella sezione relativa a Bandi di gara e contratti.

Con precipuo riferimento invece al trattamento dei dati personali degli operatori del servizio di conservazione con livello di abilitazione consultatore, il trattamento dei dati in oggetto ha luogo conformemente a quanto previsto dal GDPR sempre sotto la responsabilità del Responsabile del Polo Archivistico regionale.

L'archivio logico comprendente i dati degli operatori abilitati alla consultazione di una o più strutture contiene i soli dati obbligatori indispensabili per il rilascio delle credenziali di accesso al sistema e per la corretta gestione del sistema di autorizzazione, nel rispetto di quanto previsto dal sopraindicato GDPR.

L'articolo 35, paragrafo 1, del GDPR prevede che il processo della Valutazione di Impatto sulla Protezione dei Dati (DPIA) sia obbligatorio quando un trattamento di dati personali "*presenti un rischio elevato per i diritti e le libertà delle persone fisiche*"; il soggetto obbligato ad effettuare una DPIA è il titolare del trattamento (nel processo di conservazione quindi il *Produttore*), con il supporto del Responsabile della protezione dei dati (DPO - *Data Protection Officer*), se nominato, e del Responsabile del trattamento eventualmente coinvolto. Considerando la dimensione e la criticità dei documenti conservati, ParER, benché non Titolare, ma Responsabile del trattamento, ha comunque ritenuto opportuno effettuare la DPIA sul trattamento "*Gestione dei dati e dei documenti trasmessi dagli Enti produttori al sistema di conservazione del ParER, ai fini del corretto svolgimento del processo di conservazione (trattamento effettuato nel pubblico interesse)*", identificando le misure opportune per la mitigazione del rischio di violazione dei dati personali, sensibili e giudiziari, con il supporto del DPO della Regione Emilia-Romagna.

[\[Torna al Sommario\]](#)

11 DOCUMENTI DI RIFERIMENTO E ALLEGATI

Si riporta l'elenco dei documenti citati nel presente Manuale con indicazione della collocazione in cui sono rintracciabili.

Documento	Collocazione
Politica della qualità SID	pubblicata nel sito di ParER: https://poloarchivistico.regione.emilia-romagna.it , in "Documentazione"
Modelli dei SIP (Linee guida per la realizzazione dei SIP)	pubblicata nel sito di ParER: https://poloarchivistico.regione.emilia-romagna.it , in "Documentazione"
Modelli dei pacchetti di archiviazione (AIP)	pubblicata nel sito di ParER: https://poloarchivistico.regione.emilia-romagna.it , in "Documentazione"
Specifiche tecniche dei servizi di versamento	pubblicata nel sito di ParER: https://poloarchivistico.regione.emilia-romagna.it , in "Documentazione"
Specifiche tecniche dei servizi di recupero	pubblicata nel sito di ParER: https://poloarchivistico.regione.emilia-romagna.it , in "Documentazione"
Politica della sicurezza SID	pubblicata nel sito di ParER: https://poloarchivistico.regione.emilia-romagna.it , in "Documentazione"
Piano della Sicurezza	<i>Repository Regionale</i>
Piano di Continuità Operativa del Servizio di conservazione	<i>Repository Regionale</i>
DPIA	<i>Repository Regionale</i>
Procedura di gestione degli incidenti di sicurezza e Data Breach	<i>Repository Regionale</i>
Procedura di gestione richieste di cambiamento del Servizio di conservazione	<i>Repository Regionale</i>
Procedura di progettazione e realizzazione di software applicativo del Servizio di conservazione	<i>Repository Regionale</i>
Procedura di gestione dei rilasci del Servizio di conservazione	<i>Repository Regionale</i>
Procedura di gestione Audit	<i>Repository Regionale</i>
Procedura di gestione delle Non Conformità	<i>Repository Regionale</i>
Procedura di gestione delle vulnerabilità	<i>Repository Regionale</i>
Registro dei formati	<i>SacER</i>
Gestione utenze del Sistema Applicativo di conservazione	<i>Repository Regionale</i>

Documento	Collocazione
Procedura di cessazione del Servizio restituzione dell'archivio	<i>Repository Regionale</i>
Gestione di richieste di informazioni, reclami e segnalazioni	<i>Repository Regionale</i>

Si riporta l'elenco dei documenti allegati al presente Manuale:

- **Allegato 1 "Normativa e standard di riferimento"**
- **Allegato 2 "Registro dei responsabili"**

[\[Torna al Sommario\]](#)

DISCIPLINARE TECNICO

PER LO SVOLGIMENTO DELLA FUNZIONE DI CONSERVAZIONE DEI DOCUMENTI INFORMATICI

Versione del 13/12/2023 (ora:13:11:25)

Ente convenzionato

Estremi dell'Accordo/Convenzione tra Ente e Regione Emilia-Romagna per lo svolgimento della funzione di conservazione dei documenti informatici:

*Data di decorrenza: 12/11/2015
Data di fine validità: 31/12/2033*

Nome dell'Ente versante configurato nel Sistema di conservazione:

unione terre acqua

Descrizione dell'Ente versante:

Unione delle Terre d'Acqua

Nome della Struttura versante configurata nel Sistema di conservazione:

udctd

Descrizione della Struttura versante:

Struttura dell'Unione dei Comuni delle Terre d'Acqua

INTRODUZIONE

Scopo, ambito e struttura del documento

Il presente documento costituisce il Disciplinare Tecnico (d'ora in poi Disciplinare), cioè il documento che definisce le specifiche operative e le modalità di descrizione e di versamento nel Sistema di conservazione delle Tipologie di unità documentarie oggetto di conservazione. Il Disciplinare è redatto in esecuzione di quanto indicato nell'Accordo o Convenzione, che regola nei suoi profili generali il rapporto tra l'Ente e Regione Emilia-Romagna per lo svolgimento della funzione di conservazione dei documenti informatici affidati dall'Ente alla Regione Emilia-Romagna e più specificatamente al suo Servizio Polo archivistico dell'Emilia-Romagna (d'ora in poi ParER) in base al Manuale di conservazione (d'ora in poi Manuale) redatto da ParER.

Per lo svolgimento delle funzioni di conservazione dei documenti informatici, ParER ha sviluppato un proprio Sistema di conservazione (d'ora in poi Sistema), descritto nel Manuale.

Le modalità generali di gestione delle funzioni di conservazione sono descritte nel Manuale a cui si rimanda anche per la terminologia utilizzata nel presente Disciplinare.

Il Disciplinare definisce l'articolazione in Strutture (corrispondenti normalmente alle Aree Organizzative Omogenee, ma non escludendo altre ripartizioni) con cui l'Ente si rapporta con ParER per il versamento dei documenti.

Inoltre dettaglia tutti gli aspetti direttamente desumibili dalle configurazioni della struttura versante (d'ora in poi Struttura) nel Sistema e non espressamente trattati dal Manuale. In particolare descrive le specificità e le modalità di versamento dei documenti informatici proprie dell'Ente.

Gli utenti espressamente autorizzati dall'Ente possono accedere al Sistema tramite credenziali personali rilasciate da ParER e comunicate al singolo utente. L'accesso al Sistema consente di consultare i documenti digitali versati nel Sistema e le configurazioni specifiche adottate.

ParER nell'erogazione dei servizi di conservazione garantisce ai Produttori i livelli di servizio che sono riportati nel catalogo dei servizi SaaS pubblicato da AgID alla pagina <https://cloud.italia.it/marketplace/show/all?searchCategory=SaaS>, in quanto dal 3/3/2020 ParER è fornitore accreditato di Software as a Service nel Cloud delle pubbliche amministrazioni.

Referenti

In questo capitolo sono definiti i nominativi e i recapiti dei Referenti ParER e dei Referenti dell'Ente che seguono o hanno seguito i test di versamento e l'attività di avvio del servizio di conservazione.

Nome e cognome	Recapiti	Archivista di riferimento (ParER) / Referente Ente	Note
Antonio Augenti	antonio.augenti@regione.emilia-romagna.it	Archivista di riferimento (ParER)	
Giulia Feliciani	giulia.feliciani@regione.emilia-romagna.it	Archivista di riferimento (ParER)	
Sara Parenti	sara.parenti@regione.emilia-romagna.it	Archivista di riferimento (ParER)	
Franco Sacerdotti	franco.sacerdotti@regione.emilia-romagna.it	Archivista di riferimento (ParER)	

Tabella - Referenti

Utenti del sistema

In questo capitolo sono definiti i nominativi, i recapiti, il ruolo delle diverse persone dell'Ente abilitate all'accesso al Sistema. Oltre agli utenti dell'Ente sono riportati gli utenti dell'ente amministratore Regione Emilia-Romagna e di eventuali organi di vigilanza.

A livello di regola generale, a ciascun utente viene assegnato all'interno del Sistema un userID con la sintassi "nome.cognome".

A ciascun utente del Sistema è possibile assegnare uno o più ruoli di accesso (d'ora in poi Ruoli), ognuno dei quali definisce le modalità di accesso ai documenti, alle informazioni conservate nel Sistema e alle operazioni che può effettuare.

Tra i Ruoli gestiti dal Sistema e assegnabili agli utenti:

- **Responsabile:** accede in visualizzazione a tutte le funzionalità. Può versare pacchetti standard e non standard, consistenza serie e annullare i versamenti. Inoltre accede in visualizzazione alle informazioni sugli utenti;
- **Supervisore:** consente di accedere all'archivio e al monitoraggio dei versamenti senza limitazioni sul tipo di dato;
- **Operatore:** consente di accedere al contenuto dell'archivio, anche limitatamente a determinate tipologie di contenuto;

- Conservatore: è assegnato ai Responsabili (e loro incaricati) degli enti Conservatori. Consente di accedere alle funzioni necessarie a gestire il processo di conservazione;
- Gestore: è assegnato agli utenti degli enti Gestori e consente l'accesso alle funzionalità di gestione degli utenti e delle organizzazioni degli enti produttori gestiti e ad assicurare loro il supporto per l'esercizio dei servizi di conservazione.

La Tabella Utenti abilitati mostra l'elenco degli utenti dell'Ente abilitati.

L'utente che non ha effettuato l'accesso nel Sistema negli ultimi 90 giorni viene disattivato. L'utente disattivo può essere successivamente eliminato oppure riattivato, nel caso in cui non sia scattato il limite temporale per l'eliminazione. L'utente che è disattivo da almeno 180 giorni viene eliminato automaticamente dal Sistema e non sarà più visibile nella Tabella Utenti abilitati.

Nome e cognome	Ruolo	Recapiti	Abilitazioni ai tipi di dato
Roberta Fontana	Supervisore	roberta.fontana@terredacqua.net	Abilitato a tutti i tipi di dato
Nadia Rosaria Marzano	Supervisore	nadia.marzano@terredacqua.net	Abilitato a tutti i tipi di dato
Giampiero Romanzi	Soprintendente	giampiero.romanzi@cultura.gov.it	Abilitato a tutti i tipi di dato

Tabella - Utenti abilitati

Tipologie di unità documentarie

La Tabella Tipologie di unità documentarie elenca le tipologie di unità documentarie oggetto di versamento e restituisce per ciascuna l'informazione relativa al sistema versante e alla data di primo versamento.

Per unità documentaria si intende un aggregato logico costituito da uno più documenti che sono considerati come un tutto unico. I documenti sono gli elementi dell'unità documentaria e sono identificati in base alla funzione che svolgono nel contesto dell'unità documentaria stessa, ovvero:

- Documento principale: documento che deve essere obbligatoriamente presente nell'unità documentaria, della quale definisce il contenuto primario;
- Allegato: documento che compone l'unità documentaria per integrare le informazioni contenute nel documento principale. È redatto contestualmente o precedentemente al documento principale;
- Annesso: documento che compone l'unità documentaria, generalmente prodotto e inserito nell'unità documentaria in un momento successivo a quello di creazione dell'unità documentaria, per fornire ulteriori notizie e informazioni a corredo del documento principale;
- Annotazione: documento che compone l'unità documentaria riportante gli elementi identificativi del documento e del suo iter documentale (un tipico esempio di Annotazione è rappresentato dalla segnatura di protocollo);

Per sistema versante si intende il sistema che cura, sotto forma di pacchetto di versamento (SIP), la trasmissione dei documenti al Sistema, direttamente o tramite sistemi intermedi, esterni all'Ente. Al sistema versante è associato l'utente versatore indicato nel SIP. In caso di utilizzo del client on line di versamento messo a disposizione da ParER o del servizio di versamento asincrono, la colonna Sistema versante sarà compilata rispettivamente con "SACER_VERSO" e "SACER_PREINGEST". Si precisa che il sistema versante e la modalità di versamento possono variare nel tempo e che il versamento della stessa tipologia di unità documentaria può essere contestualmente curato da più sistemi. In tali casi la tabella riporterà l'indicazione di tutti i sistemi versanti e utenti versatori utilizzati per il versamento.

Nel caso in cui alla data di estrazione del Disciplinare non siano ancora stati effettuati versamenti risolti, le informazioni relative al nome del sistema versante, utente versatore e data di primo versamento non sono riportate nella Tabella Tipologie di unità documentarie.

Tipologia di unità documentaria	Sistema versante	Utente versatore	Data di primo versamento
ACCORDO DI PROGRAMMA			
ACCORDO OPERATIVO			
DECRETO	ARCHIVER (Datagraph)	datagraph_unioneterreacqua	14/09/2016
DELIBERA	ARCHIVER (Datagraph)	datagraph_unioneterreacqua	14/09/2016
DETERMINA	ARCHIVER (Datagraph)	datagraph_unioneterreacqua	14/09/2016
DOCUMENTO PROTOCOLLATO	ARCHIVER (Datagraph)	datagraph_unioneterreacqua	14/09/2016

Tipologia di unità documentaria	Sistema versante	Utente versatore	Data di primo versamento
FATTURA ATTIVA	CITYWARE (Pal Informatica)	pal_unione_terre_acqua	22/12/2020
FATTURA PASSIVA	ARCHIVER (Datagraph), CITYWARE (Pal Informatica)	datagraph_unioneterreacqua , pal_unione_terre_acqua	07/12/2018
ORDINANZA	ARCHIVER (Datagraph)	datagraph_unioneterreacqua	14/09/2016
PIANO ARENILE			
PIANO ATTUATIVO DI INIZIATIVA PUBBLICA			
PIANO SETTORIALE			
PIANO URBANISTICO GENERALE			
PROCEDIMENTO UNICO			
REGISTRO GIORNALIERO	ARCHIVER (Datagraph)	datagraph_unioneterreacqua	14/09/2016
REGISTRO UNICO FATTURE	CITYWARE (Pal Informatica)	pal_unione_terre_acqua	07/12/2018
VARIANTE DI PIANO			

Tabella - Tipologie di unità documentarie

Nei paragrafi seguenti sono descritte in dettaglio le singole tipologie di unità documentarie in termini di struttura e metadati.

Tipologia di unità documentaria ACCORDO DI PROGRAMMA

Descrizione della tipologia di unità documentaria: Strumento Urbanistico costituito da accordi per la definizione e l'attuazione di opere, interventi e programmi di intervento di rilevante interesse pubblico che richiedano l'azione integrata e coordinata di due o più enti, ai sensi art. 59 L.R. 24/2017

Tipi struttura dell'unità documentaria: nella Tabella Tipi struttura unità documentaria sono rappresentate le varie strutture che può assumere il tipo di unità documentaria, ovvero la sua articolazione in documento principale ed eventuali allegati, annessi e annotazioni, le informazioni relative alla chiave, ai metadati di profilo e altro ancora.

Per ogni Tipo struttura è indicato il periodo di validità, ovvero per quali annualità delle unità documentarie è valido il tipo struttura e i sistemi versanti utilizzati.

Denominazione	Descrizione	Periodi di validità	Sistemi versanti
ACCORDO DI PROGRAMMA		2017	PREINGEST

Tabella - Tipi struttura unità documentaria

Nei paragrafi successivi sono riportate le informazioni di dettaglio su ogni singolo Tipo struttura dell'unità documentaria

Tipo struttura ACCORDO DI PROGRAMMA Nella tabella è riportata l'articolazione dell'unità documentaria in documento principale ed eventuali allegati, annessi e annotazioni.

Tipo documento	Descrizione
ALTRI ATTI RELAZIONI E PARERI	Altri atti relazioni e pareri L.R. 24/2017
DATI GEOGRAFICI	Dati geografici L.R. 24/2017
ELABORATI CARTOGRAFICI	Elaborati cartografici L.R. 24/2017
TESTO ACCORDO DI PROGRAMMA	Testo accordo di programma L.R. 24/2017

Tabella - Tipo struttura ACCORDO DI PROGRAMMA_Descrizione tipi documento

Tipo documento	Elemento	Obbligatorio	Periodicità di versamento	Note
ALTRI ATTI RELAZIONI E PARERI	ALLEGATO	Si		
DATI GEOGRAFICI	ALLEGATO	No		
ELABORATI CARTOGRAFICI	ALLEGATO	Si		
TESTO ACCORDO DI PROGRAMMA	PRINCIPALE	Si		

Tabella - Tipo struttura ACCORDO DI PROGRAMMA_Dettaglio tipi documento

Chiave identificativa del tipo struttura dell'unità documentaria (Tipo registro - Anno - Numero)

Registri - Nella Tabella Elenco registri è rappresentata la lista dei registri associati all'unità documentaria. Il nome del registro viene definito dall'Ente o concordato con ParER e in generale corrisponde al nome del repertorio in cui sono registrati in ordine progressivo i documenti ad esso afferenti (ex art. 53, D.P.R. 28/12/2000 n. 445) oppure al contesto applicativo/documentale nell'ambito del quale avviene l'assegnazione dell'identificativo progressivo e univoco. Il parametro "Fiscale" indica che le unità documentarie associate al Registro sono soggette alla conservazione di tipo fiscale, finalizzata alla conservazione a norma dei documenti rilevanti ai fini tributari in conformità con quanto previsto dalla normativa di settore vigente (DM del 17 giugno 2014 del Ministero dell'economia e delle finanze)

Tipo registro	Descrizione	Periodi di validità	Descrizione formato numero	Fiscale	Data disattivazione
STRUMENTI URBANISTICI	Registro per gli Strumenti Urbanistici	2017	Il numero è composto da una sigla che identifica il tipo di atto con cui è stato approvato lo strumento e dal numero di registrazione assegnato. Le sigle utilizzate sono DCC (Delibera Consiglio Comunale), DCU (Delibera Consiglio Unione), DGC (Delibera Giunta Comunale), DGU (Delibera Giunta Unione), PROT (Documento Protocollato). Il numero corrisponde al numero di registrazione nel repertorio delle delibere oppure al numero di protocollo.	No	

Tabella - Elenco registri

Anno - Anno solare di riferimento del repertorio

Numero - Numero di protocollo assegnato al documento, strutturato nella forma PROT_ddd

Riferimento temporale -

Metadati di profilo del tipo unità documentaria - Nella Tabella Metadati di profilo dell'unità documentaria sono descritti i metadati "Data" e "Oggetto" associati all'unità documentaria

Denominazione	Descrizione
Data	Data di protocollazione
Oggetto	Oggetto dello Strumento Urbanistico generato dal sistema, composto da nome dell'ente convenzionato, tipologia unità documentaria, anno, numero e data

Tabella - Metadati di profilo dell'unità documentaria

Collegamenti tra unità documentarie : L'unità documentaria costituita dall'Accordo di programma approvato può essere collegata alla unità documentaria costituita dall'Accordo di programma proposto e viceversa.

Metadati specifici associati al tipo unità documentaria - Nelle Tabelle Metadati specifici dell'unità documentaria è presentato il set di metadati associato all'unità documentaria nelle diverse versioni. La presenza di versioni diverse è legata alle eventuali modifiche/integrazioni/aggiornamenti nel set di metadati specifici o nelle obbligatorio concordate con l'Ente.

Versione metadati specifici: 1.0

Descrizione versione:

Data inizio validità: 10/10/2019

Data fine validità:

Denominazione	Descrizione
tipo_ente	tipo_ente
ente_convenzionato	ente_convenzionato
unione_comuni	unione_comuni
provincia_ente	provincia_ente
fase_elaborazione_strumento	fase_elaborazione_strumento

Tabella - Metadati specifici dell'unità documentaria

Tipologia di unità documentaria ACCORDO OPERATIVO

Descrizione della tipologia di unità documentaria: Strumento Urbanistico costituito da accordi stipulati tra i soggetti attuatori e i Comuni oppure le Unioni di Comuni, ai sensi dell'art. 38 L.R. 24/2017

Tipi struttura dell'unità documentaria: nella Tabella Tipi struttura unità documentaria sono rappresentate le varie strutture che può assumere il tipo di unità documentaria, ovvero la sua articolazione in documento principale ed eventuali allegati, annessi e annotazioni, le informazioni relative alla chiave, ai metadati di profilo e altro ancora.

Per ogni Tipo struttura è indicato il periodo di validità, ovvero per quali annualità delle unità documentarie è valido il tipo struttura e i sistemi versanti utilizzati.

Denominazione	Descrizione	Periodi di validità	Sistemi versanti
ACCORDO OPERATIVO		2017	PREINGEST

Tabella - Tipi struttura unità documentaria

Nei paragrafi successivi sono riportate le informazioni di dettaglio su ogni singolo Tipo struttura dell'unità documentaria

Tipi struttura ACCORDO OPERATIVO Nella tabella è riportata l'articolazione dell'unità documentaria in documento principale ed eventuali allegati, annessi e annotazioni.

Tipo documento	Descrizione
ALTRI ATTI RELAZIONI E PARERI	Altri atti relazioni e pareri L.R. 24/2017
ATTI NEGOZIALI E RELAZIONE ECONOMICO-FINANZIARIA	Atti negoziali e relazione economico-finanziaria L.R. 24/2017
DATI GEOGRAFICI	Dati geografici L.R. 24/2017
DELIBERA STRUMENTO URBANISTICO	Delibera strumento urbanistico L.R. 24/2017
ELABORATI CARTOGRAFICI	Elaborati cartografici L.R. 24/2017
VALSAT	Valsat L.R. 24/2017

Tabella - Tipi struttura ACCORDO OPERATIVO_Descrizione tipi documento

Tipo documento	Elemento	Obbligatorio	Periodicità di versamento	Note
ALTRI ATTI RELAZIONI E PARERI	ALLEGATO	No		
ATTI NEGOZIALI E RELAZIONE ECONOMICO-FINANZIARIA	ALLEGATO	No		
DATI GEOGRAFICI	ALLEGATO	No		
DELIBERA STRUMENTO URBANISTICO	PRINCIPALE	Si		
ELABORATI CARTOGRAFICI	ALLEGATO	No		
VALSAT	ALLEGATO	No		

Tabella - Tipo struttura ACCORDO OPERATIVO_Dettaglio tipi documento

Chiave identificativa del tipo struttura dell'unità documentaria (Tipo registro - Anno - Numero)

Registri - Nella Tabella Elenco registri è rappresentata la lista dei registri associati all'unità documentaria. Il nome del registro viene definito dall'Ente o concordato con ParER e in generale corrisponde al nome del repertorio in cui sono registrati in ordine progressivo i documenti ad esso afferenti (ex art. 53, D.P.R. 28/12/2000 n. 445) oppure al contesto applicativo/documentale nell'ambito del quale avviene l'assegnazione dell'identificativo progressivo e univoco. Il parametro "Fiscale" indica che le unità documentarie associate al Registro sono soggette alla conservazione di tipo fiscale, finalizzata alla conservazione a norma dei documenti rilevanti ai fini tributari in conformità con quanto previsto dalla normativa di settore vigente (DM del 17 giugno 2014 del Ministero dell'economia e delle finanze)

Tipo registro	Descrizione	Periodi di validità	Descrizione formato numero	Fiscale	Data disattivazione
STRUMENTI URBANISTICI	Registro per gli Strumenti Urbanistici	2017	Il numero è composto da una sigla che identifica il tipo di atto con cui è stato approvato lo strumento e dal numero di registrazione assegnato. Le sigle utilizzate sono DCC (Delibera Consiglio Comunale), DCU (Delibera Consiglio Unione), DGC	No	

Tipo registro	Descrizione	Periodi di validità	Descrizione formato numero	Fiscale	Data disattivazione
			(Delibera Giunta Comunale), DGU (Delibera Giunta Unione), PROT (Documento Protocollato). Il numero corrisponde al numero di registrazione nel repertorio delle delibere oppure al numero di protocollo.		

Tabella - Elenco registri

Anno - Anno solare di riferimento del repertorio

Numero - Numero della delibera con la quale è stato approvato l'atto, composto da una sigla che individua la tipologia dell'organo deliberante (DCC: Delibera Consiglio Comunale, DCU: Delibera Consiglio Unione, DGC: Delibera Giunta Comunale, DGU: Delibera Giunta Unione) e dal numero di repertorio, es. DCC_nnn

Riferimento temporale -

Metadati di profilo del tipo unità documentaria - Nella Tabella Metadati di profilo dell'unità documentaria sono descritti i metadati "Data" e "Oggetto" associati all'unità documentaria

Denominazione	Descrizione
Data	Data della Deliberazione che coincide con la data di seduta dell'Organo collegiale deliberante
Oggetto	Oggetto dello Strumento Urbanistico generato dal sistema, composto da nome dell'ente convenzionato, tipologia unità documentaria, anno, numero e data

Tabella - Metadati di profilo dell'unità documentaria

Collegamenti tra unità documentarie : l'unità documentaria costituita dall'Accordo operativo stipulato può essere collegata alla unità documentaria costituita dall'Accordo operativo proposto e viceversa.

Metadati specifici associati al tipo unità documentaria - Nelle Tabelle Metadati specifici dell'unità documentaria è presentato il set di metadati associato all'unità documentaria nelle diverse versioni. La presenza di versioni diverse è legata alle eventuali modifiche/integrazioni/aggiornamenti nel set di metadati specifici o nelle obbligatorioità concordate con l'Ente.

Versione metadati specifici: 1.0

Descrizione versione:

Data inizio validità: 10/10/2019

Data fine validità:

Denominazione	Descrizione
tipo_ente	tipo_ente
ente_convenzionato	ente_convenzionato
unione_comuni	unione_comuni
provincia_ente	provincia_ente
fase_elaborazione_strumento	fase_elaborazione_strumento

Tabella - Metadati specifici dell'unità documentaria

Tipologia di unità documentaria DECRETO

Descrizione della tipologia di unità documentaria: Decreto

Tipi struttura dell'unità documentaria: nella Tabella Tipi struttura unità documentaria sono rappresentate le varie strutture che può assumere il tipo di unità documentaria, ovvero la sua articolazione in documento principale ed eventuali allegati, annessi e annotazioni, le informazioni relative alla chiave, ai metadati di profilo e altro ancora.

Per ogni Tipo struttura è indicato il periodo di validità, ovvero per quali annualità delle unità documentarie è valido il tipo struttura e i sistemi versanti utilizzati.

Denominazione	Descrizione	Periodi di validità	Sistemi versanti
DECRETO	Decreto		

Tabella - Tipi struttura unità documentaria

Nei paragrafi successivi sono riportate le informazioni di dettaglio su ogni singolo Tipo struttura dell'unità documentaria

Tipi struttura DECRETO Nella tabella è riportata l'articolazione dell'unità documentaria in documento principale ed eventuali allegati, annessi e annotazioni.
Descrizione: Decreto

Tipo documento	Descrizione
DECRETO	Decreto
GENERICO	Allegato generico
RELATA PUBBLICAZIONE	Attestazione di pubblicazione del documento all'Albo Pretorio

Tabella - Tipo struttura DECRETO_Descrizione tipi documento

Tipo documento	Elemento	Obbligatorio	Periodicità di versamento	Note
DECRETO	PRINCIPALE	Si		
GENERICO	ANNOTAZIONE	No		
RELATA PUBBLICAZIONE	ANNESSO	No		

Tabella - Tipo struttura DECRETO_Dettaglio tipi documento

Chiave identificativa del tipo struttura dell'unità documentaria (Tipo registro - Anno - Numero)

Registri - Nella Tabella Elenco registri è rappresentata la lista dei registri associati all'unità documentaria. Il nome del registro viene definito dall'Ente o concordato con ParER e in generale corrisponde al nome del repertorio in cui sono registrati in ordine progressivo i documenti ad esso afferenti (ex art. 53, D.P.R. 28/12/2000 n. 445) oppure al contesto applicativo/documentale nell'ambito del quale avviene l'assegnazione dell'identificativo progressivo e univoco. Il parametro "Fiscale" indica che le unità documentarie associate al Registro sono soggette alla conservazione di tipo fiscale, finalizzata alla conservazione a norma dei documenti rilevanti ai fini tributari in conformità con quanto previsto dalla normativa di settore vigente (DM del 17 giugno 2014 del Ministero dell'economia e delle finanze)

Tipo registro	Descrizione	Periodi di validità	Descrizione formato numero	Fiscale	Data disattivazione
DECR	Registro dei Decreti	2015		No	

Tabella - Elenco registri

Anno -

Numero -

Riferimento temporale -

Metadati di profilo del tipo unità documentaria - Nella Tabella Metadati di profilo dell'unità documentaria sono descritti i metadati "Data" e "Oggetto" associati all'unità documentaria

Denominazione	Descrizione
Data	
Oggetto	

Tabella - Metadati di profilo dell'unità documentaria

Metadati specifici associati al tipo unità documentaria - Nelle Tabelle Metadati specifici dell'unità documentaria è presentato il set di metadati associato all'unità documentaria nelle diverse versioni. La presenza di versioni diverse è legata alle eventuali modifiche/integrazioni/aggiornamenti nel set di metadati specifici o nelle obbligatorietà concordate con l'Ente.

Versione metadati specifici: 1.0

Descrizione versione:

Data inizio validità: 18/06/2015

Data fine validità:

Denominazione	Descrizione
settore	settore
materia	materia
firmatario	firmatario
firmatario_ruolo	firmatario_ruolo
note	note
registrazione_data	registrazione_data
soggetti_interessati	soggetti_interessati
annullato	annullato
annullamento_data	annullamento_data
annullamento_motivo	annullamento_motivo
annullamento_soggetto	annullamento_soggetto
annullamento_atto	annullamento_atto

Tabella - Metadati specifici dell'unità documentaria

Metadati specifici tipo documento RELATA PUBBLICAZIONE - Nelle tabelle “Metadati specifici del documento” è presentato il set di metadati specifici associato al documento nelle varie versioni. La presenza di versioni diverse è legata alle eventuali modifiche/integrazioni/aggiornamenti nel set di metadati specifici e nella obbligatorietà concordate con l'Ente.

Versione metadati specifici: 1.0

Descrizione versione:

Data inizio validità: 29/04/2014

Data fine validità:

Denominazione	Descrizione
pubblicazione_anno	pubblicazione_anno
pubblicazione_numero	pubblicazione_numero

Denominazione	Descrizione
pubblicazione_registro	pubblicazione_registro
pubblicazione_data_inizio	pubblicazione_data_inizio
pubblicazione_data_fine	pubblicazione_data_fine
ripubblicazione	ripubblicazione

Tabella - Metadati specifici del documento

Tipologia di unità documentaria DELIBERA

Descrizione della tipologia di unità documentaria: Delibera

Tipi struttura dell'unità documentaria: nella Tabella Tipi struttura unità documentaria sono rappresentate le varie strutture che può assumere il tipo di unità documentaria, ovvero la sua articolazione in documento principale ed eventuali allegati, annessi e annotazioni, le informazioni relative alla chiave, ai metadati di profilo e altro ancora.

Per ogni Tipo struttura è indicato il periodo di validità, ovvero per quali annualità delle unità documentarie è valido il tipo struttura e i sistemi versanti utilizzati.

Denominazione	Descrizione	Periodi di validità	Sistemi versanti
DELIBERA	Delibera		

Tabella - Tipi struttura unità documentaria

Nei paragrafi successivi sono riportate le informazioni di dettaglio su ogni singolo Tipo struttura dell'unità documentaria

Tipologia struttura DELIBERA Nella tabella è riportata l'articolazione dell'unità documentaria in documento principale ed eventuali allegati, annessi e annotazioni.
Descrizione: Delibera

Tipo documento	Descrizione
ATTESTAZIONE ESECUTIVITA	Attestazione di avvenuta esecutività
DELIBERA	Delibera
GENERICO	Allegato generico
RELATA PUBBLICAZIONE	Attestazione di pubblicazione del documento all'Albo Pretorio

Tabella - Tipo struttura DELIBERA_Descrizione tipi documento

Tipo documento	Elemento	Obbligatorio	Periodicità di versamento	Note
ATTESTAZIONE ESECUTIVITA	ANNESSO	No		
DELIBERA	PRINCIPALE	Si		
GENERICO	ALLEGATO	No		
RELATA PUBBLICAZIONE	ANNESSO	No		

Tabella - Tipo struttura DELIBERA_Dettaglio tipi documento

Chiave identificativa del tipo struttura dell'unità documentaria (Tipo registro - Anno - Numero)

Registri - Nella Tabella Elenco registri è rappresentata la lista dei registri associati all'unità documentaria. Il nome del registro viene definito dall'Ente o concordato con ParER e in generale corrisponde al nome del repertorio in cui sono registrati in ordine progressivo i documenti ad esso afferenti (ex art. 53, D.P.R. 28/12/2000 n. 445) oppure al contesto applicativo/documentale nell'ambito del quale avviene l'assegnazione dell'identificativo progressivo e univoco. Il parametro "Fiscale" indica che le unità documentarie associate al Registro sono soggette alla conservazione di tipo fiscale, finalizzata alla conservazione a norma dei documenti rilevanti ai fini tributari in conformità con quanto previsto dalla normativa di settore vigente (DM del 17 giugno 2014 del Ministero dell'economia e delle finanze)

Tipo registro	Descrizione	Periodi di validità	Descrizione formato numero	Fiscale	Data disattivazione
CONS	Registro delle delibere di consiglio	2012		No	
GIUN	Registro delle delibere di giunta	2012		No	

Tabella - Elenco registri

Anno -

Numero -

Riferimento temporale -

Metadati di profilo del tipo unità documentaria - Nella Tabella Metadati di profilo dell'unità documentaria sono descritti i metadati "Data" e "Oggetto" associati all'unità documentaria

Denominazione	Descrizione
Data	
Oggetto	

Tabella - Metadati di profilo dell'unità documentaria

Metadati specifici associati al tipo unità documentaria - Nelle Tabelle Metadati specifici dell'unità documentaria è presentato il set di metadati associato all'unità documentaria nelle diverse versioni. La presenza di versioni diverse è legata alle eventuali modifiche/integrazioni/aggiornamenti nel set di metadati specifici o nelle obbligatorio concordate con l'Ente.

Versione metadati specifici: 1.1

Descrizione versione:

Data inizio validità: 12/09/2016

Data fine validità:

Denominazione	Descrizione
assessorato	assessorato
settore	settore
servizio	servizio
materia	materia
responsabile_procedimento	responsabile_procedimento
note	note
parere_regolarita_tecnica	parere_regolarita_tecnica
responsabile_servizio	responsabile_servizio
data_regolarita_tecnica	data_regolarita_tecnica
parere_tecnico_espresso	parere_tecnico_espresso
note_regolarita_tecnica	note_regolarita_tecnica
parere_regolarita_contabile	parere_regolarita_contabile
responsabile_regolarita_contabile	responsabile_regolarita_contabile
data_regolarita_contabile	data_regolarita_contabile
parere_contabile_espresso	parere_contabile_espresso
note_regolarita_contabile	note_regolarita_contabile
organo_deliberante	organo_deliberante
seduta_anno	seduta_anno

Denominazione	Descrizione
seduta_numero	seduta_numero
seduta_punto	seduta_punto
proposta_numero	proposta_numero
proposta_data	proposta_data
dispositivo	dispositivo
attestazione_esecutivita	attestazione_esecutivita
data_esecutivita	data_esecutivita
invio_capigruppo_data	invio_capigruppo_data
invio_capigruppo_registro	invio_capigruppo_registro
invio_capigruppo_anno	invio_capigruppo_anno
invio_capigruppo_numero	invio_capigruppo_numero
altra_registrazione_registro	altra_registrazione_registro
altra_registrazione_anno	altra_registrazione_anno
altra_registrazione_numero	altra_registrazione_numero
altra_registrazione_data	altra_registrazione_data
responsabile_trasparenza	responsabile_trasparenza
pubblicato	pubblicato
articolo	articolo

Tabella - Metadati specifici dell'unità documentaria

Metadati specifici tipo documento RELATA PUBBLICAZIONE - Nelle tabelle “Metadati specifici del documento” è presentato il set di metadati specifici associato al documento nelle varie versioni. La presenza di versioni diverse è legata alle eventuali modifiche/integrazioni/aggiornamenti nel set di metadati specifici e nella obbligatorietà concordate con l'Ente.

Versione metadati specifici: 1.0

Descrizione versione:

Data inizio validità: 29/04/2014

Data fine validità:

Denominazione	Descrizione
pubblicazione_anno	pubblicazione_anno
pubblicazione_numero	pubblicazione_numero
pubblicazione_registro	pubblicazione_registro
pubblicazione_data_inizio	pubblicazione_data_inizio
pubblicazione_data_fine	pubblicazione_data_fine
ripubblicazione	ripubblicazione

Tabella - Metadati specifici del documento

Tipologia di unità documentaria DETERMINA

Descrizione della tipologia di unità documentaria: Determina

Tipi struttura dell'unità documentaria: nella Tabella Tipi struttura unità documentaria sono rappresentate le varie strutture che può assumere il tipo di unità documentaria, ovvero la sua articolazione in documento principale ed eventuali allegati, annessi e annotazioni, le informazioni relative alla chiave, ai metadati di profilo e altro ancora.

Per ogni Tipo struttura è indicato il periodo di validità, ovvero per quali annualità delle unità documentarie è valido il tipo struttura e i sistemi versanti utilizzati.

Denominazione	Descrizione	Periodi di validità	Sistemi versanti
DETERMINA	Determina		

Tabella - Tipi struttura unità documentaria

Nei paragrafi successivi sono riportate le informazioni di dettaglio su ogni singolo Tipo struttura dell'unità documentaria

Tipi struttura DETERMINA Nella tabella è riportata l'articolazione dell'unità documentaria in documento principale ed eventuali allegati, annessi e annotazioni.

Descrizione: Determina

Tipo documento	Descrizione
DETERMINA	Determina
GENERICO	Allegato generico
RELATA PUBBLICAZIONE	Attestazione di pubblicazione del documento all'Albo Pretorio
VISTO CONTABILE	Visto contabile

Tabella - Tipi struttura DETERMINA_Descrizione tipi documento

Tipo documento	Elemento	Obbligatorio	Periodicità di versamento	Note
DETERMINA	PRINCIPALE	Si		
GENERICO	ALLEGATO	No		
RELATA PUBBLICAZIONE	ANNESSO	No		
VISTO CONTABILE	ALLEGATO	No		

Tabella - Tipo struttura DETERMINA_Dettaglio tipi documento

Chiave identificativa del tipo struttura dell'unità documentaria (Tipo registro - Anno - Numero)

Registri - Nella Tabella Elenco registri è rappresentata la lista dei registri associati all'unità documentaria. Il nome del registro viene definito dall'Ente o concordato con ParER e in generale corrisponde al nome del repertorio in cui sono registrati in ordine progressivo i documenti ad esso afferenti (ex art. 53, D.P.R. 28/12/2000 n. 445) oppure al contesto applicativo/documentale nell'ambito del quale avviene l'assegnazione dell'identificativo progressivo e univoco. Il parametro "Fiscale" indica che le unità documentarie associate al Registro sono soggette alla conservazione di tipo fiscale, finalizzata alla conservazione a norma dei documenti rilevanti ai fini tributari in conformità con quanto previsto dalla normativa di settore vigente (DM del 17 giugno 2014 del Ministero dell'economia e delle finanze)

Tipo registro	Descrizione	Periodi di validità	Descrizione formato numero	Fiscale	Data disattivazione
DETE	Registro delle determine dirigenziali	2012		No	

Tabella - Elenco registri

Anno -

Numero -

Riferimento temporale -

Metadati di profilo del tipo unità documentaria - Nella Tabella Metadati di profilo dell'unità documentaria sono descritti i metadati "Data" e "Oggetto" associati all'unità documentaria

Denominazione	Descrizione
Data	
Oggetto	

Tabella - Metadati di profilo dell'unità documentaria

Metadati specifici associati al tipo unità documentaria - Nelle Tabelle Metadati specifici dell'unità documentaria è presentato il set di metadati associato all'unità documentaria nelle diverse versioni. La presenza di versioni diverse è legata alle eventuali modifiche/integrazioni/aggiornamenti nel set di metadati specifici o nelle obbligatorioità concordate con l'Ente.

Versione metadati specifici: 1.0

Descrizione versione:

Data inizio validità: 28/04/2014

Data fine validità:

Denominazione	Descrizione
settore	settore
servizio	servizio
responsabile_procedimento	responsabile_procedimento
firmatario_atto	firmatario_atto
ruolo_frmatario_atto	ruolo_frmatario_atto
note	note
materia	materia
proposta_numero	proposta_numero
proposta_data	proposta_data
data_esecutivita	data_esecutivita
visto_regolarita_contabile	visto_regolarita_contabile
responsabile_visto_contabile	responsabile_visto_contabile
data_visto_contabile	data_visto_contabile
visto_contabile_espresso	visto_contabile_espresso
note_visto_contabile	note_visto_contabile
altra_registrazione_registro	altra_registrazione_registro
altra_registrazione_anno	altra_registrazione_anno
altra_registrazione_numero	altra_registrazione_numero
altra_registrazione_data	altra_registrazione_data
funzionario_incaricato_pubblicazione	funzionario_incaricato_pubblicazione

Denominazione	Descrizione
responsabile_trasparenza	responsabile_trasparenza
pubblicato	pubblicato
articolo	articolo

Tabella - Metadati specifici dell'unità documentaria

Metadati specifici tipo documento RELATA PUBBLICAZIONE - Nelle tabelle “Metadati specifici del documento” è presentato il set di metadati specifici associato al documento nelle varie versioni. La presenza di versioni diverse è legata alle eventuali modifiche/integrazioni/aggiornamenti nel set di metadati specifici e nella obbligatorietà concordate con l'Ente.

Versione metadati specifici: 1.0

Descrizione versione:

Data inizio validità: 29/04/2014

Data fine validità:

Denominazione	Descrizione
pubblicazione_anno	pubblicazione_anno
pubblicazione_numero	pubblicazione_numero
pubblicazione_registro	pubblicazione_registro
pubblicazione_data_inizio	pubblicazione_data_inizio
pubblicazione_data_fine	pubblicazione_data_fine
ripubblicazione	ripubblicazione

Tabella - Metadati specifici del documento

Tipologia di unità documentaria DOCUMENTO PROTOCOLLATO

Descrizione della tipologia di unità documentaria: Documento registrato a protocollo

Tipi struttura dell'unità documentaria: nella Tabella Tipi struttura unità documentaria sono rappresentate le varie strutture che può assumere il tipo di unità documentaria, ovvero la sua articolazione in documento principale ed eventuali allegati, annessi e annotazioni, le informazioni relative alla chiave, ai metadati di profilo e altro ancora.

Per ogni Tipo struttura è indicato il periodo di validità, ovvero per quali annualità delle unità documentarie è valido il tipo struttura e i sistemi versanti utilizzati.

Denominazione	Descrizione	Periodi di validità	Sistemi versanti
DOCUMENTO PROTOCOLLATO	Documento registrato a protocollo		

Tabella - Tipi struttura unità documentaria

Nei paragrafi successivi sono riportate le informazioni di dettaglio su ogni singolo Tipo struttura dell'unità documentaria

Tipi struttura DOCUMENTO PROTOCOLLATO Nella tabella è riportata l'articolazione dell'unità documentaria in documento principale ed eventuali allegati, annessi e annotazioni.

Descrizione: Documento registrato a protocollo

Tipo documento	Descrizione
AGGIORNAMENTO	Aggiornamento di conferma
ANNULLAMENTO	Notifica di annullamento della registrazione di protocollo
CONFERMA	Conferma di ricezione
DOCUMENTO PROTOCOLLATO	Documento registrato a protocollo
ECCEZIONE	Notifica di eccezione
GENERICO	Allegato generico
MESSAGGIO PEC	Email ricevuta attraverso PEC
RICEVUTA ACCETTAZIONE	Ricevuta di accettazione della PEC
RICEVUTA CONSEGNA	Ricevuta di consegna della PEC
RICEVUTA PEC IN ERRORE	Ricevuta PEC in caso di errore
SEGNATURA	Segnatura di protocollo

Tipo documento	Descrizione
SEGNATURA MITTENTE	Segnatura di protocollo del documento in entrata

Tabella - Tipo struttura DOCUMENTO PROTOCOLLATO_Descrizione tipi documento

Tipo documento	Elemento	Obbligatorio	Periodicità di versamento	Note
AGGIORNAMENTO	ANNESSO	No		
ANNULLAMENTO	ANNESSO	No		
CONFERMA	ANNESSO	No		
DOCUMENTO PROTOCOLLATO	PRINCIPALE	Si		
ECCEZIONE	ANNESSO	No		
GENERICO	PRINCIPALE	No		
GENERICO	ALLEGATO	No		
MESSAGGIO PEC	ANNESSO	No		
RICEVUTA ACCETTAZIONE	ANNESSO	No		
RICEVUTA CONSEGNA	ANNESSO	No		
RICEVUTA PEC IN ERRORE	ANNESSO	No		
SEGNATURA	ANNOTAZIONE	No		
SEGNATURA MITTENTE	ANNOTAZIONE	No		

Tabella - Tipo struttura DOCUMENTO PROTOCOLLATO_Dettaglio tipi documento

Chiave identificativa del tipo struttura dell'unità documentaria (Tipo registro - Anno - Numero)

Registri - Nella Tabella Elenco registri è rappresentata la lista dei registri associati all'unità documentaria. Il nome del registro viene definito dall'Ente o concordato con ParER e in generale corrisponde al nome del repertorio in cui sono registrati in ordine progressivo i documenti ad esso afferenti (ex art. 53, D.P.R. 28/12/2000 n. 445) oppure al contesto applicativo/documentale nell'ambito del quale avviene l'assegnazione dell'identificativo progressivo e univoco.

Il parametro "Fiscale" indica che le unità documentarie associate al Registro sono soggette alla conservazione di tipo fiscale, finalizzata alla conservazione a norma dei documenti rilevanti ai fini tributari in conformità con quanto previsto dalla normativa di settore vigente (DM del 17 giugno 2014 del Ministero dell'economia e delle finanze)

Tipo registro	Descrizione	Periodi di validità	Descrizione formato numero	Fiscale	Data disattivazione
PROTO	Registro dei documenti protocollati	2012		No	

Tabella - Elenco registri

Anno -

Numero -

Riferimento temporale -

Metadati di profilo del tipo unità documentaria - Nella Tabella Metadati di profilo dell'unità documentaria sono descritti i metadati "Data" e "Oggetto" associati all'unità documentaria

Denominazione	Descrizione
Data	
Oggetto	

Tabella - Metadati di profilo dell'unità documentaria

Metadati specifici associati al tipo unità documentaria - Nelle Tabelle Metadati specifici dell'unità documentaria è presentato il set di metadati associato all'unità documentaria nelle diverse versioni. La presenza di versioni diverse è legata alle eventuali modifiche/integrazioni/aggiornamenti nel set di metadati specifici o nelle obbligatorio concordate con l'Ente.

Versione metadati specifici: 1.0

Descrizione versione:

Data inizio validità: 17/02/2016

Data fine validità:

Denominazione	Descrizione
Corrispondenti	Corrispondenti
Movimento	Movimento
NumeroDocumentoMittente	NumeroDocumentoMittente
DataDocumentoMittente	DataDocumentoMittente
ModalitaTrasmissione	ModalitaTrasmissione
DescrizioneDocumento	DescrizioneDocumento
OperatoreProtocollo	OperatoreProtocollo
Annullato	Annullato
DataAnnullamento	DataAnnullamento
MotivoAnnullamento	MotivoAnnullamento
ProvvedimentoAnnullamento	ProvvedimentoAnnullamento
EsecutoreAnnullamento	EsecutoreAnnullamento
Note	Note
ProtocolloRiservato	ProtocolloRiservato
AnnoPubblicazione	AnnoPubblicazione
NumeroPubblicazione	NumeroPubblicazione
DataInizioPubblicazione	DataInizioPubblicazione
DataFinePubblicazione	DataFinePubblicazione
RegistroPubblicazione	RegistroPubblicazione
RegistroNumero	RegistroNumero
RegistroAnno	RegistroAnno
RegistroData	RegistroData
TipoRegistro	TipoRegistro
ConsegnatariEmittenti	ConsegnatariEmittenti

Tabella - Metadati specifici dell'unità documentaria

Tipologia di unità documentaria FATTURA ATTIVA

Descrizione della tipologia di unità documentaria: Fattura attiva

Tipi struttura dell'unità documentaria: nella Tabella Tipi struttura unità documentaria sono rappresentate le varie strutture che può assumere il tipo di unità documentaria, ovvero la sua articolazione in documento principale ed eventuali allegati, annessi e annotazioni, le informazioni relative alla chiave, ai metadati di profilo e altro ancora.

Per ogni Tipo struttura è indicato il periodo di validità, ovvero per quali annualità delle unità documentarie è valido il tipo struttura e i sistemi versanti utilizzati.

Denominazione	Descrizione	Periodi di validità	Sistemi versanti
FATTURA ATTIVA	Struttura UD della FATTURA ATTIVA		

Tabella - Tipi struttura unità documentaria

Nei paragrafi successivi sono riportate le informazioni di dettaglio su ogni singolo Tipo struttura dell'unità documentaria

Tipi struttura FATTURA ATTIVA Nella tabella è riportata l'articolazione dell'unità documentaria in documento principale ed eventuali allegati, annessi e annotazioni.

Descrizione: Struttura UD della FATTURA ATTIVA

Tipo documento	Descrizione
ACCONTO/ANTICIPO SU FATTURA	Acconto/anticipo su fattura
ACCONTO/ANTICIPO SU PARCELLA	Acconto/anticipo su parcella
ATTESTAZIONE IMPOSSIBILITÀ DI RECAPITO	Attestazione impossibilità di recapito
FATTURA	Fattura
GENERICO	Allegato generico
NOTA DI CREDITO	Nota di credito
NOTA DI DEBITO	Nota di debito
NOTIFICA DI DECORRENZA DEI TERMINI	Notifica con cui Sdl comunica al destinatario l'impossibilità di inviare, da quel momento in poi, Notifica di esito committente e al trasmittente l'impossibilità di ricevere Notifica di esito
NOTIFICA DI ESITO	Notifica di esito
NOTIFICA DI MANCATA CONSEGNA	Notifica di mancata consegna

Tipo documento	Descrizione
NOTIFICA DI SCARTO	Notifica di scarto
PARCELLA	Parcella
RICEVUTA DI CONSEGNA	Messaggio che SdI invia al trasmittente per certificare l'avvenuta consegna al destinatario della fattura
TRANSCODIFICA FATTURA	Transcodifica fattura

Tabella - Tipo struttura FATTURA ATTIVA_Descrizione tipi documento

Tipo documento	Elemento	Obbligatorio	Periodicità di versamento	Note
ACCONTO/ANTICIPO SU FATTURA	PRINCIPALE	Si		
ACCONTO/ANTICIPO SU PARCELLA	PRINCIPALE	Si		
ATTESTAZIONE IMPOSSIBILITÀ DI RECAPITO	ANNESSO	No		
FATTURA	PRINCIPALE	Si		
GENERICO	ALLEGATO	No		
NOTA DI CREDITO	PRINCIPALE	Si		
NOTA DI DEBITO	PRINCIPALE	Si		
NOTIFICA DI DECORRENZA DEI TERMINI	ANNESSO	No		
NOTIFICA DI ESITO	ANNESSO	No		
NOTIFICA DI MANCATA CONSEGNA	ANNESSO	No		
NOTIFICA DI SCARTO	ANNESSO	No		
PARCELLA	PRINCIPALE	Si		
RICEVUTA DI CONSEGNA	ANNESSO	No		

Tipo documento	Elemento	Obbligatorio	Periodicità di versamento	Note
TRANSCODIFICA FATTURA	ANNESSO	No		

Tabella - Tipo struttura FATTURA ATTIVA_Dettaglio tipi documento

Metadati di profilo del tipo unità documentaria - Nella Tabella Metadati di profilo dell'unità documentaria sono descritti i metadati "Data" e "Oggetto" associati all'unità documentaria

Denominazione	Descrizione
Data	
Oggetto	

Tabella - Metadati di profilo dell'unità documentaria

Metadati specifici associati al tipo unità documentaria - Nelle Tabelle Metadati specifici dell'unità documentaria è presentato il set di metadati associato all'unità documentaria nelle diverse versioni. La presenza di versioni diverse è legata alle eventuali modifiche/integrazioni/aggiornamenti nel set di metadati specifici o nelle obbligatorietà concordate con l'Ente.

Versione metadati specifici: cityware_fattura_attiva_1.0

Descrizione versione:

Data inizio validità: 09/12/2020

Data fine validità:

Denominazione	Descrizione
NumeroProtocollo	NumeroProtocollo
DataProtocollo	DataProtocollo
DenominazioneDestinatario	DenominazioneDestinatario
TipoDenominazioneDestinatario	TipoDenominazioneDestinatario
IdentificativoDestinatario	IdentificativoDestinatario
TipoidentificativoDestinatario	TipoidentificativoDestinatario

Denominazione	Descrizione
ImportoTotale	ImportoTotale
ScadenzaFattura	ScadenzaFattura
AliquotaIvaReverseCharge	AliquotaIvaReverseCharge
IvaTotaleReverseCharge	IvaTotaleReverseCharge

Tabella - Metadati specifici dell'unità documentaria

Tipologia di unità documentaria FATTURA PASSIVA

Descrizione della tipologia di unità documentaria: Fattura passiva

Tipi struttura dell'unità documentaria: nella Tabella Tipi struttura unità documentaria sono rappresentate le varie strutture che può assumere il tipo di unità documentaria, ovvero la sua articolazione in documento principale ed eventuali allegati, annessi e annotazioni, le informazioni relative alla chiave, ai metadati di profilo e altro ancora.

Per ogni Tipo struttura è indicato il periodo di validità, ovvero per quali annualità delle unità documentarie è valido il tipo struttura e i sistemi versanti utilizzati.

Denominazione	Descrizione	Periodi di validità	Sistemi versanti
FATTURA PASSIVA	Struttura UD della FATTURA PASSIVA	2020	ARCHIVER (Datagraph)

Tabella - Tipi struttura unità documentaria

Nei paragrafi successivi sono riportate le informazioni di dettaglio su ogni singolo Tipo struttura dell'unità documentaria

Tipologia struttura FATTURA PASSIVA Nella tabella è riportata l'articolazione dell'unità documentaria in documento principale ed eventuali allegati, annessi e annotazioni.

Descrizione: Struttura UD della FATTURA PASSIVA

Tipo documento	Descrizione
ACCONTO/ANTICIPO SU FATTURA	Acconto/anticipo su fattura
ACCONTO/ANTICIPO SU PARCELLA	Acconto/anticipo su parcella
FATTURA	Fattura
FATTURA ESTRATTA DAL LOTTO	Fattura estratta dal lotto
FILE DEI METADATI	File che Sdl invia al destinatario contenente l'identificativo della fattura
GENERICO	Allegato generico
NOTA DI CREDITO	Nota di credito
NOTA DI DEBITO	Nota di debito
NOTIFICA DI DECORRENZA DEI TERMINI	Notifica con cui Sdl comunica al destinatario l'impossibilità di inviare, da quel momento in poi, Notifica di esito committente e al trasmittente l'impossibilità di ricevere Notifica di esito
NOTIFICA DI ESITO COMMITTENTE	Messaggio facoltativo del destinatario a Sdl che segnala l'accettazione o il rifiuto della fattura
PARCELLA	Parcella

Tipo documento	Descrizione
PEC RICEVUTA CONSEGNA	Ricevuta di consegna
PEC RICEVUTA ERRORE	Ricevuta di errore
SCARTO ESITO COMMITTENTE	Scarto esito committente
TRANSCODIFICA FATTURA	Transcodifica fattura

Tabella - Tipo struttura FATTURA PASSIVA_Descrizione tipi documento

Tipo documento	Elemento	Obbligatorio	Periodicità di versamento	Note
ACCONTO/ANTICIPO SU FATTURA	PRINCIPALE	Si		
ACCONTO/ANTICIPO SU PARCELLA	PRINCIPALE	Si		
FATTURA	PRINCIPALE	Si		
FATTURA ESTRATTA DAL LOTTO	ANNESSO	No		
FILE DEI METADATI	ANNESSO	No		
GENERICO	ALLEGATO	No		
NOTA DI CREDITO	PRINCIPALE	Si		
NOTA DI DEBITO	PRINCIPALE	Si		
NOTIFICA DI DECORRENZA DEI TERMINI	ANNESSO	No		
NOTIFICA DI ESITO COMMITTENTE	ANNESSO	No		
PARCELLA	PRINCIPALE	Si		
PEC RICEVUTA CONSEGNA	ANNESSO	No		
PEC RICEVUTA ERRORE	ANNESSO	No		

Tipo documento	Elemento	Obbligatorio	Periodicità di versamento	Note
SCARTO ESITO COMMITTENTE	ANNESSO	No		
TRANSCODIFICA FATTURA	ANNESSO	No		

Tabella - Tipo struttura FATTURA PASSIVA_Dettaglio tipi documento

Chiave identificativa del tipo struttura dell'unità documentaria (Tipo registro - Anno - Numero)

Registri - Nella Tabella Elenco registri è rappresentata la lista dei registri associati all'unità documentaria. Il nome del registro viene definito dall'Ente o concordato con ParER e in generale corrisponde al nome del repertorio in cui sono registrati in ordine progressivo i documenti ad esso afferenti (ex art. 53, D.P.R. 28/12/2000 n. 445) oppure al contesto applicativo/documentale nell'ambito del quale avviene l'assegnazione dell'identificativo progressivo e univoco. Il parametro "Fiscale" indica che le unità documentarie associate al Registro sono soggette alla conservazione di tipo fiscale, finalizzata alla conservazione a norma dei documenti rilevanti ai fini tributari in conformità con quanto previsto dalla normativa di settore vigente (DM del 17 giugno 2014 del Ministero dell'economia e delle finanze)

Tipo registro	Descrizione	Periodi di validità	Descrizione formato numero	Fiscale	Data disattivazione
FATT_P	Registro delle Fatture elettroniche di ciclo passivo	2020		Si	
RUF.PROTO	Registro delle fatture passive (tipo registro della ditta e comune a tutti gli enti PAL INFORMATICA)	2015		Si	

Tabella - Elenco registri

Anno -

Numero -

Riferimento temporale -

Metadati di profilo del tipo unità documentaria - Nella Tabella Metadati di profilo dell'unità documentaria sono descritti i metadati "Data" e "Oggetto" associati all'unità documentaria

Denominazione	Descrizione
Data	
Oggetto	

Tabella - Metadati di profilo dell'unità documentaria

Metadati specifici associati al tipo unità documentaria - Nelle Tabelle Metadati specifici dell'unità documentaria è presentato il set di metadati associato all'unità documentaria nelle diverse versioni. La presenza di versioni diverse è legata alle eventuali modifiche/integrazioni/aggiornamenti nel set di metadati specifici o nelle obbligatorio concordate con l'Ente.

Versione metadati specifici: 1.0

Descrizione versione:

Data inizio validità: 04/11/2016

Data fine validità:

Denominazione	Descrizione
NumeroProtocollo	NumeroProtocollo
DataProtocollo	DataProtocollo
NumeroRUF	NumeroRUF
DataRegistrazioneRUF	DataRegistrazioneRUF
CodiceRegistroIVA	CodiceRegistroIVA
NumeroRegistroIVA	NumeroRegistroIVA
DataRegistrazioneIVA	DataRegistrazioneIVA
NumeroEmissione	NumeroEmissione
DataEmissione	DataEmissione
DenominazioneMittente	DenominazioneMittente
TipoDenominazioneMittente	TipoDenominazioneMittente
IdentificativoMittente	IdentificativoMittente

Denominazione	Descrizione
TipoidentificativoMittente	TipoidentificativoMittente
OggettoFornitura	OggettoFornitura
ImportoTotale	ImportoTotale
Scadenza	Scadenza
RiferimentoContabile	RiferimentoContabile
TipoRifContabile	TipoRifContabile
RilevanzaIVA	RilevanzaIVA
CIG	CIG
CUP	CUP
AliquotalvaReverseCharge	AliquotalvaReverseCharge
IvaTotaleReverseCharge	IvaTotaleReverseCharge

Tabella - Metadati specifici dell'unità documentaria

Versione metadati specifici: 2.0

Descrizione versione: Xsd valido per l'invio in conservazione delle Fatture Passive inviate tramite l'applicativo di Datagraph

Data inizio validità: 18/10/2023

Data fine validità:

Denominazione	Descrizione
NumeroProtocollo	NumeroProtocollo
DataProtocollo	DataProtocollo
NumeroEmissione	NumeroEmissione
DataEmissione	DataEmissione
DenominazioneMittente	DenominazioneMittente
TipoDenominazioneMittente	TipoDenominazioneMittente
IdentificativoMittente	IdentificativoMittente

Denominazione	Descrizione
TipIdentificativoMittente	TipIdentificativoMittente
OggettoFornitura	OggettoFornitura
ImportoTotale	ImportoTotale
Scadenza	Scadenza
RiferimentiContabili	RiferimentiContabili
RilevanzaIVA	RilevanzaIVA

Tabella - Metadati specifici dell'unità documentaria

Tipologia di unità documentaria ORDINANZA

Descrizione della tipologia di unità documentaria: Ordinanza

Tipi struttura dell'unità documentaria: nella Tabella Tipi struttura unità documentaria sono rappresentate le varie strutture che può assumere il tipo di unità documentaria, ovvero la sua articolazione in documento principale ed eventuali allegati, annessi e annotazioni, le informazioni relative alla chiave, ai metadati di profilo e altro ancora.

Per ogni Tipo struttura è indicato il periodo di validità, ovvero per quali annualità delle unità documentarie è valido il tipo struttura e i sistemi versanti utilizzati.

Denominazione	Descrizione	Periodi di validità	Sistemi versanti
ORDINANZA	Ordinanza		

Tabella - Tipi struttura unità documentaria

Nei paragrafi successivi sono riportate le informazioni di dettaglio su ogni singolo Tipo struttura dell'unità documentaria

Tipi struttura ORDINANZA Nella tabella è riportata l'articolazione dell'unità documentaria in documento principale ed eventuali allegati, annessi e annotazioni.

Descrizione: Ordinanza

Tipo documento	Descrizione
GENERICO	Allegato generico
ORDINANZA	Ordinanza
RELATA PUBBLICAZIONE	Attestazione di pubblicazione del documento all'Albo Pretorio

Tabella - Tipo struttura ORDINANZA_Descrizione tipi documento

Tipo documento	Elemento	Obbligatorio	Periodicità di versamento	Note
GENERICO	ALLEGATO	No		
ORDINANZA	PRINCIPALE	Si		
RELATA PUBBLICAZIONE	ANNESSO	No		

Tabella - Tipo struttura ORDINANZA_Dettaglio tipi documento

Chiave identificativa del tipo struttura dell'unità documentaria (Tipo registro - Anno - Numero)

Registri - Nella Tabella Elenco registri è rappresentata la lista dei registri associati all'unità documentaria. Il nome del registro viene definito dall'Ente o concordato con ParER e in generale corrisponde al nome del repertorio in cui sono registrati in ordine progressivo i documenti ad esso afferenti (ex art. 53, D.P.R. 28/12/2000 n. 445) oppure al contesto applicativo/documentale nell'ambito del quale avviene l'assegnazione dell'identificativo progressivo e univoco. Il parametro "Fiscale" indica che le unità documentarie associate al Registro sono soggette alla conservazione di tipo fiscale, finalizzata alla conservazione a norma dei documenti rilevanti ai fini tributari in conformità con quanto previsto dalla normativa di settore vigente (DM del 17 giugno 2014 del Ministero dell'economia e delle finanze)

Tipo registro	Descrizione	Periodi di validità	Descrizione formato numero	Fiscale	Data disattivazione
ORDI	Registro delle Ordinanze	2015		No	

Tabella - Elenco registri

Anno -

Numero -

Riferimento temporale -

Metadati di profilo del tipo unità documentaria - Nella Tabella Metadati di profilo dell'unità documentaria sono descritti i metadati "Data" e "Oggetto" associati all'unità documentaria

Denominazione	Descrizione
Data	
Oggetto	

Tabella - Metadati di profilo dell'unità documentaria

Metadati specifici associati al tipo unità documentaria - Nelle Tabelle Metadati specifici dell'unità documentaria è presentato il set di metadati associato all'unità documentaria nelle diverse versioni. La presenza di versioni diverse è legata alle eventuali modifiche/integrazioni/aggiornamenti nel set di metadati specifici o nelle obbligatorietà concordate con l'Ente.

Versione metadati specifici: 1.0

Descrizione versione:

Data inizio validità: 18/06/2015

Data fine validità:

Denominazione	Descrizione
categoria	categoria
settore	settore
materia	materia
firmatario	firmatario
firmatario_ruolo	firmatario_ruolo
note	note
registrazione_data	registrazione_data
validita_data_inizio	validita_data_inizio
validita_data_fine	validita_data_fine
soggetti_interessati	soggetti_interessati
annullato	annullato
annullamento_data	annullamento_data
annullamento_motivo	annullamento_motivo
annullamento_soggetto	annullamento_soggetto
annullamento_atto	annullamento_atto
tipologia	tipologia

Tabella - Metadati specifici dell'unità documentaria

Metadati specifici tipo documento RELATA PUBBLICAZIONE - Nelle tabelle “Metadati specifici del documento” è presentato il set di metadati specifici associato al documento nelle varie versioni. La presenza di versioni diverse è legata alle eventuali modifiche/integrazioni/aggiornamenti nel set di metadati specifici e nella obbligatorietà concordate con l'Ente.

Versione metadati specifici: 1.0

Descrizione versione:

Data inizio validità: 29/04/2014

Data fine validità:

Denominazione	Descrizione
pubblicazione_anno	pubblicazione_anno
pubblicazione_numero	pubblicazione_numero
pubblicazione_registro	pubblicazione_registro
pubblicazione_data_inizio	pubblicazione_data_inizio
pubblicazione_data_fine	pubblicazione_data_fine
ripubblicazione	ripubblicazione

Tabella - Metadati specifici del documento

Tipologia di unità documentaria PIANO ARENILE

Descrizione della tipologia di unità documentaria: Strumento Urbanistico avente ad oggetto la regolamentazione dell'uso e delle trasformazioni dell'arenile e delle costruzioni esistenti, ai sensi art. 72 L.R. 24/2017

Tipi struttura dell'unità documentaria: nella Tabella Tipi struttura unità documentaria sono rappresentate le varie strutture che può assumere il tipo di unità documentaria, ovvero la sua articolazione in documento principale ed eventuali allegati, annessi e annotazioni, le informazioni relative alla chiave, ai metadati di profilo e altro ancora.

Per ogni Tipo struttura è indicato il periodo di validità, ovvero per quali annualità delle unità documentarie è valido il tipo struttura e i sistemi versanti utilizzati.

Denominazione	Descrizione	Periodi di validità	Sistemi versanti
PIANO ARENILE	PIANO ARENILE	2017	PREINGEST

Tabella - Tipi struttura unità documentaria

Nei paragrafi successivi sono riportate le informazioni di dettaglio su ogni singolo Tipo struttura dell'unità documentaria

Tipi struttura PIANO ARENILE Nella tabella è riportata l'articolazione dell'unità documentaria in documento principale ed eventuali allegati, annessi e annotazioni.

Descrizione: PIANO ARENILE

Tipo documento	Descrizione
ALTRI ATTI RELAZIONI E PARERI	Altri atti relazioni e pareri L.R. 24/2017
DATI GEOGRAFICI	Dati geografici L.R. 24/2017
DELIBERA STRUMENTO URBANISTICO	Delibera strumento urbanistico L.R. 24/2017
ELABORATI CARTOGRAFICI	Elaborati cartografici L.R. 24/2017
OSSERVAZIONI PERVENUTE	Osservazioni pervenute L.R. 24/2017
QUADRO CONOSCITIVO	Quadro conoscitivo L.R. 24/2017
SCHEMA DI ASSETTO DEL TERRITORIO URBANIZZATO	Schema di assetto del territorio urbanizzato L.R. 24/2017
STRATEGIA PER LA QUALITÀ URBANA ED ECOLOGICO-AMBIENTALE	Strategia per la qualità urbana ed ecologico-ambientale L.R. 24/2017
TAVOLA E SCHEDA DEI VINCOLI	Tavola e scheda dei vincoli L.R. 24/2017
VALSAT	Valsat L.R. 24/2017

Tabella - Tipo struttura PIANO ARENILE_Descrizione tipi documento

Tipo documento	Elemento	Obbligatorio	Periodicità di versamento	Note
ALTRI ATTI RELAZIONI E PARERI	ALLEGATO	No		
DATI GEOGRAFICI	ALLEGATO	No		
DELIBERA STRUMENTO URBANISTICO	PRINCIPALE	Si		
ELABORATI CARTOGRAFICI	ALLEGATO	No		
OSSERVAZIONI PERVENUTE	ALLEGATO	No		
QUADRO CONOSCITIVO	ALLEGATO	No		
SCHEMA DI ASSETTO DEL TERRITORIO URBANIZZATO	ALLEGATO	No		
STRATEGIA PER LA QUALITÀ URBANA ED ECOLOGICO-AMBIENTALE	ALLEGATO	No		
TAVOLA E SCHEDA DEI VINCOLI	ALLEGATO	No		
VALSAT	ALLEGATO	No		

Tabella - Tipo struttura PIANO ARENILE_Dettaglio tipi documento**Chiave identificativa del tipo struttura dell'unità documentaria (Tipo registro - Anno - Numero)**

Registri - Nella Tabella Elenco registri è rappresentata la lista dei registri associati all'unità documentaria. Il nome del registro viene definito dall'Ente o concordato con ParER e in generale corrisponde al nome del repertorio in cui sono registrati in ordine progressivo i documenti ad esso afferenti (ex art. 53, D.P.R. 28/12/2000 n. 445) oppure al contesto applicativo/documentale nell'ambito del quale avviene l'assegnazione dell'identificativo progressivo e univoco. Il parametro "Fiscale" indica che le unità documentarie associate al Registro sono soggette alla conservazione di tipo fiscale, finalizzata alla conservazione a norma dei documenti rilevanti ai fini tributari in conformità con quanto previsto dalla normativa di settore vigente (DM del 17 giugno 2014 del Ministero dell'economia e delle finanze)

Tipo registro	Descrizione	Periodi di validità	Descrizione formato numero	Fiscale	Data disattivazione
STRUMENTI URBANISTICI	Registro per gli Strumenti Urbanistici	2017	Il numero è composto da una sigla che identifica il tipo di atto con cui è stato approvato lo strumento e dal numero di registrazione assegnato. Le sigle utilizzate sono DCC (Delibera Consiglio Comunale), DCU (Delibera Consiglio Unione), DGC (Delibera Giunta Comunale), DGU (Delibera Giunta Unione), PROT (Documento Protocollato). Il numero corrisponde al numero di registrazione nel repertorio delle delibere oppure al numero di protocollo.	No	

Tabella - Elenco registri

Anno - Anno solare di riferimento del repertorio

Numero - Numero della delibera con la quale è stato approvato l'atto, composto da una sigla che individua la tipologia dell'organo deliberante (DCC: Delibera Consiglio Comunale, DCU: Delibera Consiglio Unione, DGC: Delibera Giunta Comunale, DGU: Delibera Giunta Unione) e dal numero di repertorio, es. DCC_nnn

Riferimento temporale -

Metadati di profilo del tipo unità documentaria - Nella Tabella Metadati di profilo dell'unità documentaria sono descritti i metadati "Data" e "Oggetto" associati all'unità documentaria

Denominazione	Descrizione
Data	Data della Deliberazione che coincide con la data di seduta dell'Organo collegiale deliberante
Oggetto	Oggetto dello Strumento Urbanistico generato dal sistema, composto da nome dell'ente convenzionato, tipologia unità documentaria, anno, numero e data

Tabella - Metadati di profilo dell'unità documentaria

Collegamenti tra unità documentarie : l'unità documentaria costituita dal Piano dell'arenile approvato può essere collegata alla unità documentaria costituita dal Piano dell'arenile assunto e/o adottato e viceversa.

Metadati specifici associati al tipo unità documentaria - Nelle Tabelle Metadati specifici dell'unità documentaria è presentato il set di metadati associato all'unità documentaria nelle diverse versioni. La presenza di versioni diverse è legata alle eventuali modifiche/integrazioni/aggiornamenti nel set di metadati specifici o nelle obbligatorio concordate con l'Ente.

Versione metadati specifici: 1.0

Descrizione versione:

Data inizio validità: 14/10/2019

Data fine validità:

Denominazione	Descrizione
tipo_ente	tipo_ente
ente_convenzionato	ente_convenzionato
unione_comuni	unione_comuni
provincia_ente	provincia_ente
fase_elaborazione_strumento	fase_elaborazione_strumento

Tabella - Metadati specifici dell'unità documentaria

Tipologia di unità documentaria PIANO ATTUATIVO DI INIZIATIVA PUBBLICA

Descrizione della tipologia di unità documentaria: Strumento urbanistico del quale l'ente può dotarsi per gli ambiti che presentano un particolare valore sotto il profilo paesaggistico o che sono caratterizzati da una significativa carenza di fattori identitari, ai sensi art. 38 c. 17 L.R. 24/2017

Tipi struttura dell'unità documentaria: nella Tabella Tipi struttura unità documentaria sono rappresentate le varie strutture che può assumere il tipo di unità documentaria, ovvero la sua articolazione in documento principale ed eventuali allegati, annessi e annotazioni, le informazioni relative alla chiave, ai metadati di profilo e altro ancora.
Per ogni Tipo struttura è indicato il periodo di validità, ovvero per quali annualità delle unità documentarie è valido il tipo struttura e i sistemi versanti utilizzati.

Denominazione	Descrizione	Periodi di validità	Sistemi versanti
PIANO ATTUATIVO DI INIZIATIVA PUBBLICA		2017	PREINGEST

Tabella - Tipi struttura unità documentaria

Nei paragrafi successivi sono riportate le informazioni di dettaglio su ogni singolo Tipo struttura dell'unità documentaria

Tipo struttura PIANO ATTUATIVO DI INIZIATIVA PUBBLICA Nella tabella è riportata l'articolazione dell'unità documentaria in documento principale ed eventuali allegati, annessi e annotazioni.

Tipo documento	Descrizione
ALTRI ATTI RELAZIONI E PARERI	Altri atti relazioni e pareri L.R. 24/2017
ATTI NEGOZIALI E RELAZIONE ECONOMICO-FINANZIARIA	Atti negoziali e relazione economico-finanziaria L.R. 24/2017
DATI GEOGRAFICI	Dati geografici L.R. 24/2017
DELIBERA STRUMENTO URBANISTICO	Delibera strumento urbanistico L.R. 24/2017
ELABORATI CARTOGRAFICI	Elaborati cartografici L.R. 24/2017
VALSAT	Valsat L.R. 24/2017

Tabella - Tipo struttura PIANO ATTUATIVO DI INIZIATIVA PUBBLICA_Descrizione tipi documento

Tipo documento	Elemento	Obbligatorio	Periodicità di versamento	Note
ALTRI ATTI RELAZIONI E PARERI	ALLEGATO	No		
ATTI NEGOZIALI E RELAZIONE ECONOMICO-FINANZIARIA	ALLEGATO	No		
DATI GEOGRAFICI	ALLEGATO	No		
DELIBERA STRUMENTO URBANISTICO	PRINCIPALE	Si		
ELABORATI CARTOGRAFICI	ALLEGATO	No		
VALSAT	ALLEGATO	No		

Tabella - Tipo struttura PIANO ATTUATIVO DI INIZIATIVA PUBBLICA_Dettaglio tipi documento

Chiave identificativa del tipo struttura dell'unità documentaria (Tipo registro - Anno - Numero)

Registri - Nella Tabella Elenco registri è rappresentata la lista dei registri associati all'unità documentaria. Il nome del registro viene definito dall'Ente o concordato con ParER e in generale corrisponde al nome del repertorio in cui sono registrati in ordine progressivo i documenti ad esso afferenti (ex art. 53, D.P.R. 28/12/2000 n. 445) oppure al contesto applicativo/documentale nell'ambito del quale avviene l'assegnazione dell'identificativo progressivo e univoco. Il parametro "Fiscale" indica che le unità documentarie associate al Registro sono soggette alla conservazione di tipo fiscale, finalizzata alla conservazione a norma dei documenti rilevanti ai fini tributari in conformità con quanto previsto dalla normativa di settore vigente (DM del 17 giugno 2014 del Ministero dell'economia e delle finanze)

Tipo registro	Descrizione	Periodi di validità	Descrizione formato numero	Fiscale	Data disattivazione
STRUMENTI URBANISTICI	Registro per gli Strumenti Urbanistici	2017	Il numero è composto da una sigla che identifica il tipo di atto con cui è stato approvato lo strumento e dal numero di registrazione assegnato. Le sigle utilizzate sono DCC (Delibera Consiglio Comunale), DCU (Delibera Consiglio Unione), DGC	No	

Tipo registro	Descrizione	Periodi di validità	Descrizione formato numero	Fiscale	Data disattivazione
			(Delibera Giunta Comunale), DGU (Delibera Giunta Unione), PROT (Documento Protocollato). Il numero corrisponde al numero di registrazione nel repertorio delle delibere oppure al numero di protocollo.		

Tabella - Elenco registri

Anno - Anno solare di riferimento del repertorio

Numero - Numero della delibera con la quale è stato approvato l'atto, composto da una sigla che individua la tipologia dell'organo deliberante (DCC: Delibera Consiglio Comunale, DCU: Delibera Consiglio Unione, DGC: Delibera Giunta Comunale, DGU: Delibera Giunta Unione) e dal numero di repertorio, es. DCC_nnn

Riferimento temporale -

Metadati di profilo del tipo unità documentaria - Nella Tabella Metadati di profilo dell'unità documentaria sono descritti i metadati "Data" e "Oggetto" associati all'unità documentaria

Denominazione	Descrizione
Data	Data della Deliberazione che coincide con la data di seduta dell'Organo collegiale deliberante
Oggetto	Oggetto dello Strumento Urbanistico generato dal sistema, composto da nome dell'ente convenzionato, tipologia unità documentaria, anno, numero e data

Tabella - Metadati di profilo dell'unità documentaria

Collegamenti tra unità documentarie : l'unità documentaria costituita dal Piano attuativo di iniziativa pubblica approvato può essere collegata alla unità documentaria costituita dal Piano attuativo di iniziativa pubblica assunto e/o adottato e viceversa.

Metadati specifici associati al tipo unità documentaria - Nelle Tabelle Metadati specifici dell'unità documentaria è presentato il set di metadati associato all'unità documentaria nelle diverse versioni. La presenza di versioni diverse è legata alle eventuali modifiche/integrazioni/aggiornamenti nel set di metadati specifici o nelle obbligatorioità concordate con l'Ente.

Versione metadati specifici: 1.0

Descrizione versione:

Data inizio validità: 10/10/2019

Data fine validità:

Denominazione	Descrizione
tipo_ente	tipo_ente
ente_convenzionato	ente_convenzionato
unione_comuni	unione_comuni
provincia_ente	provincia_ente
fase_elaborazione_strumento	fase_elaborazione_strumento

Tabella - Metadati specifici dell'unità documentaria

Tipologia di unità documentaria PIANO SETTORIALE

Descrizione della tipologia di unità documentaria: Strumento Urbanistico di valenza settoriale, ai sensi art. 50 L.R. 24/2017

Tipi struttura dell'unità documentaria: nella Tabella Tipi struttura unità documentaria sono rappresentate le varie strutture che può assumere il tipo di unità documentaria, ovvero la sua articolazione in documento principale ed eventuali allegati, annessi e annotazioni, le informazioni relative alla chiave, ai metadati di profilo e altro ancora.

Per ogni Tipo struttura è indicato il periodo di validità, ovvero per quali annualità delle unità documentarie è valido il tipo struttura e i sistemi versanti utilizzati.

Denominazione	Descrizione	Periodi di validità	Sistemi versanti
PIANO SETTORIALE		2017	PREINGEST

Tabella - Tipi struttura unità documentaria

Nei paragrafi successivi sono riportate le informazioni di dettaglio su ogni singolo Tipo struttura dell'unità documentaria

Tipi struttura PIANO SETTORIALE Nella tabella è riportata l'articolazione dell'unità documentaria in documento principale ed eventuali allegati, annessi e annotazioni.

Tipo documento	Descrizione
ALTRI ATTI RELAZIONI E PARERI	Altri atti relazioni e pareri L.R. 24/2017
DATI GEOGRAFICI	Dati geografici L.R. 24/2017
DELIBERA STRUMENTO URBANISTICO	Delibera strumento urbanistico L.R. 24/2017
ELABORATI CARTOGRAFICI	Elaborati cartografici L.R. 24/2017
OSSERVAZIONI PERVENUTE	Osservazioni pervenute L.R. 24/2017
QUADRO CONOSCITIVO	Quadro conoscitivo L.R. 24/2017
SCHEMA DI ASSETTO DEL TERRITORIO URBANIZZATO	Schema di assetto del territorio urbanizzato L.R. 24/2017
STRATEGIA PER LA QUALITÀ URBANA ED ECOLOGICO-AMBIENTALE	Strategia per la qualità urbana ed ecologico-ambientale L.R. 24/2017
TAVOLA E SCHEDA DEI VINCOLI	Tavola e scheda dei vincoli L.R. 24/2017
VALSAT	Valsat L.R. 24/2017

Tabella - Tipi struttura PIANO SETTORIALE_Descrizione tipi documento

Tipo documento	Elemento	Obbligatorio	Periodicità di versamento	Note
ALTRI ATTI RELAZIONI E PARERI	ALLEGATO	No		
DATI GEOGRAFICI	ALLEGATO	No		
DELIBERA STRUMENTO URBANISTICO	PRINCIPALE	Si		
ELABORATI CARTOGRAFICI	ALLEGATO	No		
OSSERVAZIONI PERVENUTE	ALLEGATO	No		
QUADRO CONOSCITIVO	ALLEGATO	No		
SCHEMA DI ASSETTO DEL TERRITORIO URBANIZZATO	ALLEGATO	No		
STRATEGIA PER LA QUALITÀ URBANA ED ECOLOGICO-AMBIENTALE	ALLEGATO	No		
TAVOLA E SCHEDA DEI VINCOLI	ALLEGATO	No		
VALSAT	ALLEGATO	No		

Tabella - Tipo struttura PIANO SETTORIALE_Dettaglio tipi documento

Chiave identificativa del tipo struttura dell'unità documentaria (Tipo registro - Anno - Numero)

Registri - Nella Tabella Elenco registri è rappresentata la lista dei registri associati all'unità documentaria. Il nome del registro viene definito dall'Ente o concordato con ParER e in generale corrisponde al nome del repertorio in cui sono registrati in ordine progressivo i documenti ad esso afferenti (ex art. 53, D.P.R. 28/12/2000 n. 445) oppure al contesto applicativo/documentale nell'ambito del quale avviene l'assegnazione dell'identificativo progressivo e univoco. Il parametro "Fiscale" indica che le unità documentarie associate al Registro sono soggette alla conservazione di tipo fiscale, finalizzata alla conservazione a norma dei documenti rilevanti ai fini tributari in conformità con quanto previsto dalla normativa di settore vigente (DM del 17 giugno 2014 del Ministero dell'economia e delle finanze)

Tipo registro	Descrizione	Periodi di validità	Descrizione formato numero	Fiscale	Data disattivazione
STRUMENTI URBANISTICI	Registro per gli Strumenti Urbanistici	2017	Il numero è composto da una sigla che identifica il tipo di atto con cui è stato approvato lo strumento e dal numero di registrazione assegnato. Le sigle utilizzate sono DCC (Delibera Consiglio Comunale), DCU (Delibera Consiglio Unione), DGC (Delibera Giunta Comunale), DGU (Delibera Giunta Unione), PROT (Documento Protocollato). Il numero corrisponde al numero di registrazione nel repertorio delle delibere oppure al numero di protocollo.	No	

Tabella - Elenco registri

Anno - Anno solare di riferimento del repertorio

Numero - Numero della delibera con la quale è stato approvato l'atto, composto da una sigla che individua la tipologia dell'organo deliberante (DCC: Delibera Consiglio Comunale, DCU: Delibera Consiglio Unione, DGC: Delibera Giunta Comunale, DGU: Delibera Giunta Unione) e dal numero di repertorio, es. DCC_nnn

Riferimento temporale -

Metadati di profilo del tipo unità documentaria - Nella Tabella Metadati di profilo dell'unità documentaria sono descritti i metadati "Data" e "Oggetto" associati all'unità documentaria

Denominazione	Descrizione
Data	Data della Deliberazione che coincide con la data di seduta dell'Organo collegiale deliberante
Oggetto	Oggetto dello Strumento Urbanistico generato dal sistema, composto da nome dell'ente convenzionato, tipologia unità documentaria, anno, numero e data

Tabella - Metadati di profilo dell'unità documentaria

Collegamenti tra unità documentarie : l'unità documentaria costituita dal Piano settoriale approvato può essere collegata alla unità documentaria costituita dal Piano settoriale assunto e/o adottato e viceversa.

Metadati specifici associati al tipo unità documentaria - Nelle Tabelle Metadati specifici dell'unità documentaria è presentato il set di metadati associato all'unità documentaria nelle diverse versioni. La presenza di versioni diverse è legata alle eventuali modifiche/integrazioni/aggiornamenti nel set di metadati specifici o nelle obbligatorio concordate con l'Ente.

Versione metadati specifici: 1.0

Descrizione versione:

Data inizio validità: 10/10/2019

Data fine validità:

Denominazione	Descrizione
tipo_ente	tipo_ente
ente_convenzionato	ente_convenzionato
unione_comuni	unione_comuni
provincia_ente	provincia_ente
fase_elaborazione_strumento	fase_elaborazione_strumento

Tabella - Metadati specifici dell'unità documentaria

Tipologia di unità documentaria PIANO URBANISTICO GENERALE

Descrizione della tipologia di unità documentaria: Strumento urbanistico che il Comune o l'Unione di Comuni predispone, con riferimento a tutto il proprio territorio, per delimitare le invarianze strutturali e le scelte strategiche di assetto e sviluppo urbano, ai sensi art. 30 L.R. 24/2017

Tipi struttura dell'unità documentaria: nella Tabella Tipi struttura unità documentaria sono rappresentate le varie strutture che può assumere il tipo di unità documentaria, ovvero la sua articolazione in documento principale ed eventuali allegati, annessi e annotazioni, le informazioni relative alla chiave, ai metadati di profilo e altro ancora.

Per ogni Tipo struttura è indicato il periodo di validità, ovvero per quali annualità delle unità documentarie è valido il tipo struttura e i sistemi versanti utilizzati.

Denominazione	Descrizione	Periodi di validità	Sistemi versanti
PIANO URBANISTICO GENERALE		2017	PREINGEST

Tabella - Tipi struttura unità documentaria

Nei paragrafi successivi sono riportate le informazioni di dettaglio su ogni singolo Tipo struttura dell'unità documentaria

Tipologia struttura PIANO URBANISTICO GENERALE Nella tabella è riportata l'articolazione dell'unità documentaria in documento principale ed eventuali allegati, annessi e annotazioni.

Tipo documento	Descrizione
ALTRI ATTI RELAZIONI E PARERI	Altri atti relazioni e pareri L.R. 24/2017
DATI GEOGRAFICI	Dati geografici L.R. 24/2017
DELIBERA STRUMENTO URBANISTICO	Delibera strumento urbanistico L.R. 24/2017
ELABORATI CARTOGRAFICI	Elaborati cartografici L.R. 24/2017
OSSERVAZIONI PERVENUTE	Osservazioni pervenute L.R. 24/2017
QUADRO CONOSCITIVO	Quadro conoscitivo L.R. 24/2017
SCHEMA DI ASSETTO DEL TERRITORIO URBANIZZATO	Schema di assetto del territorio urbanizzato L.R. 24/2017
STRATEGIA PER LA QUALITÀ URBANA ED ECOLOGICO-AMBIENTALE	Strategia per la qualità urbana ed ecologico-ambientale L.R. 24/2017
TAVOLA E SCHEDA DEI VINCOLI	Tavola e scheda dei vincoli L.R. 24/2017
VALSAT	Valsat L.R. 24/2017

Tabella - Tipologia struttura PIANO URBANISTICO GENERALE_Descrizione tipi documento

Tipo documento	Elemento	Obbligatorio	Periodicità di versamento	Note
ALTRI ATTI RELAZIONI E PARERI	ALLEGATO	No		
DATI GEOGRAFICI	ALLEGATO	No		
DELIBERA STRUMENTO URBANISTICO	PRINCIPALE	Si		
ELABORATI CARTOGRAFICI	ALLEGATO	No		
OSSERVAZIONI PERVENUTE	ALLEGATO	No		
QUADRO CONOSCITIVO	ALLEGATO	No		
SCHEMA DI ASSETTO DEL TERRITORIO URBANIZZATO	ALLEGATO	No		
STRATEGIA PER LA QUALITÀ URBANA ED ECOLOGICO-AMBIENTALE	ALLEGATO	No		
TAVOLA E SCHEDA DEI VINCOLI	ALLEGATO	No		
VALSAT	ALLEGATO	No		

Tabella - Tipo struttura PIANO URBANISTICO GENERALE_Dettaglio tipi documento

Chiave identificativa del tipo struttura dell'unità documentaria (Tipo registro - Anno - Numero)

Registri - Nella Tabella Elenco registri è rappresentata la lista dei registri associati all'unità documentaria. Il nome del registro viene definito dall'Ente o concordato con ParER e in generale corrisponde al nome del repertorio in cui sono registrati in ordine progressivo i documenti ad esso afferenti (ex art. 53, D.P.R. 28/12/2000 n. 445) oppure al contesto applicativo/documentale nell'ambito del quale avviene l'assegnazione dell'identificativo progressivo e univoco. Il parametro "Fiscale" indica che le unità documentarie associate al Registro sono soggette alla conservazione di tipo fiscale, finalizzata alla conservazione a norma dei documenti rilevanti ai fini tributari in conformità con quanto previsto dalla normativa di settore vigente (DM del 17 giugno 2014 del Ministero dell'economia e delle finanze)

Tipo registro	Descrizione	Periodi di validità	Descrizione formato numero	Fiscale	Data disattivazione
STRUMENTI URBANISTICI	Registro per gli Strumenti Urbanistici	2017	Il numero è composto da una sigla che identifica il tipo di atto con cui è stato approvato lo strumento e dal numero di registrazione assegnato. Le sigle utilizzate sono DCC (Delibera Consiglio Comunale), DCU (Delibera Consiglio Unione), DGC (Delibera Giunta Comunale), DGU (Delibera Giunta Unione), PROT (Documento Protocollato). Il numero corrisponde al numero di registrazione nel repertorio delle delibere oppure al numero di protocollo.	No	

Tabella - Elenco registri

Anno - Anno solare di riferimento del repertorio

Numero - Numero della delibera con la quale è stato approvato l'atto, composto da una sigla che individua la tipologia dell'organo deliberante (DCC: Delibera Consiglio Comunale, DCU: Delibera Consiglio Unione, DGC: Delibera Giunta Comunale, DGU: Delibera Giunta Unione) e dal numero di repertorio, es. DCC_nnn

Riferimento temporale -

Metadati di profilo del tipo unità documentaria - Nella Tabella Metadati di profilo dell'unità documentaria sono descritti i metadati "Data" e "Oggetto" associati all'unità documentaria

Denominazione	Descrizione
Data	Data della Deliberazione che coincide con la data di seduta dell'Organo collegiale deliberante
Oggetto	Oggetto dello Strumento Urbanistico generato dal sistema, composto da nome dell'ente convenzionato, tipologia unità documentaria, anno, numero e data

Tabella - Metadati di profilo dell'unità documentaria

Collegamenti tra unità documentarie : L'unità documentaria costituita dal Piano urbanistico generale approvato può essere collegata alla unità documentaria costituita dal Piano urbanistico generale assunto e/o adottato e viceversa.

Metadati specifici associati al tipo unità documentaria - Nelle Tabelle Metadati specifici dell'unità documentaria è presentato il set di metadati associato all'unità documentaria nelle diverse versioni. La presenza di versioni diverse è legata alle eventuali modifiche/integrazioni/aggiornamenti nel set di metadati specifici o nelle obbligatorio concordate con l'Ente.

Versione metadati specifici: 1.0

Descrizione versione:

Data inizio validità: 10/10/2019

Data fine validità:

Denominazione	Descrizione
tipo_ente	tipo_ente
ente_convenzionato	ente_convenzionato
unione_comuni	unione_comuni
provincia_ente	provincia_ente
fase_elaborazione_strumento	fase_elaborazione_strumento

Tabella - Metadati specifici dell'unità documentaria

Tipologia di unità documentaria PROCEDIMENTO UNICO

Descrizione della tipologia di unità documentaria: Strumento urbanistico promosso per l'approvazione del progetto definitivo o esecutivo di opere pubbliche ai sensi dell'art. 53 L.R. 24/2017

Tipi struttura dell'unità documentaria: nella Tabella Tipi struttura unità documentaria sono rappresentate le varie strutture che può assumere il tipo di unità documentaria, ovvero la sua articolazione in documento principale ed eventuali allegati, annessi e annotazioni, le informazioni relative alla chiave, ai metadati di profilo e altro ancora.

Per ogni Tipo struttura è indicato il periodo di validità, ovvero per quali annualità delle unità documentarie è valido il tipo struttura e i sistemi versanti utilizzati.

Denominazione	Descrizione	Periodi di validità	Sistemi versanti
PROCEDIMENTO UNICO		2017	PREINGEST

Tabella - Tipi struttura unità documentaria

Nei paragrafi successivi sono riportate le informazioni di dettaglio su ogni singolo Tipo struttura dell'unità documentaria

Tipo struttura PROCEDIMENTO UNICO Nella tabella è riportata l'articolazione dell'unità documentaria in documento principale ed eventuali allegati, annessi e annotazioni.

Tipo documento	Descrizione
ALTRI ATTI RELAZIONI E PARERI	Altri atti relazioni e pareri L.R. 24/2017
ATTO DELLA CONFERENZA DEI SERVIZI	Atto della conferenza dei servizi L.R. 24/2017
DATI GEOGRAFICI	Dati geografici L.R. 24/2017
ELABORATI CARTOGRAFICI	Elaborati cartografici L.R. 24/2017

Tabella - Tipo struttura PROCEDIMENTO UNICO_Descrizione tipi documento

Tipo documento	Elemento	Obbligatorio	Periodicità di versamento	Note
ALTRI ATTI RELAZIONI E PARERI	ALLEGATO	No		
ATTO DELLA CONFERENZA DEI SERVIZI	PRINCIPALE	Si		

Tipo documento	Elemento	Obbligatorio	Periodicità di versamento	Note
DATI GEOGRAFICI	ALLEGATO	No		
ELABORATI CARTOGRAFICI	ALLEGATO	No		

Tabella - Tipo struttura PROCEDIMENTO UNICO_Dettaglio tipi documento

Chiave identificativa del tipo struttura dell'unità documentaria (Tipo registro - Anno - Numero)

Registri - Nella Tabella Elenco registri è rappresentata la lista dei registri associati all'unità documentaria. Il nome del registro viene definito dall'Ente o concordato con ParER e in generale corrisponde al nome del repertorio in cui sono registrati in ordine progressivo i documenti ad esso afferenti (ex art. 53, D.P.R. 28/12/2000 n. 445) oppure al contesto applicativo/documentale nell'ambito del quale avviene l'assegnazione dell'identificativo progressivo e univoco. Il parametro "Fiscale" indica che le unità documentarie associate al Registro sono soggette alla conservazione di tipo fiscale, finalizzata alla conservazione a norma dei documenti rilevanti ai fini tributari in conformità con quanto previsto dalla normativa di settore vigente (DM del 17 giugno 2014 del Ministero dell'economia e delle finanze)

Tipo registro	Descrizione	Periodi di validità	Descrizione formato numero	Fiscale	Data disattivazione
STRUMENTI URBANISTICI	Registro per gli Strumenti Urbanistici	2017	Il numero è composto da una sigla che identifica il tipo di atto con cui è stato approvato lo strumento e dal numero di registrazione assegnato. Le sigle utilizzate sono DCC (Delibera Consiglio Comunale), DCU (Delibera Consiglio Unione), DGC (Delibera Giunta Comunale), DGU (Delibera Giunta Unione), PROT (Documento Protocollato). Il numero corrisponde al numero di registrazione nel repertorio delle delibere oppure al numero di protocollo.	No	

Tabella - Elenco registri

Anno - Anno solare di riferimento del repertorio

Numero - Numero di protocollo assegnato al documento, strutturato nella forma PROT_nnn

Riferimento temporale -

Metadati di profilo del tipo unità documentaria - Nella Tabella Metadati di profilo dell'unità documentaria sono descritti i metadati "Data" e "Oggetto" associati all'unità documentaria

Denominazione	Descrizione
Data	Data di protocollazione
Oggetto	Oggetto dello Strumento Urbanistico generato dal sistema, composto da nome dell'ente convenzionato, tipologia unità documentaria, anno, numero e data

Tabella - Metadati di profilo dell'unità documentaria

Collegamenti tra unità documentarie : L'unità documentaria costituita dal Procedimento unico chiuso può essere collegata alla unità documentaria costituita dal Procedimento unico aperto e viceversa.

Metadati specifici associati al tipo unità documentaria - Nelle Tabelle Metadati specifici dell'unità documentaria è presentato il set di metadati associato all'unità documentaria nelle diverse versioni. La presenza di versioni diverse è legata alle eventuali modifiche/integrazioni/aggiornamenti nel set di metadati specifici o nelle obbligatorio concordate con l'Ente.

Versione metadati specifici: 1.0

Descrizione versione:

Data inizio validità: 10/10/2019

Data fine validità:

Denominazione	Descrizione
tipo_ente	tipo_ente
ente_convenzionato	ente_convenzionato
unione_comuni	unione_comuni
provincia_ente	provincia_ente

Denominazione	Descrizione
fase_elaborazione_strumento	fase_elaborazione_strumento

Tabella - Metadati specifici dell'unità documentaria

Tipologia di unità documentaria REGISTRO GIORNALIERO

Descrizione della tipologia di unità documentaria: Elenco delle operazioni giornaliere di protocollo

Tipi struttura dell'unità documentaria: nella Tabella Tipi struttura unità documentaria sono rappresentate le varie strutture che può assumere il tipo di unità documentaria, ovvero la sua articolazione in documento principale ed eventuali allegati, annessi e annotazioni, le informazioni relative alla chiave, ai metadati di profilo e altro ancora.

Per ogni Tipo struttura è indicato il periodo di validità, ovvero per quali annualità delle unità documentarie è valido il tipo struttura e i sistemi versanti utilizzati.

Denominazione	Descrizione	Periodi di validità	Sistemi versanti
REGISTRO GIORNALIERO	Struttura UD del REGISTRO GIORNALIERO		

Tabella - Tipi struttura unità documentaria

Nei paragrafi successivi sono riportate le informazioni di dettaglio su ogni singolo Tipo struttura dell'unità documentaria

Tipologia struttura REGISTRO GIORNALIERO Nella tabella è riportata l'articolazione dell'unità documentaria in documento principale ed eventuali allegati, annessi e annotazioni.

Descrizione: Struttura UD del REGISTRO GIORNALIERO

Tipo documento	Descrizione
GENERICO	Allegato generico
REGISTRO GIORNALIERO	Registro contenente l'elenco delle registrazioni giornaliere di protocollo

Tabella - Tipo struttura REGISTRO GIORNALIERO_Descrizione tipi documento

Tipo documento	Elemento	Obbligatorio	Periodicità di versamento	Note
GENERICO	ANNESSO	No		
GENERICO	ALLEGATO	No		
REGISTRO GIORNALIERO	PRINCIPALE	Si		

Tabella - Tipo struttura REGISTRO GIORNALIERO_Dettaglio tipi documento

Chiave identificativa del tipo struttura dell'unità documentaria (Tipo registro - Anno - Numero)

Registri - Nella Tabella Elenco registri è rappresentata la lista dei registri associati all'unità documentaria. Il nome del registro viene definito dall'Ente o concordato con ParER e in generale corrisponde al nome del repertorio in cui sono registrati in ordine progressivo i documenti ad esso afferenti (ex art. 53, D.P.R. 28/12/2000 n. 445) oppure al contesto applicativo/documentale nell'ambito del quale avviene l'assegnazione dell'identificativo progressivo e univoco. Il parametro "Fiscale" indica che le unità documentarie associate al Registro sono soggette alla conservazione di tipo fiscale, finalizzata alla conservazione a norma dei documenti rilevanti ai fini tributari in conformità con quanto previsto dalla normativa di settore vigente (DM del 17 giugno 2014 del Ministero dell'economia e delle finanze)

Tipo registro	Descrizione	Periodi di validità	Descrizione formato numero	Fiscale	Data disattivazione
RGP	Registro giornaliero di protocollo	2015		No	

Tabella - Elenco registri

Anno -

Numero -

Riferimento temporale -

Metadati di profilo del tipo unità documentaria - Nella Tabella Metadati di profilo dell'unità documentaria sono descritti i metadati "Data" e "Oggetto" associati all'unità documentaria

Denominazione	Descrizione
Data	
Oggetto	

Tabella - Metadati di profilo dell'unità documentaria

Metadati specifici associati al tipo unità documentaria - Nelle Tabelle Metadati specifici dell'unità documentaria è presentato il set di metadati associato all'unità documentaria nelle diverse versioni. La presenza di versioni diverse è legata alle eventuali modifiche/integrazioni/aggiornamenti nel set di metadati specifici o nelle obbligatorietà concordate con l'Ente.

Versione metadati specifici: 1.0

Descrizione versione:

Data inizio validità: 09/12/2015

Data fine validità:

Denominazione	Descrizione
NumeroIniziale	NumeroIniziale
NumeroFinale	NumeroFinale
DataInizioRegistrazioni	DataInizioRegistrazioni
DataFineRegistrazioni	DataFineRegistrazioni
Originatore	Originatore
Responsabile	Responsabile
Operatore	Operatore
NumeroDocumentiRegistrati	NumeroDocumentiRegistrati
NumeroDocumentiAnnullati	NumeroDocumentiAnnullati
NumeroDocumentiModificati	NumeroDocumentiModificati
DenominazioneApplicativo	DenominazioneApplicativo
VersioneApplicativo	VersioneApplicativo
ProduttoreApplicativo	ProduttoreApplicativo
DenominazioneSistemaGestioneBaseDati	DenominazioneSistemaGestioneBaseDati
VersioneSistemaGestioneBaseDati	VersioneSistemaGestioneBaseDati
ProduttoreSistemaGestioneBaseDati	ProduttoreSistemaGestioneBaseDati
TempoConservazione	TempoConservazione

Tabella - Metadati specifici dell'unità documentaria

Tipologia di unità documentaria REGISTRO UNICO FATTURE

Descrizione della tipologia di unità documentaria: Registro delle fatture passive (stampa del registro annuale)

Tipi struttura dell'unità documentaria: nella Tabella Tipi struttura unità documentaria sono rappresentate le varie strutture che può assumere il tipo di unità documentaria, ovvero la sua articolazione in documento principale ed eventuali allegati, annessi e annotazioni, le informazioni relative alla chiave, ai metadati di profilo e altro ancora.

Per ogni Tipo struttura è indicato il periodo di validità, ovvero per quali annualità delle unità documentarie è valido il tipo struttura e i sistemi versanti utilizzati.

Denominazione	Descrizione	Periodi di validità	Sistemi versanti
REGISTRO UNICO FATTURE	Struttura UD del REGISTRO UNICO FATTURE		

Tabella - Tipi struttura unità documentaria

Nei paragrafi successivi sono riportate le informazioni di dettaglio su ogni singolo Tipo struttura dell'unità documentaria

Tipologia struttura REGISTRO UNICO FATTURE Nella tabella è riportata l'articolazione dell'unità documentaria in documento principale ed eventuali allegati, annessi e annotazioni.

Descrizione: Struttura UD del REGISTRO UNICO FATTURE

Tipo documento	Descrizione
REGISTRO UNICO FATTURE	Registro unico delle fatture passive

Tabella - Tipo struttura REGISTRO UNICO FATTURE_Descrizione tipi documento

Tipo documento	Elemento	Obbligatorio	Periodicità di versamento	Note
REGISTRO UNICO FATTURE	PRINCIPALE	Si		

Tabella - Tipo struttura REGISTRO UNICO FATTURE_Dettaglio tipi documento

Chiave identificativa del tipo struttura dell'unità documentaria (Tipo registro - Anno - Numero)

Registri - Nella Tabella Elenco registri è rappresentata la lista dei registri associati all'unità documentaria. Il nome del registro viene definito dall'Ente o concordato con ParER e in generale corrisponde al nome del repertorio in cui sono registrati in ordine progressivo i documenti ad esso afferenti (ex art. 53, D.P.R. 28/12/2000 n. 445) oppure al contesto applicativo/documentale nell'ambito del quale avviene l'assegnazione dell'identificativo progressivo e univoco.

Il parametro "Fiscale" indica che le unità documentarie associate al Registro sono soggette alla conservazione di tipo fiscale, finalizzata alla conservazione a norma dei documenti rilevanti ai fini tributari in conformità con quanto previsto dalla normativa di settore vigente (DM del 17 giugno 2014 del Ministero dell'economia e delle finanze)

Tipo registro	Descrizione	Periodi di validità	Descrizione formato numero	Fiscale	Data disattivazione
RUF	Registro delle fatture (stampa del registro annuale) (tipo registro della ditta e comune a tutti gli enti PAL INFORMATICA)	2015		No	

Tabella - Elenco registri

Anno -

Numero -

Riferimento temporale -

Metadati di profilo del tipo unità documentaria - Nella Tabella Metadati di profilo dell'unità documentaria sono descritti i metadati "Data" e "Oggetto" associati all'unità documentaria

Denominazione	Descrizione
Data	
Oggetto	

Tabella - Metadati di profilo dell'unità documentaria

Metadati specifici associati al tipo unità documentaria - Nelle Tabelle Metadati specifici dell'unità documentaria è presentato il set di metadati associato all'unità documentaria nelle diverse versioni. La presenza di versioni diverse è legata alle eventuali modifiche/integrazioni/aggiornamenti nel set di metadati specifici o nelle obbligatorietà concordate con l'Ente.

Versione metadati specifici: 1.0

Descrizione versione:

Data inizio validità: 23/11/2016

Data fine validità:

Denominazione	Descrizione
NumeroIniziale	NumeroIniziale
NumeroFinale	NumeroFinale
DataInizioRegistrazioni	DataInizioRegistrazioni
DataFineRegistrazioni	DataFineRegistrazioni
Originatore	Originatore
Responsabile	Responsabile
Operatore	Operatore
NumeroDocumentiRegistrati	NumeroDocumentiRegistrati
NumeroDocumentiAnnullati	NumeroDocumentiAnnullati
DenominazioneApplicativo	DenominazioneApplicativo
VersioneApplicativo	VersioneApplicativo
ProduttoreApplicativo	ProduttoreApplicativo
DenominazioneSistemaGestioneBaseDati	DenominazioneSistemaGestioneBaseDati
VersioneSistemaGestioneBaseDati	VersioneSistemaGestioneBaseDati
ProduttoreSistemaGestioneBaseDati	ProduttoreSistemaGestioneBaseDati
TempoConservazione	TempoConservazione

Tabella - Metadati specifici dell'unità documentaria

Tipologia di unità documentaria **VARIANTE DI PIANO**

Descrizione della tipologia di unità documentaria: Variante agli Strumenti Urbanistici, ai sensi della L.R. 24/2017

Tipi struttura dell'unità documentaria: nella Tabella Tipi struttura unità documentaria sono rappresentate le varie strutture che può assumere il tipo di unità documentaria, ovvero la sua articolazione in documento principale ed eventuali allegati, annessi e annotazioni, le informazioni relative alla chiave, ai metadati di profilo e altro ancora.

Per ogni Tipo struttura è indicato il periodo di validità, ovvero per quali annualità delle unità documentarie è valido il tipo struttura e i sistemi versanti utilizzati.

Denominazione	Descrizione	Periodi di validità	Sistemi versanti
VARIANTE DI PIANO		2017	PREINGEST

Tabella - Tipi struttura unità documentaria

Nei paragrafi successivi sono riportate le informazioni di dettaglio su ogni singolo Tipo struttura dell'unità documentaria

Tipi struttura **VARIANTE DI PIANO** Nella tabella è riportata l'articolazione dell'unità documentaria in documento principale ed eventuali allegati, annessi e annotazioni.

Tipi documento	Descrizione
ALTRI ATTI RELAZIONI E PARERI	Altri atti relazioni e pareri L.R. 24/2017
DATI GEOGRAFICI	Dati geografici L.R. 24/2017
DELIBERA STRUMENTO URBANISTICO	Delibera strumento urbanistico L.R. 24/2017
ELABORATI CARTOGRAFICI	Elaborati cartografici L.R. 24/2017
OSSERVAZIONI PERVENUTE	Osservazioni pervenute L.R. 24/2017
QUADRO CONOSCITIVO	Quadro conoscitivo L.R. 24/2017
SCHEMA DI ASSETTO DEL TERRITORIO URBANIZZATO	Schema di assetto del territorio urbanizzato L.R. 24/2017
STRATEGIA PER LA QUALITÀ URBANA ED ECOLOGICO-AMBIENTALE	Strategia per la qualità urbana ed ecologico-ambientale L.R. 24/2017
TAVOLA E SCHEDA DEI VINCOLI	Tavola e scheda dei vincoli L.R. 24/2017
VALSAT	Valsat L.R. 24/2017

Tabella - Tipi struttura **VARIANTE DI PIANO**_Descrizione tipi documento

Tipo documento	Elemento	Obbligatorio	Periodicità di versamento	Note
ALTRI ATTI RELAZIONI E PARERI	ALLEGATO	No		
DATI GEOGRAFICI	ALLEGATO	No		
DELIBERA STRUMENTO URBANISTICO	PRINCIPALE	Si		
ELABORATI CARTOGRAFICI	ALLEGATO	No		
OSSERVAZIONI PERVENUTE	ALLEGATO	No		
QUADRO CONOSCITIVO	ALLEGATO	No		
SCHEMA DI ASSETTO DEL TERRITORIO URBANIZZATO	ALLEGATO	No		
STRATEGIA PER LA QUALITÀ URBANA ED ECOLOGICO-AMBIENTALE	ALLEGATO	No		
TAVOLA E SCHEDA DEI VINCOLI	ALLEGATO	No		
VALSAT	ALLEGATO	No		

Tabella - Tipo struttura VARIANTE DI PIANO_Dettaglio tipi documento

Chiave identificativa del tipo struttura dell'unità documentaria (Tipo registro - Anno - Numero)

Registri - Nella Tabella Elenco registri è rappresentata la lista dei registri associati all'unità documentaria. Il nome del registro viene definito dall'Ente o concordato con ParER e in generale corrisponde al nome del repertorio in cui sono registrati in ordine progressivo i documenti ad esso afferenti (ex art. 53, D.P.R. 28/12/2000 n. 445) oppure al contesto applicativo/documentale nell'ambito del quale avviene l'assegnazione dell'identificativo progressivo e univoco. Il parametro "Fiscale" indica che le unità documentarie associate al Registro sono soggette alla conservazione di tipo fiscale, finalizzata alla conservazione a norma dei documenti rilevanti ai fini tributari in conformità con quanto previsto dalla normativa di settore vigente (DM del 17 giugno 2014 del Ministero dell'economia e delle finanze)

Tipo registro	Descrizione	Periodi di validità	Descrizione formato numero	Fiscale	Data disattivazione
STRUMENTI URBANISTICI	Registro per gli Strumenti Urbanistici	2017	Il numero è composto da una sigla che identifica il tipo di atto con cui è stato approvato lo strumento e dal numero di registrazione assegnato. Le sigle utilizzate sono DCC (Delibera Consiglio Comunale), DCU (Delibera Consiglio Unione), DGC (Delibera Giunta Comunale), DGU (Delibera Giunta Unione), PROT (Documento Protocollato). Il numero corrisponde al numero di registrazione nel repertorio delle delibere oppure al numero di protocollo.	No	

Tabella - Elenco registri

Anno - Anno solare di riferimento del repertorio

Numero - Numero della delibera con la quale è stato approvato l'atto, composto da una sigla che individua la tipologia dell'organo deliberante (DCC: Delibera Consiglio Comunale, DCU: Delibera Consiglio Unione, DGC: Delibera Giunta Comunale, DGU: Delibera Giunta Unione) e dal numero di repertorio, es. DCC_nnn

Riferimento temporale -

Metadati di profilo del tipo unità documentaria - Nella Tabella Metadati di profilo dell'unità documentaria sono descritti i metadati "Data" e "Oggetto" associati all'unità documentaria

Denominazione	Descrizione
Data	Data della Deliberazione che coincide con la data di seduta dell'Organo collegiale deliberante
Oggetto	Oggetto dello Strumento Urbanistico generato dal sistema, composto da nome dell'ente convenzionato, tipologia unità documentaria, anno, numero e data.

Tabella - Metadati di profilo dell'unità documentaria

Metadati specifici associati al tipo unità documentaria - Nelle Tabelle Metadati specifici dell'unità documentaria è presentato il set di metadati associato all'unità documentaria nelle diverse versioni. La presenza di versioni diverse è legata alle eventuali modifiche/integrazioni/aggiornamenti nel set di metadati specifici o nelle obbligatorioità concordate con l'Ente.

Versione metadati specifici: 1.0

Descrizione versione:

Data inizio validità: 10/10/2019

Data fine validità:

Denominazione	Descrizione
tipo_ente	tipo_ente
ente_convenzionato	ente_convenzionato
unione_comuni	unione_comuni
provincia_ente	provincia_ente
fase_elaborazione_strumento	fase_elaborazione_strumento

Tabella - Metadati specifici dell'unità documentaria

Parametri di Struttura per le verifiche al versamento

Nella fase di acquisizione del pacchetto di versamento (SIP) il Sistema effettua una serie di verifiche automatiche finalizzate ad individuare eventuali anomalie. In questo capitolo è descritta l'impostazione dell'intera Struttura in relazione ai controlli operati dal Sistema. Si precisa che l'impostazione della struttura interessa tutte le tipologie documentarie configurate. Il sistema consente inoltre di impostare specifici controlli a livello di singola tipologia documentaria. Le eventuali impostazioni definite per la tipologia documentaria sono dettagliate nel capitolo "Parametri sul tipo unità documentaria per le verifiche al versamento".

Per ciascun parametro sono fornite le seguenti informazioni:

- sintetica descrizione;
- indicazione dello stato di attivazione previsto dalla configurazione "standard" definita da ParER;
- indicazione dello stato di attivazione effettivo.

Si precisa che l'eventuale difformità tra lo stato di attivazione definito da ParER e lo stato effettivo dipende da un'esplicita richiesta di modifica del parametro "standard" da parte dell'Ente. Le verifiche automatiche a cui sono sottoposti i SIP nonché i parametri di accettazione sono infatti regolabili a discrezione dell'Ente.

L'esito del versamento è condizionato dai parametri impostati a livello di Struttura dettagliati nelle tabelle sottostanti e dai parametri definiti dall'Ente a livello di Indice SIP (file XML che contiene i metadati nonché i riferimenti ai file dei Componenti del SIP dell'unità documentaria).

I parametri definiti nell'Indice SIP sono tre:

- Forza Accettazione: definisce il comportamento del Sistema in relazione agli esiti delle verifiche di firma e/o formato dei file contenuti nel SIP. Assume valori "False" o "True":
 - False: il Sistema accetta il versamento solo se tutti i controlli relativi alla firma e al formato hanno esito positivo
 - True: il Sistema accetta il versamento anche nel caso in cui almeno uno dei controlli relativi alla firma e al formato hanno esito negativo
- Forza Conservazione: definisce il comportamento del Sistema in relazione al versamento di SIP contenenti file non firmati. Assume valori "False" o "True":
 - False: il Sistema accetta il versamento solo se è presente almeno un file firmato
 - True: il Sistema accetta il versamento anche nel caso in cui nessuno dei file sia firmato
- Forza Collegamento: definisce il comportamento del Sistema in funzione della presenza o meno nel Sistema stesso del SIP oggetto di collegamento. Assume valori "False" o "True":
 - False: il Sistema accetta il versamento di SIP i cui eventuali Collegamenti siano rivolti a SIP già presenti nel Sistema
 - True: il Sistema accetta il versamento di SIP anche nel caso in cui gli eventuali Collegamenti siano rivolti a SIP non presenti nel Sistema.

L'impostazione "standard" riguarda unicamente i parametri configurati a livello di Struttura e prevede l'attivazione di tutti i controlli sul formato del file e sulla validità della firma e di tutti i relativi parametri di accettazione dei SIP per i quali il Sistema abbia restituito un esito negativo del controllo.

Si precisa che i controlli sulle eventuali firme digitali è effettuata alla data indicata nell'Indice SIP (che può essere quella contenuta nella firma, in una marca temporale o un riferimento temporale dichiarato nell'Indice SIP) o, in assenza di questa, alla data del versamento.

Secondo l'impostazione "standard", il SIP con esito negativo del controllo sulla validità della firma viene accettato in conservazione solo se la trasmissione dello stesso viene "forzata" dal versatore in sede di versamento. La forzatura consiste nel valorizzare con "True" il parametro "Forza Accettazione" presente nell'Indice SIP.

A titolo di esempio si riporta l'esito del versamento di un SIP con certificato di firma scaduto in relazione all'impostazione del parametro "Forza Accettazione" e all'impostazione "standard" dei parametri di Struttura:

CASO A - Parametro "Forza Accettazione" attivo

- Controllo certificato: SI (configurazione standard)

- Accetta controllo certificato scaduto: SI (configurazione standard)
- Forza Accettazione: SI (definito nell'IndiceSIP)

In questo caso il SIP viene acquisito in conservazione e l'esito del versamento è di tipo WARNING.

CASO B - Parametro "Forza Accettazione" NON attivo

- Controllo certificato: SI (configurazione standard)
- Accetta controllo certificato scaduto: SI (configurazione standard)
- Forza Accettazione: NO (definito nell'IndiceSIP)

In questo caso il SIP viene rifiutato e l'esito del versamento è NEGATIVO.

Il registro viene definito dall'Ente o concordato con ParER e in generale corrisponde al nome del repertorio in cui sono registrati in ordine progressivo i documenti ad esso afferenti (ex art. 53, D.P.R. 28/12/2000 n. 445) oppure al contesto applicativo/documentale nell'ambito del quale viene attribuito all'unità documentaria l'identificativo progressivo e univoco.

In relazione a ciascun registro associato alle tipologie documentarie oggetto di versamento (vedere Tabella Elenco registri), è definito il formato del metadato "Numero" della chiave del SIP dell'unità documentaria afferente al registro medesimo. Il metadato "Numero" può assumere caratteri diversi ad esempio numerici, alfabetici, alfanumerici, caratteri speciali o numeri romani.

Il Sistema verifica che il valore inserito nel metadato "Numero" risponda al formato definito.

In assenza di indicazioni concordate con l'Ente, il numero della chiave viene accettato come se fosse una stringa (calcolo di ordinamento del numero di tipo "GENERICO").

Funzione	Parametro	Descrizione	Valore standard	Valore effettivo (Richiesto dall'Ente)
Abilitazione fascicoli	FL_GEST_FASCICOLI	Abilita la gestione dei fascicoli nella Struttura (false, true)	NO	NO
Accettazione formati file	FL_ABILITA_CONTR_FMT	Abilita il controllo del formato file versato (false, true)	SI	SI
Accettazione formati file	FL_ACCETTA_CONTR_FMT_NEG	Consente di superare un esito controllo formato file negativo con il Forza formato (false, true)	SI	SI
Accettazione formati file	FL_FORZA_FMT	Forza l'accettazione del controllo formato file negativo (false, true)	SI	SI
Accettazione formati numero unità doc	FL_ABILITA_CONTR_FMT_NUM	Abilita il controllo del formato del numero dell'unità doc (false, true)	SI	SI
Accettazione formati	FL_ACCETTA_FMT_NUM_NEG	Consente di superare un esito controllo formato del numero dell'unità doc negativo con il Forza formato (false, true)	NO	NO

Funzione	Parametro	Descrizione	Valore standard	Valore effettivo (Richiesto dall'Ente)
numero unità doc				
Accettazione formati numero unità doc	FL_FORZA_FMT_NUM	Forza l'accettazione del controllo formato del numero dell'unità doc negativo (false, true)	NO	NO
Accettazione hash versato	FL_ABILITA_CONTR_HASH_VERS	Abilita il controllo del hash versato (false, true)	NO	NO
Accettazione hash versato	FL_ACCETTA_CONTR_HASH_NEG	Consente di superare un esito controllo hash versato negativo con il Forza hash versato (false, true)	SI	NO
Accettazione hash versato	FL_FORZA_HASH_VERS	Forza l'accettazione del controllo hash versato negativo (false, true)	SI	NO
Aggiornamento metadati	FL_ABILITA_UPD_META	Indica se e' abilitato il servizio di aggiornamento metadati unita' doc (false, true)	NO	NO
Aggiornamento metadati	FL_ACCETTA_UPD_META_INARK	Indica si accetta l'aggiornamento metadati per unita' doc in archivio con il Forza aggiornamento (false, true)	NO	NO
Aggiornamento metadati	FL_FORZA_UPD_META_INARK	Indica se si forza l'aggiornamento metadati per unita' doc in archivio (false, true)	NO	NO
Aggiunta documento	FL_ABILITA_FORZA_DOC_AGG	Abilita Forza aggiunta documento(false, true)	SI	SI
Aggiunta documento	FL_ACCETTA_DOC_AGG_NEG	Consente di superare un esito di controllo negativo per documento aggiunto(false, true)	NO	NO
Aggiunta documento	FL_FORZA_DOC_AGG	Forza l'accettazione del controllo per documento aggiunto negativo (false, true)	NO	NO
Controlli file non firmati	FL_ABILITA_CONTR_NON_FIRMATI	Consente di abilitare/disabilitare la conservazione del documento (false, true)	SI	SI
Controlli file non firmati	FL_ACCETTA_CONTR_NON_FIRMATI_NEG	Consente di superare un esito documento non firmato digitalmente con il Forza accettazione (false, true)	NO	NO

Funzione	Parametro	Descrizione	Valore standard	Valore effettivo (Richiesto dall'Ente)
Controlli file non firmati	FL_FORZA_CONTR_NON_FIRMATI_NEG	Definisce il valore che assume il parametro Forza conservazione se non presente nell'Indice SIP (false, true)	NO	NO
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NEG	Consente di superare un esito di controllo CRL negativo con il Forza accettazione (false, true)	SI	SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NOSCAR	Consente di superare un esito di controllo CRL non scaricabile con il Forza accettazione (false, true)	SI	SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NOVAL	Consente di superare un esito di controllo CRL non valida con il Forza accettazione (false, true)	SI	SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_SCAD	Consente di superare un esito di controllo CRL scaduta con il Forza accettazione (false, true)	SI	SI
Controlli firma CRL	FL_FORZA_CONTR_CRL_VERS	Definisce il valore di default che assume l'eventuale parametro di forzatura se non presente nell'Indice SIP (false, true)	NO	NO
Controlli firma certificato	FL_ABILITA_CONTR_CERTIF_VERS	Abilita il controllo sulla validità del certificato di firma (false, true)	SI	SI
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_NOCERT	Consente di superare un esito di controllo certificato che non e' un certificato con il Forza accettazione (false, true)	SI	SI
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_NOVAL	Consente di superare un esito di controllo certificato non valido con il Forza accettazione (false, true)	SI	SI
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_SCAD	Consente di superare un esito di controllo certificato scaduto con il Forza accettazione (false, true)	SI	SI
Controlli firma certificato	FL_FORZA_CONTR_CERTIF_VERS	Definisce il valore di default che assume l'eventuale parametro di forzatura se non presente nell'Indice SIP (false, true)	NO	NO

Funzione	Parametro	Descrizione	Valore standard	Valore effettivo (Richiesto dall'Ente)
Controlli firma crittografico	FL_ABILITA_CONTR_CRITTOG_VERS	Abilita il controllo crittografico (false, true)	SI	SI
Controlli firma crittografico	FL_ACCETTA_CONTR_CRITTOG_NEG	Consente di superare un esito di controllo crittografico negativo con il Forza accettazione (false, true)	SI	SI
Controlli firma crittografico	FL_FORZA_CONTR_CRITTOG_VERS	Definisce il valore di default che assume l'eventuale parametro di forzatura se non presente nell'Indice SIP (false, true)	NO	NO
Controlli firma non conforme	FL_ABILITA_VERIFICA_FIRMA	Consente di abilitare/disabilitare i servizi di verifica firma, prima EIDAS, eventualmente CRYPTO (false, true). Nota : se FL_ABILITA_VERIFICA_FIRMA_SOLO_CRYPTO e FL_ABILITA_VERIFICA_FIRMA entrambi false non si effettua la verifica firma	SI	SI
Controlli firma non conforme	FL_ACCETTA_FIRMA_GIUGNO_2011	Consente di superare un esito di controllo negativo per firma no delibera 45 con il Forza accettazione (false, true)	SI	SI
Controlli firma non conforme	FL_ACCETTA_FIRMA_NOCONF	Consente di superare un esito di controllo negativo per firma non conforme con il Forza accettazione (false, true)	SI	SI
Controlli firma non conforme	FL_ACCETTA_FIRMA_NOCONOS	Consente di superare un esito di controllo negativo per firma sconosciuta con il Forza accettazione (false, true)	SI	SI
Controlli firma non conforme	FL_ACCETTA_MARCA_NOCONOS	Consente di superare un esito di controllo negativo per marca sconosciuta con il Forza accettazione (false, true)	SI	SI
Controlli firma non conforme	FL_FORZA_CONTR_NOCONF	Definisce il valore di default che assume l'eventuale parametro di forzatura se non presente nell'Indice SIP (false, true)	NO	NO

Funzione	Parametro	Descrizione	Valore standard	Valore effettivo (Richiesto dall'Ente)
Controlli firma trusted	FL_ABILITA_CONTR_TRUST_VERS	Abilita il controllo di catena trusted (false, true)	SI	SI
Controlli firma trusted	FL_ACCETTA_CONTR_TRUST_NEG	Consente di superare un esito di controllo catena trusted negativo con il Forza accettazione (false, true)	SI	SI
Controlli firma trusted	FL_FORZA_CONTR_TRUST_VERS	Definisce il valore di default che assume l'eventuale parametro di forzatura se non presente nell'Indice SIP (false, true)	NO	NO
Controllo classificazione	FL_ABILITA_CONTR_CLASSIF	Abilita il controllo della classificazione dei fascicoli (false, true)	NO	NO
Controllo classificazione	FL_ACCETTA_CONTR_CLASSIF_NEG	Consente di superare un esito del controllo della classificazione negativo con il Forza controllo classificazione (false, true)	NO	NO
Controllo classificazione	FL_FORZA_CONTR_CLASSIF	Forza l'accettazione del controllo classificazione negativo (false, true)	NO	NO
Controllo collegamenti fascicoli	FL_ABILITA_CONTR_COLLEG	Abilita il controllo dei collegamenti fra fascicoli (false, true)	NO	NO
Controllo collegamenti fascicoli	FL_ACCETTA_CONTR_COLLEG_NEG_FAS	Consente di superare un esito del controllo collegamenti fra fascicoli negativo con il Forza controllo collegamenti (false, true)	SI	SI
Controllo collegamenti fascicoli	FL_FORZA_CONTR_COLLEG	Forza l'accettazione del controllo collegamenti fra fascicoli negativo (false, true)	NO	NO
Controllo collegamenti fra unità doc	FL_ABILITA_CONTR_COLLEG_UD	Abilita il controllo dei collegamenti fra unità documentarie (false, true)	SI	SI
Controllo collegamenti fra unità doc	FL_ACCETTA_CONTR_COLLEG_NEG	Consente di superare un esito controllo collegamenti negativo con il Forza collegamenti (false, true)	NO	NO

Funzione	Parametro	Descrizione	Valore standard	Valore effettivo (Richiesto dall'Ente)
Controllo collegamenti fra unità doc	FL_FORZA_COLLEG	Forza l'accettazione del controllo collegamenti negativo (false, true)	NO	NO
Controllo formato numero fascicoli	FL_ABILITA_CONTR_NUMERO	Abilita il controllo del numero dei fascicoli (false, true)	NO	NO
Controllo formato numero fascicoli	FL_ACCETTA_CONTR_NUMERO_NEG	Consente di superare un esito del controllo numero fascicolo negativo con il Forza controllo numero (false, true)	NO	NO
Controllo formato numero fascicoli	FL_FORZA_CONTR_NUMERO	Forza l'accettazione del controllo numero fascicolo negativo (false, true)	NO	NO
Obbligatorietà dati di profilo unità doc	FL_OBBL_DATA	Indica se la data e' obbligatoria al versamento (false, true)	SI	NO
Obbligatorietà dati di profilo unità doc	FL_OBBL_OGGETTO	Indica se l'oggetto e' obbligatorio al versamento (false, true)	SI	NO

Parametri sul tipo unità documentaria per le verifiche al versamento

In questo paragrafo sono indicati (se presenti) i valori dei parametri utilizzati per le verifiche al versamento definiti in modo specifico per la tipologia di unità documentaria.

Tipologia di unità documentaria ACCORDO DI PROGRAMMA

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Accettazione formati file	FL_ABILITA_CONTR_FMT	Abilita il controllo del formato file versato (false, true)	SI		SI
Accettazione formati file	FL_ACCETTA_CONTR_FMT_NEG	Consente di superare un esito controllo formato file negativo con il Forza formato (false, true)	SI		SI
Accettazione formati file	FL_FORZA_FMT	Forza l'accettazione del controllo formato file negativo (false, true)	SI		SI
Accettazione formati numero unità doc	FL_ABILITA_CONTR_FMT_NUM	Abilita il controllo del formato del numero dell'unità doc (false, true)	SI	SI	SI
Accettazione formati numero unità doc	FL_ACCETTA_FMT_NUM_NEG	Consente di superare un esito controllo formato del numero dell'unità doc negativo con il Forza formato (false, true)	NO	NO	SI
Accettazione formati numero unità doc	FL_FORZA_FMT_NUM	Forza l'accettazione del controllo formato del numero dell'unità doc negativo (false, true)	NO	NO	SI
Accettazione hash versato	FL_ABILITA_CONTR_HASH_VERS	Abilita il controllo del hash versato (false, true)	NO	NO	SI
Accettazione hash versato	FL_ACCETTA_CONTR_HASH_NEG	Consente di superare un esito controllo hash versato negativo con il Forza hash versato (false, true)	SI	NO	SI
Accettazione hash versato	FL_FORZA_HASH_VERS	Forza l'accettazione del controllo hash versato negativo (false, true)	SI	NO	SI

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Aggiornamento metadati	FL_ABILITA_UPD_META	Indica se e' abilitato il servizio di aggiornamento metadati unita' doc (false, true)	NO	NO	SI
Aggiornamento metadati	FL_ACCETTA_UPD_META_INARK	Indica si accetta l'aggiornamento metadati per unita' doc in archivio con il Forza aggiornamento (false, true)	NO	NO	SI
Aggiornamento metadati	FL_FORZA_UPD_META_INARK	Indica se si forza l'aggiornamento metadati per unita' doc in archivio (false, true)	NO	NO	SI
Aggiunta documento	FL_ABILITA_FORZA_DOC_AGG	Abilita Forza aggiunta documento(false, true)	SI		SI
Aggiunta documento	FL_ACCETTA_DOC_AGG_NEG	Consente di superare un esito di controllo negativo per documento aggiunto(false, true)	NO		SI
Aggiunta documento	FL_FORZA_DOC_AGG	Forza l'accettazione del controllo per documento aggiunto negativo (false, true)	NO		SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NEG	Consente di superare un esito di controllo CRL negativo con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NOSCAR	Consente di superare un esito di controllo CRL non scaricabile con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NOVAL	Consente di superare un esito di controllo CRL non valida con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_SCAD	Consente di superare un esito di controllo CRL scaduta con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_NOCERT	Consente di superare un esito di controllo certificato che non e' un certificato con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_NOVAL	Consente di superare un esito di controllo certificato non valido con il Forza accettazione (false, true)	SI	SI	SI

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_SCAD	Consente di superare un esito di controllo certificato scaduto con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma crittografico	FL_ABILITA_CONTR_CRITTOG_VERS	Abilita il controllo crittografico (false, true)	SI	SI	SI
Controlli firma crittografico	FL_ACCETTA_CONTR_CRITTOG_NEG	Consente di superare un esito di controllo crittografico negativo con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_FIRMA_GIUGNO_2011	Consente di superare un esito di controllo negativo per firma no delibera 45 con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_FIRMA_NOCONF	Consente di superare un esito di controllo negativo per firma non conforme con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_FIRMA_NOCONOS	Consente di superare un esito di controllo negativo per firma sconosciuta con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_MARCA_NOCONOS	Consente di superare un esito di controllo negativo per marca sconosciuta con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma trusted	FL_ABILITA_CONTR_TRUST_VERS	Abilita il controllo di catena trusted (false, true)	SI	SI	SI
Controlli firma trusted	FL_ACCETTA_CONTR_TRUST_NEG	Consente di superare un esito di controllo catena trusted negativo con il Forza accettazione (false, true)	SI	SI	SI
Controllo collegamenti fra unità doc	FL_ABILITA_CONTR_COLLEG_UD	Abilita il controllo dei collegamenti fra unità documentarie (false, true)	SI		SI

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Controllo collegamenti fra unità doc	FL_ACCETTA_CONTR_COLLEG_NEG	Consente di superare un esito controllo collegamenti negativo con il Forza collegamenti (false, true)	NO		SI
Controllo collegamenti fra unità doc	FL_FORZA_COLLEG	Forza l'accettazione del controllo collegamenti negativo (false, true)	NO		SI

Tipologia di unità documentaria ACCORDO OPERATIVO

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Accettazione formati file	FL_ABILITA_CONTR_FMT	Abilita il controllo del formato file versato (false, true)	SI		SI
Accettazione formati file	FL_ACCETTA_CONTR_FMT_NEG	Consente di superare un esito controllo formato file negativo con il Forza formato (false, true)	SI		SI
Accettazione formati file	FL_FORZA_FMT	Forza l'accettazione del controllo formato file negativo (false, true)	SI		SI
Accettazione formati numero unità doc	FL_ABILITA_CONTR_FMT_NUM	Abilita il controllo del formato del numero dell'unità doc (false, true)	SI	SI	SI
Accettazione formati numero unità doc	FL_ACCETTA_FMT_NUM_NEG	Consente di superare un esito controllo formato del numero dell'unità doc negativo con il Forza formato (false, true)	NO	NO	SI
Accettazione formati numero unità doc	FL_FORZA_FMT_NUM	Forza l'accettazione del controllo formato del numero dell'unità doc negativo (false, true)	NO	NO	SI

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Accettazione hash versato	FL_ABILITA_CONTR_HASH_VERS	Abilita il controllo del hash versato (false, true)	NO	NO	SI
Accettazione hash versato	FL_ACCETTA_CONTR_HASH_NEG	Consente di superare un esito controllo hash versato negativo con il Forza hash versato (false, true)	SI	NO	SI
Accettazione hash versato	FL_FORZA_HASH_VERS	Forza l'accettazione del controllo hash versato negativo (false, true)	SI	NO	SI
Aggiornamento metadati	FL_ABILITA_UPD_META	Indica se e' abilitato il servizio di aggiornamento metadati unita' doc (false, true)	NO	NO	SI
Aggiornamento metadati	FL_ACCETTA_UPD_META_INARK	Indica si accetta l'aggiornamento metadati per unita' doc in archivio con il Forza aggiornamento (false, true)	NO	NO	SI
Aggiornamento metadati	FL_FORZA_UPD_META_INARK	Indica se si forza l'aggiornamento metadati per unita' doc in archivio (false, true)	NO	NO	SI
Aggiunta documento	FL_ABILITA_FORZA_DOC_AGG	Abilita Forza aggiunta documento(false, true)	SI		SI
Aggiunta documento	FL_ACCETTA_DOC_AGG_NEG	Consente di superare un esito di controllo negativo per documento aggiunto(false, true)	NO		SI
Aggiunta documento	FL_FORZA_DOC_AGG	Forza l'accettazione del controllo per documento aggiunto negativo (false, true)	NO		SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NEG	Consente di superare un esito di controllo CRL negativo con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NOSCAR	Consente di superare un esito di controllo CRL non scaricabile con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NOVAL	Consente di superare un esito di controllo CRL non valida con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_SCAD	Consente di superare un esito di controllo CRL scaduta con il Forza accettazione (false, true)	SI	SI	SI

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_NOCERT	Consente di superare un esito di controllo certificato che non e' un certificato con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_NOVAL	Consente di superare un esito di controllo certificato non valido con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_SCAD	Consente di superare un esito di controllo certificato scaduto con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma crittografico	FL_ABILITA_CONTR_CRITTOG_VERS	Abilita il controllo crittografico (false, true)	SI	SI	SI
Controlli firma crittografico	FL_ACCETTA_CONTR_CRITTOG_NEG	Consente di superare un esito di controllo crittografico negativo con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_FIRMA_GIUGNO_2011	Consente di superare un esito di controllo negativo per firma no delibera 45 con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_FIRMA_NOCONF	Consente di superare un esito di controllo negativo per firma non conforme con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_FIRMA_NOCONOS	Consente di superare un esito di controllo negativo per firma sconosciuta con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_MARCA_NOCONOS	Consente di superare un esito di controllo negativo per marca sconosciuta con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma trusted	FL_ABILITA_CONTR_TRUST_VERS	Abilita il controllo di catena trusted (false, true)	SI	SI	SI

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Controlli firma trusted	FL_ACCETTA_CONTR_TRUST_NEG	Consente di superare un esito di controllo catena trusted negativo con il Forza accettazione (false, true)	SI	SI	SI
Controllo collegamenti fra unità doc	FL_ABILITA_CONTR_COLLEG_UD	Abilita il controllo dei collegamenti fra unità documentarie (false, true)	SI		SI
Controllo collegamenti fra unità doc	FL_ACCETTA_CONTR_COLLEG_NEG	Consente di superare un esito controllo collegamenti negativo con il Forza collegamenti (false, true)	NO		SI
Controllo collegamenti fra unità doc	FL_FORZA_COLLEG	Forza l'accettazione del controllo collegamenti negativo (false, true)	NO		SI

Tipologia di unità documentaria PIANO ARENILE

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Accettazione formati file	FL_ABILITA_CONTR_FMT	Abilita il controllo del formato file versato (false, true)	SI		SI
Accettazione formati file	FL_ACCETTA_CONTR_FMT_NEG	Consente di superare un esito controllo formato file negativo con il Forza formato (false, true)	SI		SI
Accettazione formati file	FL_FORZA_FMT	Forza l'accettazione del controllo formato file negativo (false, true)	SI		SI
Accettazione formati numero unità doc	FL_ABILITA_CONTR_FMT_NUM	Abilita il controllo del formato del numero dell'unità doc (false, true)	SI	SI	SI

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Accettazione formati numero unità doc	FL_ACCETTA_FMT_NUM_NEG	Consente di superare un esito controllo formato del numero dell'unità doc negativo con il Forza formato (false, true)	NO	NO	SI
Accettazione formati numero unità doc	FL_FORZA_FMT_NUM	Forza l'accettazione del controllo formato del numero dell'unità doc negativo (false, true)	NO	NO	SI
Accettazione hash versato	FL_ABILITA_CONTR_HASH_VERS	Abilita il controllo del hash versato (false, true)	NO	NO	SI
Accettazione hash versato	FL_ACCETTA_CONTR_HASH_NEG	Consente di superare un esito controllo hash versato negativo con il Forza hash versato (false, true)	SI	NO	SI
Accettazione hash versato	FL_FORZA_HASH_VERS	Forza l'accettazione del controllo hash versato negativo (false, true)	SI	NO	SI
Aggiornamento metadati	FL_ABILITA_UPD_META	Indica se e' abilitato il servizio di aggiornamento metadati unita' doc (false, true)	NO	NO	SI
Aggiornamento metadati	FL_ACCETTA_UPD_META_INARK	Indica si accetta l'aggiornamento metadati per unita' doc in archivio con il Forza aggiornamento (false, true)	NO	NO	SI
Aggiornamento metadati	FL_FORZA_UPD_META_INARK	Indica se si forza l'aggiornamento metadati per unita' doc in archivio (false, true)	NO	NO	SI
Aggiunta documento	FL_ABILITA_FORZA_DOC_AGG	Abilita Forza aggiunta documento(false, true)	SI		SI
Aggiunta documento	FL_ACCETTA_DOC_AGG_NEG	Consente di superare un esito di controllo negativo per documento aggiunto(false, true)	NO		SI
Aggiunta documento	FL_FORZA_DOC_AGG	Forza l'accettazione del controllo per documento aggiunto negativo (false, true)	NO		SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NEG	Consente di superare un esito di controllo CRL negativo con il Forza accettazione (false, true)	SI	SI	SI

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NOSCAR	Consente di superare un esito di controllo CRL non scaricabile con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NOVAL	Consente di superare un esito di controllo CRL non valida con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_SCAD	Consente di superare un esito di controllo CRL scaduta con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_NOCERT	Consente di superare un esito di controllo certificato che non e' un certificato con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_NOVAL	Consente di superare un esito di controllo certificato non valido con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_SCAD	Consente di superare un esito di controllo certificato scaduto con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma crittografico	FL_ABILITA_CONTR_CRITTOG_VERS	Abilita il controllo crittografico (false, true)	SI	SI	SI
Controlli firma crittografico	FL_ACCETTA_CONTR_CRITTOG_NEG	Consente di superare un esito di controllo crittografico negativo con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_FIRMA_GIUGNO_2011	Consente di superare un esito di controllo negativo per firma no delibera 45 con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_FIRMA_NOCONF	Consente di superare un esito di controllo negativo per firma non conforme con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_FIRMA_NOCONOS	Consente di superare un esito di controllo negativo per firma sconosciuta con il Forza accettazione (false, true)	SI	SI	SI

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Controlli firma non conforme	FL_ACCETTA_MARCA_NOCONOS	Consente di superare un esito di controllo negativo per marca sconosciuta con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma trusted	FL_ABILITA_CONTR_TRUST_VERS	Abilita il controllo di catena trusted (false, true)	SI	SI	SI
Controlli firma trusted	FL_ACCETTA_CONTR_TRUST_NEG	Consente di superare un esito di controllo catena trusted negativo con il Forza accettazione (false, true)	SI	SI	SI
Controllo collegamenti fra unità doc	FL_ABILITA_CONTR_COLLEG_UD	Abilita il controllo dei collegamenti fra unità documentarie (false, true)	SI		SI
Controllo collegamenti fra unità doc	FL_ACCETTA_CONTR_COLLEG_NEG	Consente di superare un esito controllo collegamenti negativo con il Forza collegamenti (false, true)	NO		SI
Controllo collegamenti fra unità doc	FL_FORZA_COLLEG	Forza l'accettazione del controllo collegamenti negativo (false, true)	NO		SI

Tipologia di unità documentaria PIANO ATTUATIVO DI INIZIATIVA PUBBLICA

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Accettazione formati file	FL_ABILITA_CONTR_FMT	Abilita il controllo del formato file versato (false, true)	SI		SI
Accettazione formati file	FL_ACCETTA_CONTR_FMT_NEG	Consente di superare un esito controllo formato file negativo con il Forza formato (false, true)	SI		SI
Accettazione formati file	FL_FORZA_FMT	Forza l'accettazione del controllo formato file negativo (false, true)	SI		SI

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Accettazione formati numero unità doc	FL_ABILITA_CONTR_FMT_NUM	Abilita il controllo del formato del numero dell'unità doc (false, true)	SI	SI	SI
Accettazione formati numero unità doc	FL_ACCETTA_FMT_NUM_NEG	Consente di superare un esito controllo formato del numero dell'unità doc negativo con il Forza formato (false, true)	NO	NO	SI
Accettazione formati numero unità doc	FL_FORZA_FMT_NUM	Forza l'accettazione del controllo formato del numero dell'unità doc negativo (false, true)	NO	NO	SI
Accettazione hash versato	FL_ABILITA_CONTR_HASH_VERS	Abilita il controllo del hash versato (false, true)	NO	NO	SI
Accettazione hash versato	FL_ACCETTA_CONTR_HASH_NEG	Consente di superare un esito controllo hash versato negativo con il Forza hash versato (false, true)	SI	NO	SI
Accettazione hash versato	FL_FORZA_HASH_VERS	Forza l'accettazione del controllo hash versato negativo (false, true)	SI	NO	SI
Aggiornamento metadati	FL_ABILITA_UPD_META	Indica se e' abilitato il servizio di aggiornamento metadati unita' doc (false, true)	NO	NO	SI
Aggiornamento metadati	FL_ACCETTA_UPD_META_INARK	Indica si accetta l'aggiornamento metadati per unita' doc in archivio con il Forza aggiornamento (false, true)	NO	NO	SI
Aggiornamento metadati	FL_FORZA_UPD_META_INARK	Indica se si forza l'aggiornamento metadati per unita' doc in archivio (false, true)	NO	NO	SI
Aggiunta documento	FL_ABILITA_FORZA_DOC_AGG	Abilita Forza aggiunta documento(false, true)	SI		SI
Aggiunta documento	FL_ACCETTA_DOC_AGG_NEG	Consente di superare un esito di controllo negativo per documento aggiunto(false, true)	NO		SI

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Aggiunta documento	FL_FORZA_DOC_AGG	Forza l'accettazione del controllo per documento aggiunto negativo (false, true)	NO		SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NEG	Consente di superare un esito di controllo CRL negativo con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NOSCAR	Consente di superare un esito di controllo CRL non scaricabile con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NOVAL	Consente di superare un esito di controllo CRL non valida con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_SCAD	Consente di superare un esito di controllo CRL scaduta con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_NOCERT	Consente di superare un esito di controllo certificato che non e' un certificato con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_NOVAL	Consente di superare un esito di controllo certificato non valido con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_SCAD	Consente di superare un esito di controllo certificato scaduto con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma crittografico	FL_ABILITA_CONTR_CRITTOG_VERS	Abilita il controllo crittografico (false, true)	SI	SI	SI
Controlli firma crittografico	FL_ACCETTA_CONTR_CRITTOG_NEG	Consente di superare un esito di controllo crittografico negativo con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_FIRMA_GIUGNO_2011	Consente di superare un esito di controllo negativo per firma no delibera 45 con il Forza accettazione (false, true)	SI	SI	SI

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Controlli firma non conforme	FL_ACCETTA_FIRMA_NOCONF	Consente di superare un esito di controllo negativo per firma non conforme con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_FIRMA_NOCONOS	Consente di superare un esito di controllo negativo per firma sconosciuta con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_MARCA_NOCONOS	Consente di superare un esito di controllo negativo per marca sconosciuta con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma trusted	FL_ABILITA_CONTR_TRUST_VERS	Abilita il controllo di catena trusted (false, true)	SI	SI	SI
Controlli firma trusted	FL_ACCETTA_CONTR_TRUST_NEG	Consente di superare un esito di controllo catena trusted negativo con il Forza accettazione (false, true)	SI	SI	SI
Controllo collegamenti fra unità doc	FL_ABILITA_CONTR_COLLEG_UD	Abilita il controllo dei collegamenti fra unità documentarie (false, true)	SI		SI
Controllo collegamenti fra unità doc	FL_ACCETTA_CONTR_COLLEG_NEG	Consente di superare un esito controllo collegamenti negativo con il Forza collegamenti (false, true)	NO		SI
Controllo collegamenti fra unità doc	FL_FORZA_COLLEG	Forza l'accettazione del controllo collegamenti negativo (false, true)	NO		SI

Tipologia di unità documentaria PIANO SETTORIALE

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Accettazione formati file	FL_ABILITA_CONTR_FMT	Abilita il controllo del formato file versato (false, true)	SI		SI
Accettazione formati file	FL_ACCETTA_CONTR_FMT_NEG	Consente di superare un esito controllo formato file negativo con il Forza formato (false, true)	SI		SI
Accettazione formati file	FL_FORZA_FMT	Forza l'accettazione del controllo formato file negativo (false, true)	SI		SI
Accettazione formati numero unità doc	FL_ABILITA_CONTR_FMT_NUM	Abilita il controllo del formato del numero dell'unità doc (false, true)	SI	SI	SI
Accettazione formati numero unità doc	FL_ACCETTA_FMT_NUM_NEG	Consente di superare un esito controllo formato del numero dell'unità doc negativo con il Forza formato (false, true)	NO	NO	SI
Accettazione formati numero unità doc	FL_FORZA_FMT_NUM	Forza l'accettazione del controllo formato del numero dell'unità doc negativo (false, true)	NO	NO	SI
Accettazione hash versato	FL_ABILITA_CONTR_HASH_VERS	Abilita il controllo del hash versato (false, true)	NO	NO	SI
Accettazione hash versato	FL_ACCETTA_CONTR_HASH_NEG	Consente di superare un esito controllo hash versato negativo con il Forza hash versato (false, true)	SI	NO	SI
Accettazione hash versato	FL_FORZA_HASH_VERS	Forza l'accettazione del controllo hash versato negativo (false, true)	SI	NO	SI
Aggiornamento metadati	FL_ABILITA_UPD_META	Indica se e' abilitato il servizio di aggiornamento metadati unita' doc (false, true)	NO	NO	SI
Aggiornamento metadati	FL_ACCETTA_UPD_META_INARK	Indica si accetta l'aggiornamento metadati per unita' doc in archivio con il Forza aggiornamento (false, true)	NO	NO	SI

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Aggiornamento metadati	FL_FORZA_UPD_META_INARK	Indica se si forza l'aggiornamento metadati per unita' doc in archivio (false, true)	NO	NO	SI
Aggiunta documento	FL_ABILITA_FORZA_DOC_AGG	Abilita Forza aggiunta documento(false, true)	SI		SI
Aggiunta documento	FL_ACCETTA_DOC_AGG_NEG	Consente di superare un esito di controllo negativo per documento aggiunto(false, true)	NO		SI
Aggiunta documento	FL_FORZA_DOC_AGG	Forza l'accettazione del controllo per documento aggiunto negativo (false, true)	NO		SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NEG	Consente di superare un esito di controllo CRL negativo con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NOSCAR	Consente di superare un esito di controllo CRL non scaricabile con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NOVAL	Consente di superare un esito di controllo CRL non valida con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_SCAD	Consente di superare un esito di controllo CRL scaduta con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_NOCERT	Consente di superare un esito di controllo certificato che non e' un certificato con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_NOVAL	Consente di superare un esito di controllo certificato non valido con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_SCAD	Consente di superare un esito di controllo certificato scaduto con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma crittografico	FL_ABILITA_CONTR_CRITTOG_VERS	Abilita il controllo crittografico (false, true)	SI	SI	SI

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Controlli firma crittografico	FL_ACCETTA_CONTR_CRITTOG_NEG	Consente di superare un esito di controllo crittografico negativo con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_FIRMA_GIUGNO_2011	Consente di superare un esito di controllo negativo per firma no delibera 45 con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_FIRMA_NOCONF	Consente di superare un esito di controllo negativo per firma non conforme con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_FIRMA_NOCONOS	Consente di superare un esito di controllo negativo per firma sconosciuta con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_MARCA_NOCONOS	Consente di superare un esito di controllo negativo per marca sconosciuta con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma trusted	FL_ABILITA_CONTR_TRUST_VERS	Abilita il controllo di catena trusted (false, true)	SI	SI	SI
Controlli firma trusted	FL_ACCETTA_CONTR_TRUST_NEG	Consente di superare un esito di controllo catena trusted negativo con il Forza accettazione (false, true)	SI	SI	SI
Controllo collegamenti fra unità doc	FL_ABILITA_CONTR_COLLEG_UD	Abilita il controllo dei collegamenti fra unità documentarie (false, true)	SI		SI
Controllo collegamenti fra unità doc	FL_ACCETTA_CONTR_COLLEG_NEG	Consente di superare un esito controllo collegamenti negativo con il Forza collegamenti (false, true)	NO		SI
Controllo collegamenti fra unità doc	FL_FORZA_COLLEG	Forza l'accettazione del controllo collegamenti negativo (false, true)	NO		SI

Tipologia di unità documentaria PIANO URBANISTICO GENERALE

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Accettazione formati file	FL_ABILITA_CONTR_FMT	Abilita il controllo del formato file versato (false, true)	SI		SI
Accettazione formati file	FL_ACCETTA_CONTR_FMT_NEG	Consente di superare un esito controllo formato file negativo con il Forza formato (false, true)	SI		SI
Accettazione formati file	FL_FORZA_FMT	Forza l'accettazione del controllo formato file negativo (false, true)	SI		SI
Accettazione formati numero unità doc	FL_ABILITA_CONTR_FMT_NUM	Abilita il controllo del formato del numero dell'unità doc (false, true)	SI	SI	SI
Accettazione formati numero unità doc	FL_ACCETTA_FMT_NUM_NEG	Consente di superare un esito controllo formato del numero dell'unità doc negativo con il Forza formato (false, true)	NO	NO	SI
Accettazione formati numero unità doc	FL_FORZA_FMT_NUM	Forza l'accettazione del controllo formato del numero dell'unità doc negativo (false, true)	NO	NO	SI
Accettazione hash versato	FL_ABILITA_CONTR_HASH_VERS	Abilita il controllo del hash versato (false, true)	NO	NO	SI
Accettazione hash versato	FL_ACCETTA_CONTR_HASH_NEG	Consente di superare un esito controllo hash versato negativo con il Forza hash versato (false, true)	SI	NO	SI
Accettazione hash versato	FL_FORZA_HASH_VERS	Forza l'accettazione del controllo hash versato negativo (false, true)	SI	NO	SI
Aggiornamento metadati	FL_ABILITA_UPD_META	Indica se e' abilitato il servizio di aggiornamento metadati unita' doc (false, true)	NO	NO	SI

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Aggiornamento metadati	FL_ACCETTA_UPD_META_INARK	Indica se si accetta l'aggiornamento metadati per unita' doc in archivio con il Forza aggiornamento (false, true)	NO	NO	SI
Aggiornamento metadati	FL_FORZA_UPD_META_INARK	Indica se si forza l'aggiornamento metadati per unita' doc in archivio (false, true)	NO	NO	SI
Aggiunta documento	FL_ABILITA_FORZA_DOC_AGG	Abilita Forza aggiunta documento(false, true)	SI		SI
Aggiunta documento	FL_ACCETTA_DOC_AGG_NEG	Consente di superare un esito di controllo negativo per documento aggiunto(false, true)	NO		SI
Aggiunta documento	FL_FORZA_DOC_AGG	Forza l'accettazione del controllo per documento aggiunto negativo (false, true)	NO		SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NEG	Consente di superare un esito di controllo CRL negativo con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NOSCAR	Consente di superare un esito di controllo CRL non scaricabile con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NOVAL	Consente di superare un esito di controllo CRL non valida con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_SCAD	Consente di superare un esito di controllo CRL scaduta con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_NOCERT	Consente di superare un esito di controllo certificato che non e' un certificato con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_NOVAL	Consente di superare un esito di controllo certificato non valido con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_SCAD	Consente di superare un esito di controllo certificato scaduto con il Forza accettazione (false, true)	SI	SI	SI

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Controlli firma crittografico	FL_ABILITA_CONTR_CRITTOG_VERS	Abilita il controllo crittografico (false, true)	SI	SI	SI
Controlli firma crittografico	FL_ACCETTA_CONTR_CRITTOG_NEG	Consente di superare un esito di controllo crittografico negativo con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_FIRMA_GIUGNO_2011	Consente di superare un esito di controllo negativo per firma no delibera 45 con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_FIRMA_NOCONF	Consente di superare un esito di controllo negativo per firma non conforme con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_FIRMA_NOCONOS	Consente di superare un esito di controllo negativo per firma sconosciuta con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_MARCA_NOCONOS	Consente di superare un esito di controllo negativo per marca sconosciuta con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma trusted	FL_ABILITA_CONTR_TRUST_VERS	Abilita il controllo di catena trusted (false, true)	SI	SI	SI
Controlli firma trusted	FL_ACCETTA_CONTR_TRUST_NEG	Consente di superare un esito di controllo catena trusted negativo con il Forza accettazione (false, true)	SI	SI	SI
Controllo collegamenti fra unità doc	FL_ABILITA_CONTR_COLLEG_UD	Abilita il controllo dei collegamenti fra unità documentarie (false, true)	SI		SI
Controllo collegamenti fra unità doc	FL_ACCETTA_CONTR_COLLEG_NEG	Consente di superare un esito controllo collegamenti negativo con il Forza collegamenti (false, true)	NO		SI

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Controllo collegamenti fra unità doc	FL_FORZA_COLLEG	Forza l'accettazione del controllo collegamenti negativo (false, true)	NO		SI

Tipologia di unità documentaria PROCEDIMENTO UNICO

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Accettazione formati file	FL_ABILITA_CONTR_FMT	Abilita il controllo del formato file versato (false, true)	SI		SI
Accettazione formati file	FL_ACCETTA_CONTR_FMT_NEG	Consente di superare un esito controllo formato file negativo con il Forza formato (false, true)	SI		SI
Accettazione formati file	FL_FORZA_FMT	Forza l'accettazione del controllo formato file negativo (false, true)	SI		SI
Accettazione formati numero unità doc	FL_ABILITA_CONTR_FMT_NUM	Abilita il controllo del formato del numero dell'unità doc (false, true)	SI	SI	SI
Accettazione formati numero unità doc	FL_ACCETTA_FMT_NUM_NEG	Consente di superare un esito controllo formato del numero dell'unità doc negativo con il Forza formato (false, true)	NO	NO	SI
Accettazione formati numero unità doc	FL_FORZA_FMT_NUM	Forza l'accettazione del controllo formato del numero dell'unità doc negativo (false, true)	NO	NO	SI
Accettazione hash versato	FL_ABILITA_CONTR_HASH_VERS	Abilita il controllo del hash versato (false, true)	NO	NO	SI

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Accettazione hash versato	FL_ACCETTA_CONTR_HASH_NEG	Consente di superare un esito controllo hash versato negativo con il Forza hash versato (false, true)	SI	NO	SI
Accettazione hash versato	FL_FORZA_HASH_VERS	Forza l'accettazione del controllo hash versato negativo (false, true)	SI	NO	SI
Aggiornamento metadati	FL_ABILITA_UPD_META	Indica se e' abilitato il servizio di aggiornamento metadati unita' doc (false, true)	NO	NO	SI
Aggiornamento metadati	FL_ACCETTA_UPD_META_INARK	Indica si accetta l'aggiornamento metadati per unita' doc in archivio con il Forza aggiornamento (false, true)	NO	NO	SI
Aggiornamento metadati	FL_FORZA_UPD_META_INARK	Indica se si forza l'aggiornamento metadati per unita' doc in archivio (false, true)	NO	NO	SI
Aggiunta documento	FL_ABILITA_FORZA_DOC_AGG	Abilita Forza aggiunta documento(false, true)	SI		SI
Aggiunta documento	FL_ACCETTA_DOC_AGG_NEG	Consente di superare un esito di controllo negativo per documento aggiunto(false, true)	NO		SI
Aggiunta documento	FL_FORZA_DOC_AGG	Forza l'accettazione del controllo per documento aggiunto negativo (false, true)	NO		SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NEG	Consente di superare un esito di controllo CRL negativo con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NOSCAR	Consente di superare un esito di controllo CRL non scaricabile con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NOVAL	Consente di superare un esito di controllo CRL non valida con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_SCAD	Consente di superare un esito di controllo CRL scaduta con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_NOCERT	Consente di superare un esito di controllo certificato che non e' un certificato con il Forza accettazione (false, true)	SI	SI	SI

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_NOVAL	Consente di superare un esito di controllo certificato non valido con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_SCAD	Consente di superare un esito di controllo certificato scaduto con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma crittografico	FL_ABILITA_CONTR_CRITTOG_VERS	Abilita il controllo crittografico (false, true)	SI	SI	SI
Controlli firma crittografico	FL_ACCETTA_CONTR_CRITTOG_NEG	Consente di superare un esito di controllo crittografico negativo con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_FIRMA_GIUGNO_2011	Consente di superare un esito di controllo negativo per firma no delibera 45 con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_FIRMA_NOCONF	Consente di superare un esito di controllo negativo per firma non conforme con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_FIRMA_NOCONOS	Consente di superare un esito di controllo negativo per firma sconosciuta con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_MARCA_NOCONOS	Consente di superare un esito di controllo negativo per marca sconosciuta con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma trusted	FL_ABILITA_CONTR_TRUST_VERS	Abilita il controllo di catena trusted (false, true)	SI	SI	SI
Controlli firma trusted	FL_ACCETTA_CONTR_TRUST_NEG	Consente di superare un esito di controllo catena trusted negativo con il Forza accettazione (false, true)	SI	SI	SI

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Controllo collegamenti fra unità doc	FL_ABILITA_CONTR_COLLEG_UD	Abilita il controllo dei collegamenti fra unità documentarie (false, true)	SI		SI
Controllo collegamenti fra unità doc	FL_ACCETTA_CONTR_COLLEG_NEG	Consente di superare un esito controllo collegamenti negativo con il Forza collegamenti (false, true)	NO		SI
Controllo collegamenti fra unità doc	FL_FORZA_COLLEG	Forza l'accettazione del controllo collegamenti negativo (false, true)	NO		SI

Tipologia di unità documentaria VARIANTE DI PIANO

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Accettazione formati file	FL_ABILITA_CONTR_FMT	Abilita il controllo del formato file versato (false, true)	SI		SI
Accettazione formati file	FL_ACCETTA_CONTR_FMT_NEG	Consente di superare un esito controllo formato file negativo con il Forza formato (false, true)	SI		SI
Accettazione formati file	FL_FORZA_FMT	Forza l'accettazione del controllo formato file negativo (false, true)	SI		SI
Accettazione formati numero unità doc	FL_ABILITA_CONTR_FMT_NUM	Abilita il controllo del formato del numero dell'unità doc (false, true)	SI	SI	SI
Accettazione formati numero unità doc	FL_ACCETTA_FMT_NUM_NEG	Consente di superare un esito controllo formato del numero dell'unità doc negativo con il Forza formato (false, true)	NO	NO	SI

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Accettazione formati numero unità doc	FL_FORZA_FMT_NUM	Forza l'accettazione del controllo formato del numero dell'unità doc negativo (false, true)	NO	NO	SI
Accettazione hash versato	FL_ABILITA_CONTR_HASH_VERS	Abilita il controllo del hash versato (false, true)	NO	NO	SI
Accettazione hash versato	FL_ACCETTA_CONTR_HASH_NEG	Consente di superare un esito controllo hash versato negativo con il Forza hash versato (false, true)	SI	NO	SI
Accettazione hash versato	FL_FORZA_HASH_VERS	Forza l'accettazione del controllo hash versato negativo (false, true)	SI	NO	SI
Aggiornamento metadati	FL_ABILITA_UPD_META	Indica se e' abilitato il servizio di aggiornamento metadati unita' doc (false, true)	NO	NO	SI
Aggiornamento metadati	FL_ACCETTA_UPD_META_INARK	Indica si accetta l'aggiornamento metadati per unita' doc in archivio con il Forza aggiornamento (false, true)	NO	NO	SI
Aggiornamento metadati	FL_FORZA_UPD_META_INARK	Indica se si forza l'aggiornamento metadati per unita' doc in archivio (false, true)	NO	NO	SI
Aggiunta documento	FL_ABILITA_FORZA_DOC_AGG	Abilita Forza aggiunta documento(false, true)	SI		SI
Aggiunta documento	FL_ACCETTA_DOC_AGG_NEG	Consente di superare un esito di controllo negativo per documento aggiunto(false, true)	NO		SI
Aggiunta documento	FL_FORZA_DOC_AGG	Forza l'accettazione del controllo per documento aggiunto negativo (false, true)	NO		SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NEG	Consente di superare un esito di controllo CRL negativo con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NOSCAR	Consente di superare un esito di controllo CRL non scaricabile con il Forza accettazione (false, true)	SI	SI	SI

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_NOVAL	Consente di superare un esito di controllo CRL non valida con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma CRL	FL_ACCETTA_CONTR_CRL_SCAD	Consente di superare un esito di controllo CRL scaduta con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_NOCERT	Consente di superare un esito di controllo certificato che non e' un certificato con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_NOVAL	Consente di superare un esito di controllo certificato non valido con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma certificato	FL_ACCETTA_CONTR_CERTIF_SCAD	Consente di superare un esito di controllo certificato scaduto con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma crittografico	FL_ABILITA_CONTR_CRITTOG_VERS	Abilita il controllo crittografico (false, true)	SI	SI	SI
Controlli firma crittografico	FL_ACCETTA_CONTR_CRITTOG_NEG	Consente di superare un esito di controllo crittografico negativo con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_FIRMA_GIUGNO_2011	Consente di superare un esito di controllo negativo per firma no delibera 45 con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_FIRMA_NOCONF	Consente di superare un esito di controllo negativo per firma non conforme con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma non conforme	FL_ACCETTA_FIRMA_NOCONOS	Consente di superare un esito di controllo negativo per firma sconosciuta con il Forza accettazione (false, true)	SI	SI	SI

Funzione	Parametro	Descrizione	Valore standard	Valore sulla struttura	Valore effettivo (Richiesto dall'Ente)
Controlli firma non conforme	FL_ACCETTA_MARCA_NOCONOS	Consente di superare un esito di controllo negativo per marca sconosciuta con il Forza accettazione (false, true)	SI	SI	SI
Controlli firma trusted	FL_ABILITA_CONTR_TRUST_VERS	Abilita il controllo di catena trusted (false, true)	SI	SI	SI
Controlli firma trusted	FL_ACCETTA_CONTR_TRUST_NEG	Consente di superare un esito di controllo catena trusted negativo con il Forza accettazione (false, true)	SI	SI	SI
Controllo collegamenti fra unità doc	FL_ABILITA_CONTR_COLLEG_UD	Abilita il controllo dei collegamenti fra unità documentarie (false, true)	SI		SI
Controllo collegamenti fra unità doc	FL_ACCETTA_CONTR_COLLEG_NEG	Consente di superare un esito controllo collegamenti negativo con il Forza collegamenti (false, true)	NO		SI
Controllo collegamenti fra unità doc	FL_FORZA_COLLEG	Forza l'accettazione del controllo collegamenti negativo (false, true)	NO		SI

Formati ammessi

Nella Tabella dei Formati sono elencati i formati configurati nella struttura.

In base all'impostazione "standard" tutti i formati classificati come IDONEI e GESTITI ai fini della conservazione a lungo termine sono ammessi con modalità automatica corrispondentemente ai formati classificati come tali nel Registro dei formati di ParER (accessibile dall'interfaccia di Sacer).

E' facoltà dell'Ente richiedere l'ammissione dei formati appartenenti alle categorie sopra dette con gestione alternativa a quella automatica, anche in relazione a formati definiti in modo specifico per la tipologia di unità documentaria.

I formati classificati come DEPRECATI possono essere ammessi solo su richiesta dell'Ente.

Nel Registro dei formati di ParER, unitamente all'attribuzione della qualifica di idoneità alla conservazione, viene associato a ciascun formato un punteggio in base al principio di interoperabilità, coerentemente con quanto previsto nell'Allegato 2 (Formati di file e riversamento) alle "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici".

In base all'idoneità in relazione alla conservazione a lungo termine, nel Registro dei formati di ParER i formati sono classificati come segue:

- **Formati idonei:** sono i formati che sono reputati idonei alla conservazione a lungo termine, con riferimento anche alle indicazioni fornite nelle stesse Linee Guida Agid (capitolo 2 dell'Allegato 2) in merito all'utilizzo del formato ai fini della conservazione;
- **Formati gestiti:** sono i formati non ritenuti idonei per la conservazione a lungo termine ma che possono essere opportunamente riversati in formati adatti alla conservazione, coerentemente a quanto indicato nel capitolo 3.3 dell'Allegato 2 delle Linee Guida;
- **Formati deprecati:** sono formati ritenuti non idonei per la conservazione a lungo termine e che al contempo non possono essere riversati in Formati idonei, per i quali, quindi, non è possibile assicurare la conservazione a lungo termine.

Formato versato ammesso	Mimetype	Idoneità alla conservazione
7Z	application/x-7z-compressed	GESTITO
7Z.ASICE	application/x-7z-compressed	GESTITO
7Z.ASICS	application/x-7z-compressed	GESTITO
7Z.P7M	application/x-7z-compressed	GESTITO
7Z.P7S	application/x-7z-compressed	GESTITO
ACE	application/x-ace-compressed	IDONEO
ACE.ASICE	application/x-ace-compressed	IDONEO
ACE.ASICS	application/x-ace-compressed	IDONEO
ACE.P7M	application/x-ace-compressed	IDONEO
ACE.P7S	application/x-ace-compressed	IDONEO
AXX	application/x-axcrypt	GESTITO
AXX.ASICE	application/x-axcrypt	GESTITO
AXX.ASICS	application/x-axcrypt	GESTITO
AXX.P7M	application/x-axcrypt	GESTITO
AXX.P7S	application/x-axcrypt	GESTITO
BMP	image/x-ms-bmp	IDONEO
BMP.ASICE	image/x-ms-bmp	IDONEO
BMP.ASICS	image/x-ms-bmp	IDONEO
BMP.P7M	image/x-ms-bmp	IDONEO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
BMP.P7S	image/x-ms-bmp	IDONEO
CER	application/octet-stream	GESTITO
CER.ASICE	application/octet-stream	GESTITO
CER.ASICS	application/octet-stream	GESTITO
CER.P7M	application/octet-stream	GESTITO
CER.P7S	application/octet-stream	GESTITO
CPG	text/plain	GESTITO
CPG.ASICE	text/plain	GESTITO
CPG.ASICS	text/plain	GESTITO
CPG.P7M	text/plain	GESTITO
CPG.P7S	text/plain	GESTITO
CRL	application/octet-stream	GESTITO
CRL.ASICE	application/octet-stream	GESTITO
CRL.ASICS	application/octet-stream	GESTITO
CRL.P7M	application/octet-stream	GESTITO
CRL.P7S	application/octet-stream	GESTITO
CSS	text/plain	IDONEO
CSS.ASICE	text/plain	IDONEO
CSS.ASICS	text/plain	IDONEO
CSS.P7M	text/plain	IDONEO
CSS.P7S	text/plain	IDONEO
CSV	text/plain	IDONEO
CSV.ASICE	text/plain	IDONEO
CSV.ASICS	text/plain	IDONEO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
CSV.P7M	text/plain	IDONEO
CSV.P7S	text/plain	IDONEO
DBF	application/x-dbf	GESTITO
DBF.ASICE	application/x-dbf	GESTITO
DBF.ASICS	application/x-dbf	GESTITO
DBF.P7M	application/x-dbf	GESTITO
DBF.P7S	application/x-dbf	GESTITO
DER	application/x-x509-ca-cert	GESTITO
DIB	image/x-ms-bmp	IDONEO
DIB.ASICE	image/x-ms-bmp	IDONEO
DIB.ASICS	image/x-ms-bmp	IDONEO
DIB.P7M	image/x-ms-bmp	IDONEO
DIB.P7S	image/x-ms-bmp	IDONEO
DOC	application/msword	GESTITO
DOC.ASICE	application/msword	GESTITO
DOC.ASICS	application/msword	GESTITO
DOC.P7M	application/msword	GESTITO
DOC.P7S	application/msword	GESTITO
DOCM	application/vnd.ms-word.document.macroenabled.12	DEPRECATO
DOCM.ASICE	application/vnd.ms-word.document.macroenabled.12	DEPRECATO
DOCM.ASICS	application/vnd.ms-word.document.macroenabled.12	DEPRECATO
DOCM.P7M	application/vnd.ms-word.document.macroenabled.12	DEPRECATO
DOCM.P7S	application/vnd.ms-word.document.macroenabled.12	DEPRECATO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
DOCX	application/vnd.openxmlformats-officedocument.wordprocessingml.document	GESTITO
DOCX.ASICE	application/vnd.openxmlformats-officedocument.wordprocessingml.document	GESTITO
DOCX.ASICS	application/vnd.openxmlformats-officedocument.wordprocessingml.document	GESTITO
DOCX.P7M	application/vnd.openxmlformats-officedocument.wordprocessingml.document	GESTITO
DOCX.P7S	application/vnd.openxmlformats-officedocument.wordprocessingml.document	GESTITO
DOT	application/msword	GESTITO
DOT.ASICE	application/msword	GESTITO
DOT.ASICS	application/msword	GESTITO
DOT.P7M	application/msword	GESTITO
DOT.P7S	application/msword	GESTITO
DOTX	application/vnd.openxmlformats-officedocument.wordprocessingml.template	GESTITO
DOTX.ASICE	application/vnd.openxmlformats-officedocument.wordprocessingml.template	GESTITO
DOTX.ASICS	application/vnd.openxmlformats-officedocument.wordprocessingml.template	GESTITO
DOTX.P7M	application/vnd.openxmlformats-officedocument.wordprocessingml.template	GESTITO
DOTX.P7S	application/vnd.openxmlformats-officedocument.wordprocessingml.template	GESTITO
DTD	text/plain	IDONEO
DTD.ASICE	text/plain	IDONEO
DTD.ASICS	text/plain	IDONEO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
DTD.P7M	text/plain	IDONEO
DTD.P7S	text/plain	IDONEO
DWF	model/vnd.dwf	GESTITO
DWF.ASICE	model/vnd.dwf	GESTITO
DWF.ASICS	model/vnd.dwf	GESTITO
DWF.P7M	model/vnd.dwf	GESTITO
DWF.P7S	model/vnd.dwf	GESTITO
DWFX	model/vnd.dwfx+xps	GESTITO
DWFX.ASICE	model/vnd.dwfx+xps	GESTITO
DWFX.ASICS	model/vnd.dwfx+xps	GESTITO
DWFX.P7M	model/vnd.dwfx+xps	GESTITO
DWFX.P7S	model/vnd.dwfx+xps	GESTITO
DWG	image/vnd.dwg	DEPRECATO
DWG.ASICE	image/vnd.dwg	DEPRECATO
DWG.ASICS	image/vnd.dwg	DEPRECATO
DWG.P7M	image/vnd.dwg	DEPRECATO
DWG.P7S	image/vnd.dwg	DEPRECATO
DXF	image/vnd.dxf	GESTITO
DXF.ASICE	image/vnd.dxf	GESTITO
DXF.ASICS	image/vnd.dxf	GESTITO
DXF.P7M	image/vnd.dxf	GESTITO
DXF.P7S	image/vnd.dxf	GESTITO
EML	message/rfc822	IDONEO
EML.ASICE	message/rfc822	IDONEO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
EML.ASICS	message/rfc822	IDONEO
EML.P7M	message/rfc822	IDONEO
EML.P7S	message/rfc822	IDONEO
EMLX	message/x-emlx	GESTITO
EMLX.ASICE	message/x-emlx	GESTITO
EMLX.ASICS	message/x-emlx	GESTITO
EMLX.P7M	message/x-emlx	GESTITO
EMLX.P7S	message/x-emlx	GESTITO
ENC	application/octet-stream	DEPRECATO
EPS	application/postscript	GESTITO
EPS.ASICE	application/postscript	GESTITO
EPS.ASICS	application/postscript	GESTITO
EPS.P7M	application/postscript	GESTITO
EPS.P7S	application/postscript	GESTITO
FO	application/xslfo+xml	IDONEO
FO.ASICE	application/xslfo+xml	IDONEO
FO.ASICS	application/xslfo+xml	IDONEO
FO.P7M	application/xslfo+xml	IDONEO
FO.P7S	application/xslfo+xml	IDONEO
FODG	application/vnd.oasis.opendocument.graphics-flat+xml	GESTITO
FODG.ASICE	application/vnd.oasis.opendocument.graphics-flat+xml	GESTITO
FODG.ASICS	application/vnd.oasis.opendocument.graphics-flat+xml	GESTITO
FODG.P7M	application/vnd.oasis.opendocument.graphics-flat+xml	GESTITO
FODG.P7S	application/vnd.oasis.opendocument.graphics-flat+xml	GESTITO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
GIF	image/gif	IDONEO
GIF.ASICE	image/gif	IDONEO
GIF.ASICS	image/gif	IDONEO
GIF.P7M	image/gif	IDONEO
GIF.P7S	image/gif	IDONEO
GZ	application/gzip	GESTITO
GZ.ASICE	application/gzip	GESTITO
GZ.ASICS	application/gzip	GESTITO
GZ.P7M	application/gzip	GESTITO
GZ.P7S	application/gzip	GESTITO
HTM	text/html	GESTITO
HTM.ASICE	text/html	GESTITO
HTM.ASICS	text/html	GESTITO
HTM.P7M	text/html	GESTITO
HTM.P7S	text/html	GESTITO
HTML	text/html	GESTITO
HTML.ASICE	text/html	GESTITO
HTML.ASICS	text/html	GESTITO
HTML.P7M	text/html	GESTITO
HTML.P7S	text/html	GESTITO
ICO	image/vnd.microsoft.icon	IDONEO
ICO.ASICE	image/vnd.microsoft.icon	IDONEO
ICO.ASICS	image/vnd.microsoft.icon	IDONEO
ICO.P7M	image/vnd.microsoft.icon	IDONEO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
ICO.P7S	image/vnd.microsoft.icon	IDONEO
INDD	application/x-adobe-indesign	GESTITO
INDD.ASICE	application/x-adobe-indesign	GESTITO
INDD.ASICS	application/x-adobe-indesign	GESTITO
INDD.P7M	application/x-adobe-indesign	GESTITO
INDD.P7S	application/x-adobe-indesign	GESTITO
JFIF	image/jpeg	IDONEO
JFIF.ASICE	image/jpeg	IDONEO
JFIF.ASICS	image/jpeg	IDONEO
JFIF.P7M	image/jpeg	IDONEO
JFIF.P7S	image/jpeg	IDONEO
JPE	image/jpeg	IDONEO
JPE.ASICE	image/jpeg	IDONEO
JPE.ASICS	image/jpeg	IDONEO
JPE.P7M	image/jpeg	IDONEO
JPE.P7S	image/jpeg	IDONEO
JPEG	image/jpeg	IDONEO
JPEG.ASICE	image/jpeg	IDONEO
JPEG.ASICS	image/jpeg	IDONEO
JPEG.P7M	image/jpeg	IDONEO
JPEG.P7S	image/jpeg	IDONEO
JPG	image/jpeg	IDONEO
JPG.ASICE	image/jpeg	IDONEO
JPG.ASICS	image/jpeg	IDONEO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
JPG.P7M	image/jpeg	IDONEO
JPG.P7S	image/jpeg	IDONEO
JSON	text/plain	GESTITO
JSON.ASICE	text/plain	GESTITO
JSON.ASICS	text/plain	GESTITO
JSON.P7M	text/plain	GESTITO
JSON.P7S	text/plain	GESTITO
KML	application/vnd.google-earth.kml+xml	GESTITO
KML.ASICE	application/vnd.google-earth.kml+xml	GESTITO
KML.ASICS	application/vnd.google-earth.kml+xml	GESTITO
KML.P7M	application/vnd.google-earth.kml+xml	GESTITO
KML.P7S	application/vnd.google-earth.kml+xml	GESTITO
KMZ	application/vnd.google-earth.kmz	GESTITO
KMZ.ASICE	application/vnd.google-earth.kmz	GESTITO
KMZ.ASICS	application/vnd.google-earth.kmz	GESTITO
KMZ.P7M	application/vnd.google-earth.kmz	GESTITO
KMZ.P7S	application/vnd.google-earth.kmz	GESTITO
LNK	application/octet-stream	DEPRECATO
LOG	text/plain	IDONEO
M7M	multipart/mixed	IDONEO
MHT	message/rfc822	IDONEO
MHT.ASICE	message/rfc822	IDONEO
MHT.ASICS	message/rfc822	IDONEO
MHT.P7M	message/rfc822	IDONEO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
MHT.P7S	message/rfc822	IDONEO
MIME	message/rfc822	DEPRECATO
MSG	application/vnd.ms-outlook	GESTITO
MSG.ASICE	application/vnd.ms-outlook	GESTITO
MSG.ASICS	application/vnd.ms-outlook	GESTITO
MSG.P7M	application/vnd.ms-outlook	GESTITO
MSG.P7S	application/vnd.ms-outlook	GESTITO
MSO	application/octet-stream	DEPRECATO
MXD	application/octet-stream	DEPRECATO
ODB	application/vnd.oasis.opendocument.base	GESTITO
ODB.ASICE	application/vnd.oasis.opendocument.base	GESTITO
ODB.ASICS	application/vnd.oasis.opendocument.base	GESTITO
ODB.P7M	application/vnd.oasis.opendocument.base	GESTITO
ODB.P7S	application/vnd.oasis.opendocument.base	GESTITO
ODF	application/vnd.oasis.opendocument.formula	IDONEO
ODF.ASICE	application/vnd.oasis.opendocument.formula	IDONEO
ODF.ASICS	application/vnd.oasis.opendocument.formula	IDONEO
ODF.P7M	application/vnd.oasis.opendocument.formula	IDONEO
ODF.P7S	application/vnd.oasis.opendocument.formula	IDONEO
ODG	application/vnd.oasis.opendocument.graphics	GESTITO
ODG.ASICE	application/vnd.oasis.opendocument.graphics	GESTITO
ODG.ASICS	application/vnd.oasis.opendocument.graphics	GESTITO
ODG.P7M	application/vnd.oasis.opendocument.graphics	GESTITO
ODG.P7S	application/vnd.oasis.opendocument.graphics	GESTITO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
ODP	application/vnd.oasis.opendocument.presentation	GESTITO
ODP.ASICE	application/vnd.oasis.opendocument.presentation	GESTITO
ODP.ASICS	application/vnd.oasis.opendocument.presentation	GESTITO
ODP.P7M	application/vnd.oasis.opendocument.presentation	GESTITO
ODP.P7S	application/vnd.oasis.opendocument.presentation	GESTITO
ODS	application/vnd.oasis.opendocument.spreadsheet	GESTITO
ODS.ASICE	application/vnd.oasis.opendocument.spreadsheet	GESTITO
ODS.ASICS	application/vnd.oasis.opendocument.spreadsheet	GESTITO
ODS.P7M	application/vnd.oasis.opendocument.spreadsheet	GESTITO
ODS.P7S	application/vnd.oasis.opendocument.spreadsheet	GESTITO
ODT	application/vnd.oasis.opendocument.text	GESTITO
ODT.ASICE	application/vnd.oasis.opendocument.text	GESTITO
ODT.ASICS	application/vnd.oasis.opendocument.text	GESTITO
ODT.P7M	application/vnd.oasis.opendocument.text	GESTITO
ODT.P7S	application/vnd.oasis.opendocument.text	GESTITO
OFT	application/vnd.ms-outlook	GESTITO
OFT.ASICE	application/vnd.ms-outlook	GESTITO
OFT.ASICS	application/vnd.ms-outlook	GESTITO
OFT.P7M	application/vnd.ms-outlook	GESTITO
OFT.P7S	application/vnd.ms-outlook	GESTITO
OTS	application/vnd.oasis.opendocument.spreadsheet-template	GESTITO
OTS.ASICE	application/vnd.oasis.opendocument.spreadsheet-template	GESTITO
OTS.ASICS	application/vnd.oasis.opendocument.spreadsheet-template	GESTITO
OTS.P7M	application/vnd.oasis.opendocument.spreadsheet-template	GESTITO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
OTS.P7S	application/vnd.oasis.opendocument.spreadsheet-template	GESTITO
OTT	application/vnd.oasis.opendocument.text-template	GESTITO
OTT.ASICE	application/vnd.oasis.opendocument.text-template	GESTITO
OTT.ASICS	application/vnd.oasis.opendocument.text-template	GESTITO
OTT.P7M	application/vnd.oasis.opendocument.text-template	GESTITO
OTT.P7S	application/vnd.oasis.opendocument.text-template	GESTITO
P7M	application/pkcs7-mime	GESTITO
P7S	application/pkcs7-signature	GESTITO
P7S.ASICE	application/pkcs7-signature	GESTITO
P7S.ASICS	application/pkcs7-signature	GESTITO
P7S.P7M	application/pkcs7-signature	GESTITO
P7S.P7S	application/pkcs7-signature	GESTITO
P7X	multipart/mixed	GESTITO
PDF	application/pdf	IDONEO
PDF.ASICE	application/pdf	IDONEO
PDF.ASICS	application/pdf	IDONEO
PDF.P7M	application/pdf	IDONEO
PDF.P7M.TSD	application/pdf	IDONEO
PDF.P7S	application/pdf	IDONEO
PNG	image/png	GESTITO
PNG.ASICE	image/png	GESTITO
PNG.ASICS	image/png	GESTITO
PNG.P7M	image/png	GESTITO
PNG.P7S	image/png	GESTITO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
POT	application/vnd.ms-powerpoint	GESTITO
POT.ASICE	application/vnd.ms-powerpoint	GESTITO
POT.ASICS	application/vnd.ms-powerpoint	GESTITO
POT.P7M	application/vnd.ms-powerpoint	GESTITO
POT.P7S	application/vnd.ms-powerpoint	GESTITO
PPS	application/vnd.ms-powerpoint	GESTITO
PPS.ASICE	application/vnd.ms-powerpoint	GESTITO
PPS.ASICS	application/vnd.ms-powerpoint	GESTITO
PPS.P7M	application/vnd.ms-powerpoint	GESTITO
PPS.P7S	application/vnd.ms-powerpoint	GESTITO
PPSX	application/vnd.openxmlformats-officedocument.presentationml.slideshow	IDONEO
PPSX.ASICE	application/vnd.openxmlformats-officedocument.presentationml.slideshow	IDONEO
PPSX.ASICS	application/vnd.openxmlformats-officedocument.presentationml.slideshow	IDONEO
PPSX.P7M	application/vnd.openxmlformats-officedocument.presentationml.slideshow	IDONEO
PPSX.P7S	application/vnd.openxmlformats-officedocument.presentationml.slideshow	IDONEO
PPT	application/vnd.ms-powerpoint	GESTITO
PPT.ASICE	application/vnd.ms-powerpoint	GESTITO
PPT.ASICS	application/vnd.ms-powerpoint	GESTITO
PPT.P7M	application/vnd.ms-powerpoint	GESTITO
PPT.P7S	application/vnd.ms-powerpoint	GESTITO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
PPTM	application/vnd.ms-powerpoint.presentation.macroenabled.12	GESTITO
PPTM.ASICE	application/vnd.ms-powerpoint.presentation.macroenabled.12	GESTITO
PPTM.ASICS	application/vnd.ms-powerpoint.presentation.macroenabled.12	GESTITO
PPTM.P7M	application/vnd.ms-powerpoint.presentation.macroenabled.12	GESTITO
PPTM.P7S	application/vnd.ms-powerpoint.presentation.macroenabled.12	GESTITO
PPTX	application/vnd.openxmlformats-officedocument.presentationml.presentation	GESTITO
PPTX.ASICE	application/vnd.openxmlformats-officedocument.presentationml.presentation	GESTITO
PPTX.ASICS	application/vnd.openxmlformats-officedocument.presentationml.presentation	GESTITO
PPTX.P7M	application/vnd.openxmlformats-officedocument.presentationml.presentation	GESTITO
PPTX.P7S	application/vnd.openxmlformats-officedocument.presentationml.presentation	GESTITO
PRJ	text/plain	GESTITO
PRJ.ASICE	text/plain	GESTITO
PRJ.ASICS	text/plain	GESTITO
PRJ.P7M	text/plain	GESTITO
PRJ.P7S	text/plain	GESTITO
PSD	image/vnd.adobe.photoshop	GESTITO
PSD.ASICE	image/vnd.adobe.photoshop	GESTITO
PSD.ASICS	image/vnd.adobe.photoshop	GESTITO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
PSD.P7M	image/vnd.adobe.photoshop	GESTITO
PSD.P7S	image/vnd.adobe.photoshop	GESTITO
PUB	application/x-mspublisher	GESTITO
PUB.ASICE	application/x-mspublisher	GESTITO
PUB.ASICS	application/x-mspublisher	GESTITO
PUB.P7M	application/x-mspublisher	GESTITO
PUB.P7S	application/x-mspublisher	GESTITO
RAR.ASICE	application/x-rar-compressed	GESTITO
RAR.ASICS	application/x-rar-compressed	GESTITO
RAR.P7M	application/x-rar-compressed	GESTITO
RAR.P7S	application/x-rar-compressed	GESTITO
RARV4	application/x-rar-compressed; version=4	GESTITO
RARV4.ASICE	application/x-rar-compressed; version=4	GESTITO
RARV4.ASICS	application/x-rar-compressed; version=4	GESTITO
RARV4.P7M	application/x-rar-compressed; version=4	GESTITO
RARV4.P7S	application/x-rar-compressed; version=4	GESTITO
RARV5	application/x-rar-compressed; version=5	GESTITO
RARV5.ASICE	application/x-rar-compressed; version=5	GESTITO
RARV5.ASICS	application/x-rar-compressed; version=5	GESTITO
RARV5.P7M	application/x-rar-compressed; version=5	GESTITO
RARV5.P7S	application/x-rar-compressed; version=5	GESTITO
RTF	application/rtf	GESTITO
RTF.ASICE	application/rtf	GESTITO
RTF.ASICS	application/rtf	GESTITO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
RTF.P7M	application/rtf	GESTITO
RTF.P7S	application/rtf	GESTITO
SBN	application/octet-stream	GESTITO
SBN.ASICE	application/octet-stream	GESTITO
SBN.ASICS	application/octet-stream	GESTITO
SBN.P7M	application/octet-stream	GESTITO
SBN.P7S	application/octet-stream	GESTITO
SBX	application/octet-stream	GESTITO
SBX.ASICE	application/octet-stream	GESTITO
SBX.ASICS	application/octet-stream	GESTITO
SBX.P7M	application/octet-stream	GESTITO
SBX.P7S	application/octet-stream	GESTITO
SDC	application/vnd.stardivision.calc	IDONEO
SDC.ASICE	application/vnd.stardivision.calc	IDONEO
SDC.ASICS	application/vnd.stardivision.calc	IDONEO
SDC.P7M	application/vnd.stardivision.calc	IDONEO
SDC.P7S	application/vnd.stardivision.calc	IDONEO
SGP	text/plain	IDONEO
SGP.ASICE	text/plain	IDONEO
SGP.ASICS	text/plain	IDONEO
SGP.P7M	text/plain	IDONEO
SGP.P7S	text/plain	IDONEO
SHP	application/x-shapefile	GESTITO
SHP.ASICE	application/x-shapefile	GESTITO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
SHP.ASICS	application/x-shapefile	GESTITO
SHP.P7M	application/x-shapefile	GESTITO
SHP.P7S	application/x-shapefile	GESTITO
SHX	application/x-shapefile	GESTITO
SHX.ASICE	application/x-shapefile	GESTITO
SHX.ASICS	application/x-shapefile	GESTITO
SHX.P7M	application/x-shapefile	GESTITO
SHX.P7S	application/x-shapefile	GESTITO
SITX	application/x-stuffit	IDONEO
SITX.ASICE	application/x-stuffit	IDONEO
SITX.ASICS	application/x-stuffit	IDONEO
SITX.P7M	application/x-stuffit	IDONEO
SITX.P7S	application/x-stuffit	IDONEO
SVG	image/svg+xml	IDONEO
SVG.ASICE	image/svg+xml	IDONEO
SVG.ASICS	image/svg+xml	IDONEO
SVG.P7M	image/svg+xml	IDONEO
SVG.P7S	image/svg+xml	IDONEO
SWF	application/x-shockwave-flash	GESTITO
SWF.ASICE	application/x-shockwave-flash	GESTITO
SWF.ASICS	application/x-shockwave-flash	GESTITO
SWF.P7M	application/x-shockwave-flash	GESTITO
SWF.P7S	application/x-shockwave-flash	GESTITO
SXC	application/vnd.sun.xml.calc	GESTITO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
SXC.ASICE	application/vnd.sun.xml.calc	GESTITO
SXC.ASICS	application/vnd.sun.xml.calc	GESTITO
SXC.P7M	application/vnd.sun.xml.calc	GESTITO
SXC.P7S	application/vnd.sun.xml.calc	GESTITO
SXW	application/vnd.sun.xml.writer	GESTITO
SXW.ASICE	application/vnd.sun.xml.writer	GESTITO
SXW.ASICS	application/vnd.sun.xml.writer	GESTITO
SXW.P7M	application/vnd.sun.xml.writer	GESTITO
SXW.P7S	application/vnd.sun.xml.writer	GESTITO
TAR	application/x-gtar	GESTITO
TAR.ASICE	application/x-gtar	GESTITO
TAR.ASICS	application/x-gtar	GESTITO
TAR.P7M	application/x-gtar	GESTITO
TAR.P7S	application/x-gtar	GESTITO
TEXTCLIPPING	application/octet-stream	GESTITO
TEXTCLIPPING.ASICE	application/octet-stream	GESTITO
TEXTCLIPPING.ASICS	application/octet-stream	GESTITO
TEXTCLIPPING.P7M	application/octet-stream	GESTITO
TEXTCLIPPING.P7S	application/octet-stream	GESTITO
TGZ	application/gzip	GESTITO
THMX	application/vnd.openxmlformats-officedocument	GESTITO
THMX.ASICE	application/vnd.openxmlformats-officedocument	GESTITO
THMX.ASICS	application/vnd.openxmlformats-officedocument	GESTITO
THMX.P7M	application/vnd.openxmlformats-officedocument	GESTITO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
THMX.P7S	application/vnd.openxmlformats-officedocument	GESTITO
TIF	image/tiff	IDONEO
TIF.ASICE	image/tiff	IDONEO
TIF.ASICS	image/tiff	IDONEO
TIF.P7M	image/tiff	IDONEO
TIF.P7S	image/tiff	IDONEO
TIFF	image/tiff	IDONEO
TIFF.ASICE	image/tiff	IDONEO
TIFF.ASICS	image/tiff	IDONEO
TIFF.P7M	image/tiff	IDONEO
TIFF.P7S	image/tiff	IDONEO
TSD	application/timestamped-data	GESTITO
TSR	application/timestamp-reply	GESTITO
TSR.ASICE	application/timestamp-reply	GESTITO
TSR.ASICS	application/timestamp-reply	GESTITO
TSR.P7M	application/timestamp-reply	GESTITO
TSR.P7S	application/timestamp-reply	GESTITO
TXT	text/plain	IDONEO
TXT.ASICE	text/plain	IDONEO
TXT.ASICS	text/plain	IDONEO
TXT.P7M	text/plain	IDONEO
TXT.P7S	text/plain	IDONEO
UNKNOWN	parer/unknonwn	DEPRECATO
VCF	text/x-vcard	GESTITO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
VCF.ASICE	text/x-vcard	GESTITO
VCF.ASICS	text/x-vcard	GESTITO
VCF.P7M	text/x-vcard	GESTITO
VCF.P7S	text/x-vcard	GESTITO
WMZ	application/x-ms-wmz	GESTITO
WMZ.ASICE	application/x-ms-wmz	GESTITO
WMZ.ASICS	application/x-ms-wmz	GESTITO
WMZ.P7M	application/x-ms-wmz	GESTITO
WMZ.P7S	application/x-ms-wmz	GESTITO
WPS	application/vnd.ms-works	GESTITO
WPS.ASICE	application/vnd.ms-works	GESTITO
WPS.ASICS	application/vnd.ms-works	GESTITO
WPS.P7M	application/vnd.ms-works	GESTITO
WPS.P7S	application/vnd.ms-works	GESTITO
XBRL	application/xbrl-instance+xml	GESTITO
XBRL.ASICE	application/xbrl-instance+xml	GESTITO
XBRL.ASICS	application/xbrl-instance+xml	GESTITO
XBRL.P7M	application/xbrl-instance+xml	GESTITO
XBRL.P7S	application/xbrl-instance+xml	GESTITO
XHT	application/xhtml+xml	GESTITO
XHT.ASICE	application/xhtml+xml	GESTITO
XHT.ASICS	application/xhtml+xml	GESTITO
XHT.P7M	application/xhtml+xml	GESTITO
XHT.P7S	application/xhtml+xml	GESTITO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
XHTML	application/xhtml+xml	GESTITO
XHTML.ASICE	application/xhtml+xml	GESTITO
XHTML.ASICS	application/xhtml+xml	GESTITO
XHTML.P7M	application/xhtml+xml	GESTITO
XHTML.P7S	application/xhtml+xml	GESTITO
XLS	application/vnd.ms-excel	GESTITO
XLS.ASICE	application/vnd.ms-excel	GESTITO
XLS.ASICS	application/vnd.ms-excel	GESTITO
XLS.P7M	application/vnd.ms-excel	GESTITO
XLS.P7S	application/vnd.ms-excel	GESTITO
XLSB	application/vnd.ms-excel.sheet.binary.macroenabled.12	GESTITO
XLSB.ASICE	application/vnd.ms-excel.sheet.binary.macroenabled.12	GESTITO
XLSB.ASICS	application/vnd.ms-excel.sheet.binary.macroenabled.12	GESTITO
XLSB.P7M	application/vnd.ms-excel.sheet.binary.macroenabled.12	GESTITO
XLSB.P7S	application/vnd.ms-excel.sheet.binary.macroenabled.12	GESTITO
XLSM	application/vnd.ms-excel.sheet.macroenabled.12	GESTITO
XLSM.ASICE	application/vnd.ms-excel.sheet.macroenabled.12	GESTITO
XLSM.ASICS	application/vnd.ms-excel.sheet.macroenabled.12	GESTITO
XLSM.P7M	application/vnd.ms-excel.sheet.macroenabled.12	GESTITO
XLSM.P7S	application/vnd.ms-excel.sheet.macroenabled.12	GESTITO
XLSX	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	GESTITO
XLSX.ASICE	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	GESTITO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
XLSX.ASICS	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	GESTITO
XLSX.P7M	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	GESTITO
XLSX.P7S	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	GESTITO
XLTX	application/vnd.openxmlformats-officedocument.spreadsheetml.template	GESTITO
XLTX.ASICE	application/vnd.openxmlformats-officedocument.spreadsheetml.template	GESTITO
XLTX.ASICS	application/vnd.openxmlformats-officedocument.spreadsheetml.template	GESTITO
XLTX.P7M	application/vnd.openxmlformats-officedocument.spreadsheetml.template	GESTITO
XLTX.P7S	application/vnd.openxmlformats-officedocument.spreadsheetml.template	GESTITO
XML	application/xml	IDONEO
XML.ASICE	application/xml	IDONEO
XML.ASICS	application/xml	IDONEO
XML.P7M	application/xml	IDONEO
XML.P7S	application/xml	IDONEO
XPS	application/vnd.ms-xpsdocument	GESTITO
XPS.ASICE	application/vnd.ms-xpsdocument	GESTITO
XPS.ASICS	application/vnd.ms-xpsdocument	GESTITO
XPS.P7M	application/vnd.ms-xpsdocument	GESTITO
XPS.P7S	application/vnd.ms-xpsdocument	GESTITO
XSD	application/xml	IDONEO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
XSD.ASICE	application/xml	IDONEO
XSD.ASICS	application/xml	IDONEO
XSD.P7M	application/xml	IDONEO
XSD.P7S	application/xml	IDONEO
XSL	application/xml	IDONEO
XSL-FO	application/xslfo+xml	IDONEO
XSL-FO.ASICE	application/xslfo+xml	IDONEO
XSL-FO.ASICS	application/xslfo+xml	IDONEO
XSL-FO.P7M	application/xslfo+xml	IDONEO
XSL-FO.P7S	application/xslfo+xml	IDONEO
XSL.ASICE	application/xml	IDONEO
XSL.ASICS	application/xml	IDONEO
XSL.P7M	application/xml	IDONEO
XSL.P7S	application/xml	IDONEO
XSLFO	application/xslfo+xml	IDONEO
XSLFO.ASICE	application/xslfo+xml	IDONEO
XSLFO.ASICS	application/xslfo+xml	IDONEO
XSLFO.P7M	application/xslfo+xml	IDONEO
XSLFO.P7S	application/xslfo+xml	IDONEO
XSLT	application/xslt+xml	IDONEO
XSLT.ASICE	application/xslt+xml	IDONEO
XSLT.ASICS	application/xslt+xml	IDONEO
XSLT.P7M	application/xslt+xml	IDONEO
XSLT.P7S	application/xslt+xml	IDONEO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
ZIP	application/zip	IDONEO
ZIP.ASICE	application/zip	IDONEO
ZIP.ASICS	application/zip	IDONEO
ZIP.P7M	application/zip	IDONEO
ZIP.P7S	application/zip	IDONEO

Tabella Formati

Tipi oggetto da trasformare

Per oggetto da trasformare si intende un insieme di uno o più documenti che per ragioni di natura tecnica e organizzativa non è possibile produrre nel formato di SIP standard da trasmettere direttamente al Sistema di conservazione.

In tali casi il processo di conservazione prevede una fase di Preacquisizione che ha in input un oggetto da trasformare dall'Ente e in output uno o più SIP standard da versare a Sacer.

La tabella Tipi oggetto da trasformare elenca i tipi oggetto da trasformare restituendo per ciascuno l'informazione relativa al Versatore dell'oggetto, alla Trasformazione utilizzata e il tipo oggetto contenente i SIP standard da versare a Sacer.

Tipo oggetto da trasformare	Descrizione	Versatore	Trasformazione	Descrizione trasformazione
StrumentoUrbanistico	SIP da trasformare contenente strumento urbanistico - LR24/2017	UCTERREDACQUA_udctd_SU		Trasforma gli strumenti urbanistici versati dagli enti produttori utilizzando l'apposita funzione su PING

Tabella Tipi oggetto da trasformare

Gestione dei SIP rifiutati

Il Sistema registra i SIP il cui versamento è fallito in un'area temporanea del Sistema. Tali SIP sono conservati nel Sistema secondo le seguenti politiche:

- i SIP relativi a versamenti falliti e successivamente andati a buon fine (c.d. errori risolti), sono conservati nel Sistema per un anno dal loro tentato versamento;
- i SIP relativi a versamenti falliti che non saranno più ritentati (c.d. errori non risolubili), sono conservati nel Sistema per un anno dal loro tentato versamento;
- i SIP relativi a versamenti falliti non risolti e non indicati come non risolubili, per i quali è identificata la Struttura versante, la chiave e la tipologia di unità documentaria, sono conservati nel Sistema per un anno dal momento in cui tutte le aggregazioni documentali previste per quella specifica tipologia di unità documentaria per l'anno indicato nella chiave del SIP sono state chiuse e prese in custodia;
- i SIP relativi a versamenti falliti non risolti e non indicati come non risolubili, per i quali non è possibile identificare l'anno e/o la tipologia di unità documentaria e/o la Struttura versante, sono conservati per un anno dal tentato versamento.

Per ulteriori informazioni in merito alle modalità di rifiuto o accettazione dei SIP trasmessi, si rinvia al Manuale, al documento Specifiche tecniche dei servizi di versamento e al documento Codifiche errori in cui sono descritti gli errori restituiti dal Sistema a fronte delle operazioni di versamento, recupero e annullamento effettuate utilizzando i web service.

Generazione delle Serie documentarie

Le unità documentarie acquisite nel Sistema di conservazione sono selezionabili per essere aggregate in Serie di unità documentarie. Il criterio “standard” di generazione delle serie definito da ParER è basato su tre elementi:

- Anno di produzione/repertoriazione dell'unità documentaria;
- Tipologia di unità documentaria;
- Registro

In accordo con l'Ente è prevista la possibilità di configurare criteri specifici per la generazione di serie di unità documentarie che non rientrano nei criteri standard, utilizzando, ad esempio, un metadato specifico o un particolare tipo di documento.

Inoltre, è prevista per l'Ente la possibilità di comunicare la consistenza della serie specificando ad esempio il numero complessivo delle unità documentarie che appartengono alla serie o l'eventuale presenza di lacune. L'Ente può comunicare tali informazioni utilizzando apposite funzionalità del Sistema.

Il processo di generazione della serie si conclude con la sua validazione definitiva da parte del Responsabile della funzione archivistica di conservazione di ParER e la generazione del relativo pacchetto di archiviazione (d'ora in poi AIP) di livello serie.

I tipi serie eventualmente configurati sono indicati nella Tabella Elenco tipi serie.

Modalità di annullamento dei versamenti

Nel caso in cui un versamento andato a buon fine sia stato effettuato per errore o contenga degli errori non correggibili altrimenti, l'Ente provvede ad annullarlo utilizzando apposite funzionalità del Sistema oppure inviando al personale di ParER una richiesta formale completa degli estremi dei documenti da annullare e relativa motivazione.

Gli oggetti non sono cancellati dal Sistema ma marcati come Annullati e sono comunque sempre consultabili tramite l'apposita sezione di ricerca.

Modalità di restituzione degli oggetti versati in conservazione in caso di recesso

ParER garantisce il mantenimento nel proprio Sistema dei Documenti informatici e delle Aggregazioni documentali informatiche conservati, con i metadati a essi associati e le evidenze informatiche generate nel corso del processo di conservazione fino alla comunicazione da parte dell'Ente dell'effettiva messa a disposizione del Sistema in cui effettuare il riversamento.

ParER provvederà all'eliminazione dal proprio Sistema di tutti gli oggetti riversati e di tutti gli elementi riferiti all'Ente solo al termine del riversamento e solo dopo le opportune verifiche - effettuate da entrambe le Parti e svolte di concerto tra le stesse - di corretto svolgimento del riversamento stesso. In tal caso viene garantita la completa cancellazione e non leggibilità dei dati. L'intera operazione dovrà comunque avvenire con l'autorizzazione e la vigilanza delle competenti autorità, in particolare delle strutture del MIBACT.

In caso di chiusura del servizio da parte della Regione Emilia-Romagna, con interventi di modifica alla normativa regionale, si provvederà a trasferire quanto conservato al Sistema individuato per proseguire le attività. Per quanto riguarda gli aspetti operativi per il trasferimento di archivi ad altri sistemi di conservazione, ParER adotta lo standard Uni Sincro, e provvederà a trasferire secondo canali sicuri concordati con l'Ente o con il nuovo Conservatore le informazioni. Analogamente il Sistema è predisposto per la ricezione di archivi in formato Uni Sincro; qualora il precedente sistema di conservazione non sia in grado di produrre l'archivio in formato Uni Sincro, ParER, a seguito di specifici accordi, può mettere a disposizione dell'Ente consulenza e strumenti per facilitare il trasferimento dell'archivio.



S.I.A.T. – Servizi Informatici Associati Terred'Acqua

Piano della Sicurezza Informatica
*(art. 4, c. 3, lett. C, DPCM 03 dicembre
2013
Art.12, DPCM 13 novembre 2014)*



Sommario

1.	Struttura del sistema e protezioni.....	3
1.1.	Architettura della rete.....	3
1.2.	Sicurezza della rete.....	3
1.3.	Architettura del Sistema Informatico.....	3
1.1.1.	Banche dati.....	3
1.1.2.	Posta elettronica.....	4
1.1.3.	Sistema di autenticazione.....	4
1.4.	Sicurezza dei dati.....	4
1.1.4.	Banche dati centralizzate.....	5
1.1.5.	Archivi documentali centralizzati.....	5
1.1.6.	Banche dati ed archivi documentali residenti su P.C.....	5
1.5.	Aggiornamenti del software.....	5
2.	Modalità di gestione delle credenziali di autenticazione e delle autorizzazioni...	5
2.1.	Incaricati del trattamento informatico.....	5
2.2.	Soggetto preposto alla custodia delle credenziali, alla loro attribuzione, cancellazione, modifica.....	6
2.3.	Assegnazione delle credenziali di autenticazione.....	6
2.4.	Modalità di gestione delle password.....	7
2.5.	Considerazioni generali sulle password.....	7
1.1.7.	Sicurezza e limiti nell'uso delle password.....	7
1.1.8.	Durata e cambio delle password.....	8
1.1.9.	Requisiti delle password.....	8
2.6.	Disattivazione credenziali per disuso.....	8
3.	Modalità di gestione delle stazioni di lavoro.....	8
3.1.	Soggetto preposto alla pulizia o recupero delle banche dati su PC.....	8
3.2.	Programmi antivirus.....	9
3.3.	Programmi antispyware.....	9
3.4.	Interventi di manutenzione.....	9
3.5.	Società esterne o professionisti per la manutenzione e l'assistenza.....	10
4.	Salvataggio dei dati.....	10
5.	Locali.....	10
6.	Cautele generali.....	11
6.1.	Password.....	11
6.2.	Uso del computer.....	11
6.3.	Custodia dei supporti.....	11
6.4.	Supporti ricevuti dall'esterno.....	11
7.	Divieti.....	11



1. **Struttura del sistema e protezioni**

1.1 **Architettura della rete**

Presso ogni comune dell'Unione c'è un nodo principale di Lepida denominato PAL (Punto Accesso Lepida). Questi nodi sono collegati al nodo centrale di Persiceto con VPN configurando così una architettura a stella.

La rete Lepida è in fibra ottica Gbit.

Tutte le Sedi comunali sono collegate alla rete aziendale.

Tutti i dipendenti dotati di postazione di PC possono quindi collegarsi alla rete dati ed accedere ad internet. L'accesso ai dati è centralizzato in cloud Lepida, così come l'accesso ad internet, anche se ogni comune possiede indirizzi IP pubblici diversi. La navigazione e l'accesso ai servizi dall'esterno sono protetti da firewall.

1.2 **Sicurezza della rete**

Tendenzialmente e preferibilmente tutte le sedi sono connesse alle sedi comunali dotate di PAL Lepida mediante LAN o MAN (Metropolitan Area Network).

Ove non possibile si è proceduto alla connessione via VPN attestata su apposito firewall collegato alla linea tradizionale (dove possibile mediante fibra ottica).

L'accesso alla rete comunale è comunque permesso solo tramite autenticazione con nome utente e password. Tutti i sistemi elencati afferiscono a un sistema Firewall, che controlla il traffico dati in base a politiche di sicurezza prestabilite.

1.3 **Architettura del Sistema Informatico**

1.1.1. Banche dati

I dati strutturati delle applicazioni gestionali possono essere memorizzati in:

- Banche dati centralizzate, per le applicazioni utilizzate da più utenti;
- Più raramente, su stazioni di lavoro per applicazioni mono-utente o qualora il software non renda possibile l'installazione sul server

Le banche dati degli applicativi gestionali ed ulteriori banche dati, nonché archivi documentali non strutturati sono conservati in:

- server e sistemi di memorizzazione centralizzati presso il Datacenter dell'Unione in Lepida (DB server e file server);
- server e/o sistemi di memorizzazione ubicati presso Datacenter esterni (es. Lepida, ParER, ecc.);
- Personal Computer distribuiti negli uffici degli Enti.

Può quindi accadere che alcune banche dati risiedano esclusivamente sul personal computer dell'utente che le utilizza; ciò può accadere sia per scelta personale (fortemente sconsigliata) del singolo utente che volontariamente le mantiene solo sulla



S.I.A.T. – Servizi Informatici Associati Terred'Acqua

propria postazione, sia per le caratteristiche intrinseche del programma utilizzato. L'utente finale diventa quindi il responsabile unico dei documenti e della banche dati non salvate sul server di rete (e quindi non ricomprese nel sistema centralizzato di backup schedulati). Gli addetti ai S.I. hanno sensibilizzato ed informato gli assegnatari dei P.C. su questa problematica.

1.1.2. Posta elettronica

La posta elettronica viene gestita esternamente; ai dipendenti o amministratori è assegnata una casella individuale nella forma nome.cognome@. Esistono caselle non nominali corrispondenti a gruppi di lavoro o figure istituzionali ma per le quali è definito un responsabile della casella stessa.

1.1.3. Sistema di autenticazione

Il principale sistema di autenticazione è Microsoft Windows Active Directory, che viene utilizzato per autenticare gli utenti di risorse condivise sulla rete quali:

- Cartelle
- Stampanti
- Accesso agli applicativi

Alcune procedure applicative sono integrate con Active Directory di Windows e quindi le credenziali di accesso a queste procedure sono le stesse dell'accesso alla rete e ai PC. Altre procedure applicative, invece, non utilizzano questo sistema centralizzato, ma possiedono un proprio sistema di autenticazione.

Per l'accesso ai personal computer ci si avvale esclusivamente delle credenziali di Active Directory.

Solo per manutenzione, gli amministratori o incaricati esterni (ditte esterne) possiedono delle apposite credenziali locali della postazione di lavoro stessa.

1.4 **Sicurezza dei dati**

1.1.4 Banche dati centralizzate

L'accesso ai dati avviene tramite le procedure gestioni che li trattano: all'utente viene richiesta la digitazione di username e password. Queste credenziali sono verificate dall'Archive Directory per le procedure già integrate, oppure dalla procedura stessa.

Contestualmente viene verificato se l'utente è autorizzato all'utilizzo della funzionalità richiesta, cioè l'utente può essere abilitato solo ad alcuni moduli o funzionalità del programma applicativo.

Il sistema di autorizzazione è sempre gestito dalla procedura informatica.

La gestione del rilascio delle credenziali di Active directory complete al servizio informativo Associato (SIAT).



Il rilascio e gestione delle credenziali o delle funzionalità utente all'interno del programma applicativo compete agli Uffici Responsabili dell'Unione e dei singoli Comuni, che agiscono nel rispetto di quanto previsto dal "Codice in materia di protezione dei dati personali", allegato B "Disciplinare Tecnico in materia di misure minime di sicurezza", in particolare dei Punti 13 e 14, che vengono riportati di seguito:

"13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione."

1.1.5 Archivi documentali centralizzati

I server contenenti archivi documentali richiedono l'autenticazione e l'autorizzazione dell'utente tramite il dominio Active Directory.

Questa autenticazione avviene in modo trasparente per l'utente (senza la richiesta di ulteriori autenticazioni) se le credenziali di accesso al PC sono le stesse che nel dominio Active Directory

1.1.6 Banche dati ed archivi documentali residenti su P.C.

I PC che contengono banche dati locali o archivi documentali, contenenti dati personali e/o sensibili sono protetti da credenziali di accesso personali di Active Directory (oltre alle password di amministratore locale del PC utilizzata solo dal SIAT per interventi tecnici).

1.5 **Aggiornamenti del software**

I programmi per elaboratore (inclusi i sistemi operativi) vengono tempestivamente aggiornati mediante l'installazione delle nuove versioni degli stessi o delle patches rilasciate dai produttori al fine di prevenire la vulnerabilità e correggerne i difetti.

La frequenza di aggiornamento non può essere superiore ai 6 mesi.

2. **Modalità di gestione delle credenziali di autenticazione e delle autorizzazioni**

2.1 **Incaricati del trattamento informatico**

Sono tutti gli operatori tecnici del servizio SIAT

2.2 **Soggetto preposto alla custodia delle credenziali, alla loro attribuzione, cancellazione, modifica**

Il preposto alla gestione delle credenziali provvede a creare un account con password provvisoria da modificarsi obbligatoriamente al primo accesso.



2.3 **Assegnazione delle credenziali di autenticazione**

Le credenziali di autenticazione consistono in un codice per l'autenticazione dell'incaricato (user-id tipicamente terredacqua\nome.cognome) associato ad una parola chiave riservata (password).

Le credenziali di accesso al sistema e la relativa casella email vengono create dal SIAT a seguito di una richiesta, di norma inoltrata mediante l'apposita procedura informatica, in cui il Dirigente/Responsabile del Settore/Ufficio competente (o suo delegato alla gestione).

Nella richiesta vengono altresì esplicitate le abilitazioni che lo stesso dovrà avere relativamente al sistema gestito tramite Active Directory (cartelle condivise, applicativi e banche dati locali).

L'invio della richiesta al SIAT presuppone che il Dirigente/Responsabile che la inoltra attesti che l'utente abbia titolo ad accedere alla rete e ai dati a cui viene abilitato.

L'incaricato del SIAT crea le relative credenziali Active Directory ed email e comunica, in modo riservato, le password temporanee all'utente, che le dovrà sostituire al primo accesso con quelle definitive.

Può accadere che, per esigenze di servizio, esistano credenziali d'accesso non legate ad un singolo lavoratore e che possono essere condivise da tutto un gruppo di operatori. Queste credenziali non possono consentire l'accesso a banche dati o documenti contenenti dati personali e verranno assegnate unicamente a dipendenti del Comune individuati quali responsabili della gestione delle password.

2.4 **Modalità di gestione delle password**

Nel caso un utente abbia dimenticato una password, si dovrà rivolgere al SIAT che, previo riconoscimento, provvederà a resettarla e a comunicarla riservatamente all'utente, che, al primo accesso, dovrà necessariamente modificarla con una nuova di sua scelta.

Eccezionalmente, nel caso in cui si renda indispensabile ed indifferibile, per esclusive necessità tecniche di operatività e sicurezza, i tecnici SIAT preposti alla gestione delle credenziali potranno modificare la password degli utenti; in questi casi, giustificandone le ragioni, ne daranno tempestiva comunicazione scritta agli stessi, che quindi provvederanno a sostituirla obbligatoriamente al primo accesso.

Ai sensi di quanto previsto dal punto 10 dell'Allegato B al D. Lgs. 30 giugno 2003, n. 196, gli addetti del SIAT potranno modificare la password degli utenti e comunicare tale nuova password ad un altro utente.

Tale eventualità potrà verificarsi dietro richiesta scritta proveniente dal Responsabile apicale dell'Ufficio/Servizio qualora, in caso di prolungata assenza o impedimento dell'incaricato, sia indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. Qualora si tratti delle password di un Responsabile apicale di un comune o dell'Unione, la richiesta dovrà pervenire, rispettivamente, dal Sindaco o dal Presidente dell'Unione.



La richiesta dovrà contenere il nome dell'utente di cui va modificata la password, le ragioni che ne rendono indispensabile e indifferibile la modifica, e il nome dell'utente a cui la nuova password dovrà essere comunicata.

Il SIAT comunicherà tempestivamente per iscritto all'utente dell'avvenuto cambio password e delle ragioni che lo hanno reso necessario, nonché il nominativo dell'utente a cui la nuova password è stata comunicata.

L'utente dovrà quindi procedere, appena possibile, a modificare la sua password.

2.5 Considerazioni generali sulle password

1.1.7 Sicurezza e limiti nell'uso delle password

L'utilizzatore ha l'obbligo di impostare la password seguendo la procedura di cambio password nel rispetto della normativa vigente.

Ogni incaricato che riceve le proprie password ne è direttamente responsabile e non deve in alcun modo comunicare le proprie password a persone diverse od altri incaricati.

Le password sono strettamente personali e non vanno comunicate a nessuno.

Non è tecnicamente possibile ricostruire le password impostate dagli utenti.

Architetture in cui gli utenti non eseguano una validazione (logon) ad un dominio e non implementano complete funzionalità di sicurezza non sono e non dovranno essere più presenti all'interno della rete aziendale.

1.1.8 Durata e cambio delle password

Ogni utente autorizzato ad accedere alle banche dati ha ottenuto dagli addetti del SIAT un codice identificativo (USER-NAME) ed una parola segreta (PASSWORD) che deve immediatamente cambiare.

La durata delle password viene definita a livello centrale; il sistema avviserà l'utente quando la password sta per scadere ed è quindi necessario cambiarla. Alla password di accesso al dominio Windows è dato un periodo di vita massimo di 90 giorni. Trascorso tale periodo se l'utente non l'ha già autonomamente cambiata, il sistema lo costringe ad immetterne una nuova altrimenti il sistema non si attiva.

Per impostare la nuova password è necessario fornire anche quella vecchia; nel caso in cui l'utente l'avesse dimenticata, l'amministratore di sistema, dopo aver riconosciuto l'utente, può forzare la creazione di una nuova password provvisoria.

Un utente che non sia stato disabilitato può modificare la propria password anche prima della scadenza autenticandosi con userid e vecchia password (valida per questa funzione anche se scaduta).

Gli utenti possono modificare la propria password in qualsiasi momento, oppure essere chiamati a cambiarla dal sistema stesso, in risposta a policy aziendali o interventi amministrativi.

Gli utenti sono tenuti a cambiare la password anche nel caso abbiano il sospetto che la stessa non sia più segreta.



1.1.9 Requisiti delle password

Gli utenti sono stati sensibilizzati, informati ed istruiti sull'importanza dell'uso, della segretezza e sulle modalità di modifica delle password.

Le password devono essere significative e conformi ai requisiti di complessità, ovvero:

- devono essere lunghe almeno 8 caratteri
- devono essere "complesse", cioè contenere almeno 3 delle 4 seguenti tipologie: maiuscole, minuscole, numeri, caratteri speciali
- si deve evitare di immettere sequenze della stessa lettera
- deve presentare differenze significative rispetto alle password per cui non devono ricordare quelle precedenti (es. con una modifica di un solo carattere)
- non deve contenere il nome, il cognome o l'user-name (account utente)
- non deve trattarsi di una parola o di un nome comune

2.6 **Disattivazione credenziali per disuso**

Nel momento in cui un utente perde il diritto ad accedere alla rete aziendale, il dirigente referente o l'ufficio personale ne comunicano tempestivamente la data di perdita dei requisiti.

Almeno semestralmente viene fatta una verifica straordinaria del permanere, in capo agli utenti abilitati, dei requisiti necessari all'abilitazione onde evidenziare eventuali eventi di cessazione non comunicati.

Il mancato uso delle credenziali per almeno sei mesi continuativi determina la loro disattivazione salvo quelle preventivamente autorizzate per i soli scopi di gestione tecnica.

Per riattivare le credenziali, l'utente dovrà rivolgersi al servizio SIAT che, verificatone il diritto, lo riattiverà con le stesse modalità del caso di "dimenticanza di password".

Periodicamente il SIAT controllerà e disattiverà gli account non utilizzati nei sei mesi precedenti.

Il codice di identificazione, laddove inutilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

3. **Modalità di gestione delle stazioni di lavoro**

3.1 **Soggetto preposto alla pulizia o recupero delle banche dati su PC**

Preposto alla pulizia o recupero delle banche dati su PC è il Responsabile del SIAT che provvederà attraverso il personale del servizio.

3.2 **Programmi antivirus**

Un software antivirus è installato su tutti i PC e server windows.



S.I.A.T. – Servizi Informatici Associati Terred'Acqua

Il software antivirus viene aggiornato in maniera automatica ogni qualvolta la casa produttrice rilascia un aggiornamento riguardante la definizione dei virus o l'aggiornamento del software.

Il software produce report dettagliati sulla natura del Client in rete LAN (utente collegato, Sistema Operativo e stato dell'aggiornamento) e sul loro stato di infezione.

Gli utilizzatori di strumenti informatici sono stati informati sul pericolo che i "virus informatici" attacchino i personal computer e ne danneggino il contenuto oltre a propagarsi su altri computer o sui server di rete. Tutti sono tenuti ad utilizzare i programmi di antivirus presenti nell'ente per verificare che i supporti ottenuti dall'esterno, i files ricevuti via e-mail o scaricati da internet, non siano infetti.

Gli utenti non possono disattivare la procedura di aggiornamento automatico, e non possono disattivare (anche temporaneamente) la funzione di protezione antivirus.

3.3 Programmi antispam

La protezione da Spam, è ottenuta tramite un fornitore esterno che ha la gestione dell'intero sistema di posta elettronica.

Tipicamente le e-mail contenenti virus vengono già eliminate da questo antispam; qualora superassero l'antispam, le e-mail vengono anche sottoposte dal sistema del fornitore ad ulteriore controllo antivirus.

In definitiva una e-mail è soggetta a un sistema antispam e due sistemi antivirus, uno del sistema centralizzato di posta ed uno del pc locale.

3.4 Interventi di Manutenzione

Gli interventi di manutenzione sui PC degli utenti vengono di norma effettuati, in remoto o in loco, alla presenza degli assegnatari dei PC stessi.

L'accesso remoto ai PC degli utenti avviene previo consenso espresso da questi ultimi alla richiesta di accesso remoto presentata dal software di controllo.

Nel caso sia necessario inserire la password dell'utente, verrà chiesto a quest'ultimo di digitarla e non dovrà quindi essere comunicata al tecnico.

I tecnici del SIAT o di ditte esterne incaricate della manutenzione dispongono di una password di amministratore del PC che consente l'accesso senza la necessità di conoscere la password dell'utente.

Nel caso il PC debba essere trasferito presso un laboratorio per la sua riparazione, i tecnici incaricati dovranno limitarsi alle sole operazioni tecniche necessarie alla rimozione del guasto e non dovranno accedere in modo generalizzato ai file memorizzati nel disco del PC stesso.

3.5 Società esterne o professionisti per la manutenzione e l'assistenza

Il Responsabile del SIAT nomina la società che effettua la manutenzione dei sistemi hardware o software responsabile del trattamento dei dati utilizzando l'apposito modello



il quale andrà integrato con una specifica assunzione di impegno da parte del responsabile stesso al rispetto delle seguenti disposizioni:

- non effettuare copie né procedure alla eliminazione degli archivi informatici di titolarità dell'ente detenuti
- informare preventivamente gli interessati del giorno e dell'orario in cui saranno effettuati gli interventi tecnici
- richiedere preventivamente l'autorizzazione ai tecnici del SIAT nel caso di interventi di assistenza tramite collegamento remoto. Gli stessi tecnici dovranno essere avvisati al termine delle operazioni
- usare riservatezza su dati ed informazioni addivenuti in loro possesso
- trasmettere al Responsabile del SIAT l'elenco degli incaricati al trattamento e successive variazioni
- trasmettere al Responsabile del SIAT il nominativo degli amministratori di sistema affinché si possa provvedere al loro incarico

3.6 **Dismissione delle postazioni di lavoro**

In caso di dismissioni di PC, il SIAT comunica al Responsabile apicale del Servizio l'elenco dei PC da dismettere: questi segnala l'eventuale presenza, su dischi locali degli stessi, di banche dati da recuperare.

Il soggetto preposto, una volta recuperate le banche dati, disinstalla i dischi magnetici dalla postazione di lavoro. La postazione potrà essere smaltita mentre i dischi fissi dovranno essere resi illeggibili prima della rottamazione.

I dischi dei PC usati che eventualmente il Comune dovesse cedere in comodato d'uso, prima della consegna vengono riformattati con modalità sicure, impedendo il recupero di banche dati che vi erano contenute.

4. **Salvataggio dei dati**

Il salvataggio delle banche dati esistenti sul server è in carico all'Ufficio SIAT.

Sui sistemi centralizzati vengono fatte copie quotidiane degli archivi documentali e delle banche dati strutturate allo scopo di fornire almeno una versione aggiornata alla notte precedente.

L'esecuzione dell'operazione di salvataggio è verificata quotidianamente dagli operatori.

In caso di danneggiamento o perdita di dati, gli stessi vengono tempestivamente ripristinati mediante le copie presenti nel sistema di backup.

Ogni singolo lavoratore è invece responsabile dell'effettuazione di copie di sicurezza degli archivi e dei documenti memorizzati unicamente sul proprio PC.

5. **Locali**

Presso ogni comune è presente un CED ubicato in locali chiusi a chiave. Le chiavi di accesso a questi locali sono in carico al comune stesso, che forniscono al SIAT copia delle stesse.



6. Cautele generali

6.1 Password

Il sistema centralizzato di autenticazione provvede in modo automatico alla scadenza della password.

Nel caso in cui le password siano impostate dall'utente in sistemi che non ne prevedano la scadenza temporale, è sua responsabilità provvedere alla loro modifica almeno ogni 90 giorni.

Le password esterne al sistema Active Directory devono rispettare i limiti, la sicurezza e la durata di quelle precedentemente indicate nella sezione "Modalità di gestione delle Password".

6.2 Uso del computer

Il PC non deve essere lasciato incustodito.

In caso di allontanamento anche temporaneo, l'utente attivo al momento deve essere disconnesso o deve essere attivata la modalità salvaschermo con protezioni mediante password.

Il dirigente di Settore/Responsabile delegato può impartire ulteriori istruzioni per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di lavoro. E' impostata a livello centrale, una policy di sicurezza distribuita su tutte le postazioni informatiche che blocca il PC in casi di inattività per 30 minuti. Il nuovo accesso sarà consentito solo con password di Active Directory.

6.3 Custodia dei supporti

Per motivi di sicurezza e al fine di evitare accessi non autorizzati e trattamenti non consentiti, devono essere impartite, da parte del Responsabile apicale del Settore, le istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili (es. CD, DVD, Pendrive) su cui sono memorizzati i dati.

6.4 Supporti ricevuti dall'esterno

Nel caso di supporti ricevuti dall'esterno, come nel caso di allegati ricevuti via e-mail, l'utente deve prestare massima attenzione e sottoporre il supporto a controllo antivirus.

7. Divieti

Divieti per l'utente	Chi può fare questa operazione	Operazioni preliminari	Conseguenze	Responsabile nel caso di non rispetto del divieto
Vietato installare programmi	Addetti ai S.I.	- sensibilizzazione e formazione sui rischi e responsabilità	- disinstallazione programma - eliminazione	Consegnatario del computer



S.I.A.T. – Servizi Informatici Associati Terred'Acqua

		<ul style="list-style-type: none"> - verifica compatibilità con i sistemi - verifica esistenza di virus informatici - verifica della regolare licenza d'uso 	<ul style="list-style-type: none"> virus. Ripristino situazione originale - segnalazione al direttore di area 	
Vietato disinstallare programmi	Addetti ai S.I.	<ul style="list-style-type: none"> - sensibilizzazione e formazione sui rischi e responsabilità 	<ul style="list-style-type: none"> - Ripristino situazione originale - segnalazione al direttore di area 	Consegnatario del computer
Vietato utilizzare (anche senza installazione) di programmi non autorizzati dal S.I.	Addetti ai S.I.	<ul style="list-style-type: none"> - sensibilizzazione e formazione sui rischi e responsabilità - verifica compatibilità con i sistemi - verifica esistenza di virus informatici - verifica della regolare licenza d'uso 	<ul style="list-style-type: none"> - Eliminazione programma non regolare senza preavviso - Eliminazione virus - Ripristino situazione originale - Segnalazione e al direttore di area 	Consegnatario del computer
Vietato utilizzare programmi di intercettazione e dati diretti ad altri utenti	Addetti ai S.I.	<ul style="list-style-type: none"> - sensibilizzazione e formazione sui rischi e responsabilità 	<ul style="list-style-type: none"> - Eliminazione del programma - Ripristino situazione originale - Segnalazione e al direttore di area 	Consegnatario del computer
Vietato modificare o tentare di modificare la configurazione	Addetti ai S.I.	<ul style="list-style-type: none"> - sensibilizzazione e formazione sui rischi e responsabilità - verifica compatibilità con i sistemi 	<ul style="list-style-type: none"> - Ripristino situazione originale - Segnalazione e al direttore di area 	Consegnatario del computer



S.I.A.T. – Servizi Informatici Associati Terred'Acqua

Il SIAT, in conformità alle disposizioni di legge, provvede alla descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento nell'ambito del piano di disaster recovery.

Il Responsabile apicale del SIAT provvede con propria determinazione a redigere l'elenco degli amministratori di sistema e a designarli individualmente con successivo atto precisandone le funzioni e specificandone l'ambito di attività.

Gli estremi identificativi delle persone fisiche designate, con l'indicazione delle funzioni ad esse attribuite, è riportato in un elenco agli atti del SIAT stesso. Con cadenza annuale il Responsabile del SIAT verifica l'operato degli amministratori di sistema in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle normative vigenti.

Il SIAT ha adottato le misure necessarie a consentire un'attività di verifica dell'operato degli amministratori di sistema alla luce delle normative vigenti in merito al trattamento dei dati personali.



UNIONE TERRED'ACQUA

Costituita fra i Comuni di:

Anzola dell'Emilia
Calderara di Reno
Crevalcore
Sala Bolognese
San Giovanni in Persiceto
Sant'Agata Bolognese

DELIBERA DELLA GIUNTA DELL'UNIONE N. 30 del 30/06/2025

OGGETTO:

APPROVAZIONE DEL MANUALE DI GESTIONE DEL PROTOCOLLO, DEI FLUSSI DOCUMENTALI E DELL'ARCHIVIO.

Letto, approvato e sottoscritto.

FIRMATO
IL PRESIDENTE
Marco MARTELLI

FIRMATO
IL SEGRETARIO DELL'UNIONE
Luca LAURENZANO

Documento prodotto in originale informatico e firmato digitalmente ai sensi dell'art. 20 del "Codice dell'amministrazione digitale" (D.Leg.vo 82/2005).