

Manuale di gestione documentale Anno 2022

(3° revisione - anno 2022 in conformità alle linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici)

Aggiornato con Deliberazione n. del

Aggiornato con Deliberazione di Giunta Comunale n. 210 del 18/12/2008: Manuale di Gestione

Adottati con delibera di Giunta Comunale n. 217 del 20/12/2007:

il nuovo Titolario per la riorganizzazione dell'archivio del Comune di Vigevano, il Piano di conservazione dei documenti informatici, la modalità di gestione del protocollo di emergenza, le Linee guida per le pubblicazioni all'Albo Pretorio e le Linee guida per l'inserimento ed aggiornamento dei dati nel protocollo informatico

Adottato con Deliberazione di G.C. 239 del 21.12.2006:

Manuale di Gestione con allegati - Elenco documenti soggetti a registrazione particolare, Titolario di classificazione, Piano di selezione conservazione e scarto, Massimario della documentazione da archiviare, Massimario della documentazione da scartare, Piano di Sicurezza informatica

Introduzione.....	5
Capitolo 1 - Disposizioni generali.....	6
1.1 Ambito di applicazione.....	6
1.2 Definizioni dei termini.....	6
1.3 Area Organizzativa Omogenea - AOO.....	6
1.4 Casella di posta elettronica certificata.....	6
1.5 Servizio ICT, Protocollo e Gestione Documentale e - Gestione Archivio e archivio storico....	6
1.6 Responsabile del Protocollo e della gestione documentale e Responsabili della conservazione.....	7
1.7 Protocollo Informatico.....	8
1.7.1 Componenti e funzionalità.....	8
1.7.2 Accesso alle funzionalità del Protocollo Informatico.....	9
1.7.3 Unicità del Protocollo Informatico.....	10
1.8 Registro giornaliero di protocollo.....	10
Capitolo 2 – Gestione dei documenti.....	11
2.1 Modello operativo adottato per la gestione dei documenti.....	11
2.2 Modalità di formazione dei documenti.....	12
2.3 Sottoscrizione dei documenti informatici.....	13
Capitolo 3 - Ricezione dei documenti.....	13
3.1 Ricezione dei documenti su supporto cartaceo.....	13
3.2 Ricezione dei documenti informatici.....	13
3.3 Rilascio di ricevute attestanti la ricezione dei documenti.....	14
3.4 Documenti trasmessi tra Pubbliche Amministrazioni.....	14
3.5 Protocollo automatico dei documenti.....	14
Capitolo 4 - Registrazione dei documenti.....	15
4.1 Documenti soggetti a registrazione di protocollo.....	15
4.2 Registrazione di protocollo dei documenti ricevuti e spediti.....	15
4.3 Segnatura di Protocollo.....	16
4.4 Annullamento dei protocolli.....	17
4.5 Registro giornaliero e annuale di protocollo.....	17
4.6 Registro di emergenza.....	17
4.8 Documentazione particolare.....	18
4.8.1 Deliberazioni di Giunta e Consiglio, determinazioni organizzative, ordinanze, disposizioni dirigenziali, determinazioni dirigenziali e di posizione organizzativa.....	18
4.8.2 Documenti inerenti a gare d'appalto.....	18

4.8.3 Posta personale.....	19
4.8.4 Lettere anonime e documenti non firmati.....	19
4.8.5 Documenti inviati via fax.....	19
4.8.6 Documenti di competenza di altre amministrazioni.....	19
4.8.7 Corrispondenza degli irreperibili o senza fissa dimora.....	19
4.8.9 Richieste di autocertificazioni e/o dichiarazioni sostitutive ed in genere scritti avulsi da qualsiasi procedimento amministrativo dell'Ente.....	20
Capitolo 5 – Smistamento, assegnazione, presa in carico.....	20
5.1. Assegnazione dei documenti.....	20
5.2. Modifica delle assegnazioni.....	20
5.3 Presa in carico automatizzata.....	20
5.4 Assegnazione alla Segreteria Generale di atti non smistabili.....	21
Capitolo 6 - CLASSIFICAZIONE DEI DOCUMENTI.....	21
6.1 Classificazione dei documenti.....	21
6.2 Creazione e identificazione dei fascicoli.....	21
6.3 Modifica delle assegnazioni dei fascicoli.....	22
6.4 Fascicolo ibrido.....	22
6.2 Piano di conservazione dell'archivio.....	22
Capitolo 7 – Spedizione.....	22
7.1 Spedizione documentazione analogica.....	22
7.2 Spedizione dei documenti informatici.....	23
7.3 Corrispondenza con più destinatari e copie per conoscenza.....	23
7.4 Allegati.....	23
7.5 Invio di documenti tra uffici dell'Ente - Protocollo interno.....	24
Capitolo 8 – Archiviazione dei documenti.....	24
8.1 Archiviazione dei documenti e dei fascicoli cartacei.....	24
8.2 Archiviazione dei documenti e dei fascicoli informatici.....	24
8.3 Formati accettati.....	25
I formati accettati idonei alla conservazione sono specificati nell' <i>Allegato 10 – Formati accettati</i>	25
8.4 Sistema informatico.....	25
Allegati.....	26
Allegato 1 - Glossario dei Termini.....	26
Allegato 2 - Funzionigramma.....	26
Allegato 3 - Nomine.....	26
Allegato 4 - Documenti non soggetti a protocollazione - Registrazioni particolari.....	26
Allegato 5 - Piano di classificazione dell'Ente.....	26

Allegato 6 - Regolamento dell'accesso civico e dell'accesso agli atti (approvato con deliberazione di Consiglio Comunale n. 69 del 11/10/2019).....	26
Allegato 7- Procedura per l'attivazione del Registro di Emergenza.....	26
Allegato 8 - Piano di selezione, conservazione e scarto.....	26
Allegato 9 - PARER – ManualeConservazione_ver2021fin.....	26
Allegato 10 - Formati accettati.....	26
Allegato 11 – Piano della sicurezza.....	26

INTRODUZIONE

Al Comune di Vigevano, fino al 1976, l'ufficio Protocollo e Archivio inserito nel Settore Affari Generali si occupava della registrazione dei documenti e della gestione degli archivi, sia di deposito che storico. Con delibere di Consiglio Comunale n.329/1976 e n.98/1977 le competenze sono state suddivise, in quanto è stata istituita una sezione separata d'archivio, denominata "Archivio Storico" inserita nel Settore Culturale, con il compito della gestione e valorizzazione della parte storica dell'archivio comunale. Nel 1992 l'Archivio Storico Comunale ha ottenuto dal Ministero per i Beni Culturali e Ambientali la "dichiarazione di particolare importanza" ai sensi dell'art.31 del DPR 1409/1963.

Per quanto riguarda il Protocollo, dal mese di luglio 1999 si è iniziato a utilizzare la procedura informatica per la registrazione della corrispondenza.

Il Protocollo Generale del Comune di Vigevano è attualmente unico e centralizzato, anche se dal novembre 2003 è organizzato in "sedi distinte", grazie al programma informatico di registrazione che permette ad operatori remoti di lavorare in rete.

La sede principale del Protocollo si occupa della ricezione e smistamento della posta ricevuta tramite ufficio postale, della registrazione della posta non trattata dai "punti protocollo" e della spedizione di tutta la corrispondenza cartacea.

Con delibera di Giunta Comunale n. 165 del 29 luglio 2004 è stata istituita, a norma del DPR 445/2000, una sola area organizzativa omogenea denominata Comune di Vigevano composta dall'insieme di tutte le sue unità.

Ai sensi dell'articolo 61, comma 1, del DPR 445/2000 è stato istituito, con delibera di Giunta Comunale n. 230 del 22.12.2005, il Servizio archivistico per la gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi corrente e di deposito, individuato nell'Unità operativa complessa Protocollo e Archivio moderno.

In seguito con deliberazione di G.C. 239 del 21.12.2006 è stato adottato il Manuale di Gestione del protocollo informatico, dei flussi documentali e degli archivi ed i suoi allegati: Elenco documenti soggetti a registrazione particolare, Titolario di classificazione, Piano di selezione conservazione e scarto, Massimario della documentazione da archiviare, Massimario della documentazione da scartare, Piano di Sicurezza informatica.

Con delibera di Giunta Comunale n. 217 del 20/12/2007 è stato adottato il nuovo Titolario per la riorganizzazione dell'archivio del Comune di Vigevano e sono stati approvati: il Piano di conservazione dei documenti informatici, la modalità di gestione del protocollo di emergenza, le Linee guida per le pubblicazioni all'Albo Pretorio e le Linee guida per l'inserimento ed aggiornamento dei dati nel protocollo informatico.

Con Deliberazione di Giunta Comunale n. 210 del 18/12/2008 è stata approvata la Modifica del Manuale di gestione del Protocollo informatico a sostituzione di quello adottato con deliberazione di G.C. 239 del 21.12.2006.

CAPITOLO 1 - DISPOSIZIONI GENERALI

1.1 Ambito di applicazione

Il presente manuale è stato aggiornato in base alle nuove “Linee Guida sulla formazione, gestione e conservazione dei documenti informatici” emanate da AGID entrate in vigore il 10 settembre 2020 ed attuate il 7 giugno 2021, nonché ai sensi degli articoli 3 e 5 del DPCM 31 dicembre 2013 per la gestione delle attività di formazione, registrazione, classificazione, fascicolazione e conservazione dei documenti, oltre che la gestione dei flussi documentali e dei procedimenti dell’Amministrazione e degli archivi del Comune di Vigevano.

1.2 Definizioni dei termini

Per quanto riguarda la definizione dei termini, che costituisce la corretta interpretazione del dettato del presente manuale, si rimanda al glossario allegato (*Allegato 1 - Glossario*).

1.3 Area Organizzativa Omogenea - AOO

Ai fini della gestione dei documenti è individuata, con delibera di Giunta Comunale n. 165 del 29 luglio 2004, una sola area organizzativa omogenea denominata Comune di Vigevano (di seguito Comune) composta dall’insieme di tutte le sue unità organizzative individuate nell’atto di organizzazione delle aree e degli uffici dell’Amministrazione “*Allegato 2 – Funzionigramma*”.

Il codice identificativo dell’area è CoVig-1 e la casella di posta certificata istituzionale è protocollovigevano@pec.it.

1.4 Casella di posta elettronica certificata

La casella di Posta Elettronica Certificata (PEC) istituzionale protocollovigevano@pec.it, pubblicata sull’Indice delle Pubbliche Amministrazioni (IPA), è accessibile, per la ricezione di documenti, solo al Servizio Protocollo, mentre tutte le Strutture organizzative possono utilizzarla per la corrispondenza in partenza.

La casella è accessibile ai tecnici del Servizio ICT per la sua manutenzione e gestione tecnica.

Il Comune si riserva la facoltà di istituire ulteriori PEC assegnate ai Servizi, o a singoli funzionari e/o responsabili di procedimento, quando previsto dalle normative di settore. L’elenco delle PEC è pubblicato e costantemente aggiornato sul sito istituzionale dell’Ente.

1.5 Servizio ICT, PROTOCOLLO E GESTIONE DOCUMENTALE E - GESTIONE ARCHIVIO E ARCHIVIO STORICO

Nell’ambito dell’area organizzativa omogenea, ai sensi dell’articolo 61, comma 1, del DPR 445/2000, fu istituito, con deliberazione di Giunta Comunale n. 92 del 15/05/2007 il Servizio archivistico per la gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi, individuato nella Unità operativa complessa Protocollo e Archivio moderno.

Il servizio ai sensi dell’articolo 61, comma 3, del DPR 445/2000 aveva competenza sulla gestione dell’intera documentazione archivistica, ovunque trattata, distribuita o conservata, del Comune, ai fini della sua corretta registrazione, classificazione, fascicolazione, conservazione, selezione e ordinamento.

Con deliberazione di G.C. n. 228 del 10/12/2020 e n. 21 del 04/02/2021 è stata approvata la revisione del funzionigramma connesso alla macrostruttura dell'Ente, consultabile nel dettaglio all'*Allegato 2 – Funzionigramma*, che ha individuato sotto il Settore Politiche sociali e culturali l'unità "Gestione Archivio e Archivio storico" e sotto il Settore Servizi alla Città il "Servizio ICT, Protocollo e gestione documentale", determinando la suddivisione "de facto", delle competenze di gestione e conservazione dei documenti sulle due unità e sotto due responsabili diversi.

1.6 Responsabile del Protocollo e della gestione documentale e Responsabili della conservazione

Nell'ambito dell'Area Organizzativa Omogenea sono previste le funzioni di Responsabile della gestione documentale e quella di Responsabile della conservazione. Esse sono funzionalmente individuate nella struttura competente in materia di archivio e protocollo dell'Ente e fanno capo al Responsabile della stessa. Nei casi di vacanza, assenza o impedimento del Responsabile, lo stesso individua il proprio sostituto.

Stante la suddivisione del servizio sotto due settori differenti la figura di Responsabile della conservazione (soggetto responsabile dell'insieme delle attività elencate al paragrafo 3.4 delle "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" emanate da AGID entrate in vigore il 10 settembre 2020 ed attuate il 7 giugno 2021) sarà individuato per la documentazione informatica nel responsabile del "Servizio ICT, Protocollo e gestione documentale" e per la documentazione cartacea nel responsabile della "Gestione Archivio e Archivio storico".

I responsabili collaborano per la gestione corretta della conservazione degli atti dell'Ente.

Al Responsabile della gestione documentale sono assegnati i seguenti compiti, disciplinati rispettivamente dagli artt. 4 e 5 delle Regole tecniche per il Protocollo:

- predisporre ed aggiornare il manuale di gestione di cui ai paragrafi 3.1.2. e 3.5 delle Linee Guida AGID d'intesa con il Responsabile per la transizione digitale di cui all'art.17 del CAD e acquisito il parere del responsabile della protezione dei dati personali, di cui agli artt. 37 e 39 del Regolamento UE 679/2016. Per assicurare il corretto mantenimento ed aggiornamento del presente manuale, le strutture organizzative dell'Ente devono segnalare tempestivamente al Servizio di Protocollo ogni evento che può determinare la modifica od integrazione dello stesso.
- attribuire alle Strutture organizzative abilitate il livello di autorizzazione per l'accesso alle funzioni del sistema di protocollo informatico, distinguendo tra abilitazioni alla consultazione ed abilitazioni all'inserimento e alla modifica delle informazioni;
- garantire che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto della normativa vigente;
- garantire la corretta produzione e la conservazione del registro giornaliero di protocollo;
- curare che le funzionalità del sistema in caso di guasti o anomalie siano ripristinate entro ventiquattro ore dal blocco delle attività e comunque nel più breve tempo possibile;
- garantire lo svolgimento anche manuale delle operazioni di registrazione di protocollo su un registro di emergenza, ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura informatica;
- garantire il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione documentale e dei flussi documentali, adottare i provvedimenti di annullamento delle registrazioni di protocollo, qualora ne ricorrano i presupposti;
- effettuare la verifica periodica del piano di classificazione dell'Ente.

Il Responsabile della conservazione (soggetto responsabile dell'insieme delle attività elencate nel paragrafo 4.5 delle "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" redatte da AGID) deve:

- definire le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;
- gestire il processo di conservazione e garantire nel tempo la conformità alla normativa vigente;
- generare e sottoscrivere il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- generare e sottoscrivere il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- effettuare il monitoraggio della corretta funzionalità del sistema di conservazione;
- effettuare la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
- adottare le misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità al fine di garantire la conservazione e l'accesso ai documenti informatici;
- adottare analoghe misure con riguardo all'obsolescenza dei formati;
- provvedere alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- predisporre le misure necessarie per la sicurezza fisica e logica del sistema di conservazione come previsto dal par. 4.11;
- predisporre il manuale di conservazione di cui al par. 4.7 e curarne l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Le attività di cui sopra sono definite nell'*Allegato 8 - Piano di selezione, conservazione e scarto*.

1.7 Protocollo Informatico

1.7.1 Componenti e funzionalità

Il protocollo informatico comprende i seguenti moduli funzionali:

- la scrivania virtuale organizzata sulla base delle segreterie di settore/servizio;
- il sistema di apposizione di firme digitali e relativa validazione;
- strumenti eterogenei di visualizzazione dei documenti informatici gestiti;
- sistema di ricezione e gestione dei messaggi di PEC.

Il protocollo informatico garantisce le seguenti funzionalità:

- protocollazione, gestione e visualizzazione dei documenti;
- gestione del titolario d'archivio su più livelli e sua storicizzazione;
- gestione del repertorio dei fascicoli e dei sottofascicoli, consentendone l'aggiornamento in ordine alla creazione di nuovi fascicoli, con assegnazione automatica del numero sequenziale e aggiornamento delle informazioni ad essi relative, tra cui le date di creazione e chiusura;
- fascicolazione dei documenti attraverso la gestione di fascicoli e sottofascicoli repertoriati;

- gestione del legame tra precedente e susseguente dei documenti;
- integrazione funzionale con applicativi verticali;
- collegamento delle scansioni di documenti analogici alle relative registrazioni di protocollo;
- tracciamento delle modifiche, ove consentite (data, ora, utente);
- annullamento di registrazioni di protocollo;
- produzione del registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno e invio alla conservazione;
- gestione dei documenti in arrivo tramite PEC e gestione dell'interoperabilità tra pubbliche amministrazioni;
- verifica delle firme elettroniche associate ai documenti informatici ricevuti e dell'integrità del documento informatico sottoscritto;
- protocollazione manuale o automatizzata dei documenti in entrata tramite PEC;
- gestione automatizzata dell'invio tramite PEC;
- gestione automatica delle ricevute elettroniche di accettazione e consegna a fronte di invio tramite PEC;
- gestione dei flussi documentali (smistamento, presa in carico, ripudio, inoltro dei documenti);
- ricerca dei documenti avvalendosi delle informazioni fondamentali di segnatura di protocollo e in modalità full-text dell'oggetto di ogni singolo documento;
- ricerca dei fascicoli, avvalendosi delle informazioni archivistiche fondamentali e in modalità full-text dell'oggetto di ogni singolo fascicolo;
- stampa del titolario di classificazione, del repertorio dei fascicoli, con o senza visibilità dei documenti in essi contenuti, e dei documenti stessi;
- stampa degli esiti di ricerca;
- estrazione in formato "Excel" o "pdf" dei dati risultanti da ricerca.

1.7.2 Accesso alle funzionalità del Protocollo Informatico

Il protocollo informatico consente l'attribuzione di diversi profili di utilizzo delle funzioni. Sono stati individuati diversi profili di accesso in particolare: operatori decentrati, operatori decentrati con gestione "*pec funzionale*", protocollatori centrali, amministratori di sistema. Gli utenti che accedono al sistema, previa autorizzazione dei rispettivi dirigenti di Settore possono svolgere le seguenti operazioni in base al loro ruolo:

Ruolo	Operazioni consentite
Operatori decentrati	gestione dei fascicoli;
	registrazione di protocollo entrata, uscita, interna
	smistamento e presa in carico dei documenti
	invio tramite PEC istituzionale dei protocolli in uscita
	gestione dei fascicoli e dei documenti ad essi collegati
Operatori decentrati con gestione " <i>pec funzionale</i> "	gestione dei fascicoli;
	registrazione di protocollo entrata, uscita, interna
	smistamento e presa in carico dei documenti
	gestione dei fascicoli e dei documenti ad essi collegati

Ruolo	Operazioni consentite
Protocollatori centrali	invio tramite PEC istituzionale dei protocolli in uscita
	Invio tramite PEC funzionale dei protocolli in uscita
	accesso alle caselle di posta elettronica certificate funzionale
	gestione dei fascicoli;
	registrazione di protocollo entrata, uscita, interna
	smistamento e presa in carico dei documenti
	gestione dei fascicoli e dei documenti ad essi collegati
Amministratori di sistema	Gestione PEC istituzionale
	modifica non sostanziale dei campi delle informazioni obbligatorie (oggetto e mittente/destinatario); supporto alla consultazione e ricerca dei protocolli registrati
	gestione degli annullamenti
	formazione e aggiornamento dei dizionari (titolario di classificazione, unità, tipo documento, tipo oggetto)
	abilitazione degli utenti all'accesso al sistema e alle modalità di utilizzo
	gestione (attivazione e chiusura) delle scrivanie di segreteria
	gestione degli annullamenti
	modifica non sostanziale dei campi delle informazioni obbligatorie (oggetto e mittente/destinatario);

1.7.3 Unicità del Protocollo Informatico

Nell'ambito dell'Area Organizzativa Omogenea la numerazione delle registrazioni di protocollo è unica, progressiva, corrisponde all'anno solare ed è composta da almeno sette cifre numeriche ai sensi dell'articolo 57 del testo unico, tuttavia a norma dell'articolo 53, comma 5 del DPR 445/2000 sono possibili registrazioni particolari.

L'Amministrazione non riconosce validità a registrazioni particolari che non siano quelle individuate nell'elenco *"Allegato 4- Documenti non soggetti a protocollazione - Registrazioni particolari"*.

Ad ogni documento è dato un solo numero, che non può essere utilizzato per la registrazione di altri documenti anche se correlati allo stesso.

A seguito dell'introduzione del protocollo unico per garantire la corretta classificazione e organizzazione dei documenti viene adottato un unico Titolario di classificazione.

Il protocollo fa fede, anche con valore giuridico, dell'effettivo ricevimento e spedizione di un documento, pertanto la documentazione non registrata presso il Servizio di Protocollo viene considerata giuridicamente inesistente, al netto delle registrazioni particolari.

1.8 Registro giornaliero di protocollo

Il registro giornaliero di protocollo si genera quotidianamente, mediante produzione automatica dell'elenco dei protocolli e delle informazioni ad essi correlate, registrati nell'arco della giornata

lavorativa. Al fine di garantire l'immodificabilità del contenuto, ai sensi dell'art. 7, co. 5, delle Regole tecniche per il protocollo informatico, il registro giornaliero di protocollo viene trasmesso entro la giornata lavorativa successiva al sistema di conservazione dei documenti.

CAPITOLO 2 – GESTIONE DEI DOCUMENTI

2.1 Modello operativo adottato per la gestione dei documenti

Per la gestione dei documenti è adottato un modello operativo parzialmente decentrato che prevede la partecipazione attiva di più soggetti ed uffici abilitati a svolgere soltanto le operazioni di loro competenza.

Le abilitazioni sono rilasciate/revocate su indicazione del responsabile del servizio di gestione documentale a seguito di specifica richiesta del dirigente di settore.

Specificamente i documenti in entrata sono gestiti:

- in modo centralizzato dall'Ufficio Protocollo per quanto riguarda il flusso cartaceo postale ed il flusso informatico quando indirizzato alla pec istituzionale;
- in modo decentrato per quanto riguarda il flusso informatico indirizzato alle pec funzionali dei seguenti settori:

PEC IN USO		
STRUTTURA ORGANIZZATIVA	PEC	NOTE
Settore Affari Generali, Contratti, Controlli	vigevano@pec.aruba.it	Pec tecnica utilizzata per la convocazione del Consiglio comunale e delle commissioni consiliari
UOC Anagrafe, Leva	anagrafevigevano@pec.it	
UOC Stato civile, elettorale e statistica	statocivilevigevano@pec.it	
Settore Sicurezza, Polizia Locale e Protezione Civile	polizialocalevigevano@pec.it	
Servizio Urbanistica e gestione e controllo convenzioni urbanistiche	vigevanourbanistica@pec.it	
Servizio Programmazione Appalti e LL.PP.	lavoripubblicivigevano@pec.it	
Servizio Edilizia Privata e controlli, S.U.A.P., commercio e attività produttive e controlli pubblici spettacoli e sicurezza pubblica	suevigevano@pec.it	PEC tecnica Programma Archiweb e Cportal della ditta Starch
U.O.C. Sportello Unico Commercio e Attività Produttive, Impianti Pubblicitari	suapvigevano@pec.it	PEC tecnica collegata ad Imprese in un giorno della Camera di Commercio e al Programma Archiweb e Cportal della ditta Starch

- in modo decentrato per quanto riguarda il flusso di gestione delle uscite, salvo casi eccezionali e motivati.

I documenti cartacei sono depositati presso i rispettivi uffici dell'Amministrazione mentre i documenti informatici ricevuti dai soggetti abilitati, presso le diverse unità operative, sono direttamente gestiti dai responsabili di procedimento.

L'Archivio Storico e di deposito analogico situato presso la sede in Via Merula 40, Palazzo Merula, raccoglie la documentazione dell'Ente dal 1227 al 1975.

L'Archivio Moderno (sede via Martiri delle Foibe) raccoglie la documentazione dell'Ente dal 1976 e giunge orientativamente fino alla fine degli anni '90.

Non esiste una data ultima univoca per i contenuti in Archivio Moderno, dal momento che varia a seconda delle tipologie documentali o di altri parametri.

La documentazione degli ultimi 20 anni è in genere raccolta presso gli uffici che la redigono/gestiscono o presso archivi "locali" situati nelle varie sedi.

2.2 Modalità di formazione dei documenti

I documenti trattati dall'Amministrazione riportano le seguenti informazioni minime:

- denominazione e stemma dell'Amministrazione con indicazione del settore, servizio o ufficio che produce il documento (è disponibile agli uffici un modello di carta intestata);
- indirizzo completo del destinatario comprensivo di mail e/o di pec;
- oggetto del documento. L'oggetto è collegato al contenuto e deve risultare comprensibile. L'oggetto del documento, se cartaceo, e quello riportato nella protocollazione informatica dello stesso documento devono essere uguali;
- testo del documento;
- data completa, luogo, giorno, mese, anno;
- sottoscrizione autografa chiaramente leggibile o sottoscrizione digitale;
- in calce (piè di pagina): indirizzo dell'ufficio mittente con le informazioni necessarie per le comunicazioni;
- numero di protocollo (esplicitato sul documento qualora cartaceo, e associato al documento, se digitale);
- indice di classificazione e numero di fascicolo;
- numero degli allegati, se presenti;

Le regole valide per la produzione e gestione del documento informatico sono applicate al documento amministrativo informatico.

Gli originali dei documenti vengono prodotti secondo le regole tecniche di cui all'articolo 71 del CAD, mediante l'utilizzo di appositi strumenti software nel rispetto delle regole di interoperabilità acquisendo le istanze, le dichiarazioni e le comunicazioni di cui agli articoli 5-bis, 40-bis e 65 del CAD.

I sistemi per la gestione di pratiche quali: pareri, verbali, autorizzazioni, altri documenti, integrati con il Protocollo Informatico consentono la gestione di procedimenti in forma esclusivamente digitale (pratiche ambientali ed edilizie) ed utilizzano allo scopo specifiche pec funzionali elencate nella tabella "Pec in uso" al "Capitolo 2 – Gestione dei documenti - 2.1 Modello operativo adottato per la gestione dei documenti" del presente Manuale.

I restanti documenti e i loro allegati vengono formati con programmi in uso all'Ente quindi salvati di norma in formato "pdf/A" e, qualora richiesto dal procedimento, firmati digitalmente. La loro successiva protocollazione comporta l'associazione del file digitale alla scheda di protocollo.

Le comunicazioni riportanti documentazione non protocollata avvenute tramite messaggio di posta elettronica ordinaria sono da considerarsi informali.

Nel caso di comunicazioni a cittadini sprovvisti di domicilio digitale (pec), gli uffici predispongono documenti informatici sottoscritti con firma digitale, da conservare agli atti, ed inviano ai cittadini stessi, per posta ordinaria o con raccomandata con avviso di ricevimento, copia analogica di tali documenti sottoscritti con firma autografa.

Al documento amministrativo informatico viene associato l'insieme dei metadati previsti per la registrazione di protocollo ai sensi degli articoli 53 e 56 del TUDA.

Ai sensi del codice in materia di protezione dei dati personali, i certificati e gli atti trasmessi ad altre pubbliche amministrazioni o altri enti esterni, contengono le informazioni relative a stati, fatti e qualità personali previste da legge o da regolamento, strettamente necessarie per il perseguimento delle finalità per le quali vengono acquisite.

2.3 Sottoscrizione dei documenti informatici

La sottoscrizione dei documenti informatici è ottenuta con un processo di firma digitale ai sensi della normativa vigente.

Tutti i Dirigenti, i Responsabili di Servizio ed alcuni dipendenti con specifiche mansioni sono dotati di firma digitale.

Con riferimento alla PEC, l'Ente utilizza la firma digitale ad eccezione dei casi in cui si trasmettano documenti originali informatici sottoscritti digitalmente. L'utilizzo dell'applicativo di protocollo prevede la firma digitale.

CAPITOLO 3 - RICEZIONE DEI DOCUMENTI

3.1 Ricezione dei documenti su supporto cartaceo

I documenti su supporto cartaceo possono pervenire all'Ente attraverso:

- a) il servizio postale (servizio effettuato da Poste Italiane o altre società abilitate e certificate ai servizi postali);
- b) la consegna diretta agli uffici;
- c) sistema fax management.

I documenti che transitano attraverso il servizio postale tradizionale pervengono ogni giorno nell'orario di apertura dell'Ufficio Protocollo, tramite il servizio di consegna effettuato dal servizio postale di cui al sopracitato punto a).

Dei documenti analogici ricevuti viene effettuata la scansione sostitutiva e la documentazione cartacea viene consegnata agli uffici destinatari.

I documenti consegnati direttamente agli uffici dell'Ente se sono soggetti a registrazione di protocollo, sono fatti pervenire, a cura del personale che li riceve e nell'arco preferibilmente della stessa giornata, agli operatori abilitati alla registrazione di protocollo dei documenti in arrivo per il proprio servizio o recapitati all'Ufficio Protocollo, qualora non di propria competenza.

I documenti ricevuti attraverso il sistema di fax management dell'Ente, che li recapita via email ai operatori abilitati, se soggetti a registrazione di protocollo, sono trattati secondo le procedure previste per la ricezione dei documenti informatici.

3.2 Ricezione dei documenti informatici

Il Comune di Vigevano riceve i documenti informatici in una delle seguenti modalità:

1. a mezzo posta elettronica certificata (PEC);
2. a mezzo posta elettronica ordinaria (PEO);

3. tramite trasmissioni telematiche e cooperazione applicativa;
4. su supporto rimovibile (quale, ad esempio, CD ROM, DVD, pen drive, etc.)

1. La ricezione dei documenti informatici indirizzati all'Ente tramite PEC avviene di norma sulla PEC protocollovigevano@pec.it, dichiarata istituzionalmente e pubblicata nell'Indice nazionale della Pubblica Amministrazione IPA da parte del Responsabile della gestione documentale ai sensi dell'articolo 12, comma 2, lettera c), del DPCM 31 ottobre 2000 ed integrata al sistema di gestione del Protocollo. Come specificato al *Capitolo 2 – Gestione dei documenti* paragrafo *“2.1 Modello operativo adottato per la gestione dei documenti”*, esistono altre PEC funzionali, pubblicate sul sito del Comune, alle quali possono essere inoltrate direttamente o tramite appositi sw le istanze o eventuale documentazione. Le PEC funzionali sono gestite direttamente dalle strutture preposte.

2. Nel caso in cui istanze o altri documenti significativi ai fini del procedimento pervengano su indirizzi di posta elettronica ordinaria PEO, è consigliata la comunicazione al mittente della necessità di rinnovare l'invio del messaggio se in possesso di PEC, al fine di garantire la correttezza delle procedure di protocollazione, spedendo lo stesso alla casella PEC istituzionale.

3. Il Comune di Vigevano ha predisposto appositi form per presentazione di istanze da parte dei cittadini autenticati tramite SPID che vengono protocollate automaticamente tramite la connessione al sistema centrale di protocollo.

4. Nel caso di presentazione di documenti su supporti rimovibili di cui al punto 4 del paragrafo 3.2, viene protocollata solo la lettera di accompagnamento e gli eventuali allegati ed indicata nella registrazione di protocollo la presenza di supporto rimovibile.

L'Ufficio Protocollo trasmette il tutto all'ufficio competente.

I formati accettati dalla PEC istituzionale, dalle PEC funzionali e dalle PEO devono rispettare i formati elencati nell'“*Allegato 10– Formati accettati*”

3.3 Rilascio di ricevute attestanti la ricezione dei documenti

L'ufficio Protocollo rilascia la ricevuta attestante l'avvenuta consegna di un documento, effettuando fotocopia del primo foglio su cui viene apposto il timbro di pervenuto indicante la data e la sigla dell'operatore. Nel caso di bandi con scadenze, l'Ufficio utilizza un timbro apposito che reca oltre la data, la modalità di arrivo del documento e l'orario.

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

Nel caso di ricezione di documenti tramite Posta elettronica ordinaria (PEO), si trasmette al mittente numero e data di protocollazione e su richiesta la “*Copia Conforme col numero di protocollo*”.

3.4 Documenti trasmessi tra Pubbliche Amministrazioni

Le comunicazioni tra il Comune di Vigevano e altre pubbliche amministrazioni avvengono mediante l'utilizzo della posta elettronica certificata garantendone l'interoperabilità;

Il sistema informatico assicura l'autenticità ed integrità della segnatura di protocollo applicando un sigillo elettronico avanzato.

3.5 Protocollazione automatica dei documenti

Il Comune ha adottato piattaforme tecnologiche online che consentono al cittadino o al professionista di presentare istanze telematiche.

Le procedure attualmente collegate utilizzano la PEC istituzionale o in taluni casi delle apposite PEC funzionali elencate nel dettaglio al paragrafo “2.1 Modello operativo adottato per la gestione dei documenti” del presente manuale.

Elenco delle procedure collegate al Protocollo:

- Software di back office per la gestione delle pratiche del settore territorio
- Software di front office per la gestione delle pratiche del settore territorio
- Software gestione prenotazione sale comunali
- Software di gestione per le prenotazioni spazi fiere (in fase di attivazione)
- Software di gestione delle pratiche di richiesta contributo del Piano di Zona

Il Comune si riserva la facoltà di attivare altre procedure informatizzate collegate automaticamente al protocollo dell'Ente in ottica di dematerializzazione delle procedure cartacee.

CAPITOLO 4 - REGISTRAZIONE DEI DOCUMENTI

4.1 Documenti soggetti a registrazione di protocollo

Tutti i documenti prodotti e ricevuti dall'Amministrazione, indipendentemente dal supporto sul quale sono formati, ad eccezione di quelli indicati nell'*Allegato 4- “Documenti non soggetti a protocollazione - Registrazioni particolari”* sono registrati al Protocollo.

4.2 Registrazione di protocollo dei documenti ricevuti e spediti

La registrazione dei documenti ricevuti o spediti è effettuata in un'unica operazione.

Il sistema di protocollo prevede una voce specifica per i protocolli interni, utilizzato per la protocollazione dei documenti prodotti dagli uffici dell'Ente e non spediti a soggetti esterni al Comune.

I requisiti necessari per ciascuna registrazione di protocollo sono elencati di seguito e categorizzati nella tabella sottostante in base alla tipologia di documento:

- a) numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
- b) data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
- c) mittente o destinatario dei documenti ricevuti o spediti, registrato in forma non modificabile;
- d) oggetto del documento, registrato in forma non modificabile;
- e) data e numero di protocollo del documento ricevuto se disponibili;
- f) documento principale
- g) impronta del documento informatico, se trasmesso per via telematica, registrato in forma non modificabile;
- h) classificazione: categoria, classe
- i) assegnazione all'ufficio di competenza
- j) ufficio dell'Ente che ha prodotto il documento

I requisiti facoltativi sono:

- k) data di arrivo;
- l) numero degli allegati;
- m) descrizione sintetica degli allegati;
- n) documenti allegati

- o) estremi di differimento dei termini di registrazione;
- p) mezzo di ricezione o in alternativa mezzo di spedizione;
- q) copia per conoscenza
- r) tipo di documento
- s) indicazione del tipo di riservatezza
- t) fascicolo¹

Tipologia di documento

Cartaceo

Interno

Documenti informatici

Dati obbligatori

a) b) c) d) e) g) h) j)

a) b) c) d) e) f) g) h) i) j)

a) b) c) d) e) f) g) h) j)

Dati facoltativi

k) l) m) n) o) p) q) t)

k) l) m) n) o) p) q) t)

k) l) m) n) o) p) q) t)

4.3 Segnatura di Protocollo

La segnatura di protocollo apposta o associata al documento è effettuata contemporaneamente alla registrazione di protocollo.

La segnatura dei documenti analogici in ingresso avviene tramite l'utilizzo di apposite etichette o in alternativa per ovviare ad eventuali guasti, tramite timbro (Timbro di Protocollo).

Le etichette riportano i seguenti dati: codice identificativo dell'amministrazione, data di protocollo, numero di protocollo, oggetto, classifica, assegnatario del documento, barcode;

Il timbro riporta: codice identificativo dell'Amministrazione, data di protocollo, numero di protocollo, titolo, classifica, fascicolazione, assegnatario del documento.

La segnatura dei documenti informatici è contenuta nell'ambito dello stesso messaggio in un file conforme alle specifiche XML e compatibile con il DTD reso disponibile a livello nazionale dalle strutture tecniche competenti.

Le informazioni minime contenute nella segnatura di protocollo di un documento informatico sono le seguenti:

- a) codice identificativo dell'amministrazione
- b) codice identificativo dell'area organizzativa omogenea
- c) data di protocollo;
- d) numero di protocollo.
- e) indice di classificazione;
- f) numero del fascicolo;
- g) oggetto del documento
- h) mittente
- i) destinatario o destinatari
- j) "signature" per permettere la firma della segnatura di protocollo conformemente al profilo XADEX

¹ Vista la gestione attuale che prevede la protocollazione centralizzata per quanto attiene alla documentazione cartacea e alla pec istituzionale, la fascicolazione viene demandata all'ufficio di competenza.

4.4 Annullamento dei protocolli

Le registrazioni di protocollo possono essere annullate con una specifica funzione del sistema di gestione informatica dei documenti previa autorizzazione del responsabile della gestione documentale a seguito di motivata richiesta, o per iniziativa dello stesso responsabile.

Le registrazioni annullate rimangono memorizzate nella base dati e sono evidenziate dal sistema. Il sistema durante la fase di annullamento registra gli estremi del provvedimento autorizzativo redatto dal responsabile della gestione documentale.

Sui documenti cartacei è apposto un timbro/dicitura che attesti l'annullamento del protocollo.

Le richieste di annullamento dei numeri di protocollo devono pervenire in forma scritta all'ufficio Protocollo che provvederà ogni quattro mesi ad effettuare tale procedura. Nella registrazione informatica del documento verrà riportata una dicitura con gli estremi del verbale di annullamento.

L'autorizzazione all'annullamento dei documenti viene protocollata e conservata, insieme alle richieste di annullamento inviate dai servizi.

Non è possibile annullare il solo numero di protocollo e mantenere valide le altre informazioni della registrazione.

4.5 Registro giornaliero e annuale di protocollo

Il registro giornaliero di protocollo è prodotto automaticamente dal sistema di Protocollo e trasmesso automaticamente entro la giornata lavorativa successiva al sistema di conservazione, garantendone la non modificabilità del contenuto, secondo quanto previsto nel Manuale di conservazione (*Allegato 8 - Piano di selezione, conservazione e scarto*).

Delle registrazioni del protocollo informatico è sempre possibile estrarre evidenza analogica.

4.6 Registro di emergenza

Il Responsabile della gestione documentale autorizza lo svolgimento delle operazioni di protocollo su un registro di emergenza a norma dell'articolo 63 del DPR 455/2000, ogni qualvolta non sia possibile utilizzare il sistema, per cause tecniche, provvedendo successivamente a impartire le disposizioni per il riversamento dei dati nel protocollo informatico tramite le procedure previste dal manuale operativo del sistema informatico e dalla guida all'attivazione del registro *Allegato 7 – Procedura per l'attivazione del Registro di Emergenza*.

Il registro di emergenza informatico è gestito attraverso l'utilizzo di un apposito programma standalone, opportunamente configurato per gestire i dati minimi di protocollo, che verranno inviati al sistema di protocollo al termine del periodo di emergenza.

Nel caso di prolungata interruzione di energia elettrica, l'Ufficio Protocollo gestisce un registro di emergenza cartaceo, che consta di pagine preventivamente numerate, timbrate e firmate dal Responsabile della gestione documentale.

Sul registro di emergenza, limitatamente alle operazioni di registrazione dei documenti e di recupero dei dati nel sistema di protocollo informatico, gli operatori dell'Ufficio Protocollo, applicano le modalità previste dalla normativa vigente come segue:

- 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;
- qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre le ventiquattro ore, per cause di eccezionale gravità, il Responsabile può autorizzare l'uso del registro di emergenza per periodi ulteriori 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 delle 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'Area Organizzativa Omogenea;
- le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico utilizzando un'apposita funzione di recupero 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 informativo ordinario, che provvede a mantenere stabilmente la correlazione con il numero assegnato in emergenza.

All'inizio di ogni anno il Responsabile della gestione documentale provvede a istituire il Registro di Emergenza sia su supporto cartaceo sia su postazione adibita all'installazione dell'applicativo stand alone.

L'applicativo per essere utilizzato in modo efficace deve essere aggiornato almeno ogni 6 mesi o comunque quando si verificano modifiche al titolare o alla struttura organizzativa per importare correttamente i dizionari necessari al suo utilizzo.

La numerazione delle registrazioni di emergenza è unica per l'anno solare e inizia da 1.

4.8 Documentazione particolare

4.8.1 Deliberazioni di Giunta e Consiglio, determinazioni organizzative, ordinanze, disposizioni dirigenziali, determinazioni dirigenziali e di posizione organizzativa

Le deliberazioni di Giunta e Consiglio, le determinazioni organizzative, le ordinanze e le disposizioni dirigenziali e i contratti sono documenti soggetti a registrazione particolare dell'Amministrazione "*Allegato 4- Documenti non soggetti a protocollazione - Registrazioni particolari*", non registrati al protocollo.

Il software di produzione e conservazione di questa tipologia particolare di documentazione consente di eseguire su di essi tutte le operazioni previste nell'ambito della gestione dei documenti e del sistema adottato per il protocollo informatico.

Questi documenti costituiscono delle serie archivistiche, ciascuna delle quali è corredata da un repertorio contenente le seguenti informazioni:

- i dati identificativi di ciascun atto;
- i dati di classificazione e fascicolazione;
- il numero di repertorio che è un numero progressivo, annuale.

4.8.2 Documenti inerenti a gare d'appalto

Tutte le gare rientranti nel codice degli appalti D.lgs 50/2016 vengono obbligatoriamente gestite dal 01/01/2019 solo in modalità telematica.

Le procedure di gara condotte tramite le piattaforme telematiche Sintel o MEPA devono essere registrate nel sistema di gestione documentale dell'Ente in quanto le suddette piattaforme non garantiscono la conservazione della documentazione informatica prodotta.

Gli elementi che devono essere registrati sono:

- il bando, il disciplinare, il capitolato e gli altri allegati di gara, e l'aggiudicazione con tutti gli allegati ed il report di gara che riassume tutte le operazioni condotte dalla Stazione appaltante e le comunicazioni intercorse.

La registrazione delle offerte non vincitrici, delle comunicazioni tramite piattaforma, e di tutto il resto della documentazione di gara, non elencata nel paragrafo precedente, è soggetta a registrazione particolare, si utilizzano in tal caso i numeri univoci di registrazione della documentazione prodotta dalle piattaforme Sintel o MEPA.

Relativamente a procedure di gara per le quali non vi è l'obbligo del ricorso al mercato elettronico, la documentazione dovrà pervenire in modalità analogica.

4.8.3 Posta personale

I documenti analogici o digitali, ricevuti e indirizzati al personale dell'Ente sono regolarmente aperti e registrati al protocollo, a meno che sulla busta non sia riportata la dicitura "personale" o "riservata personale", in questo caso la busta sarà trasmessa chiusa al destinatario senza essere protocollata.

4.8.4 Lettere anonime e documenti non firmati

Le lettere anonime non sono registrate al protocollo, ma semplicemente inoltrate, se contengono informazioni o dati di interesse per l'Amministrazione, agli uffici di competenza i quali valutano l'opportunità di dare seguito a queste comunicazioni ed individuano le eventuali procedure da sviluppare.

4.8.5 Documenti inviati via fax

La normativa vigente prevede l'esclusione della corrispondenza via fax fra pubbliche amministrazioni.

La trasmissione di documenti via fax con cittadini o altri soggetti privati non aventi l'obbligo di comunicazione in forma telematica con la pubblica amministrazione richiede la registrazione di protocollo.

L'Ente utilizza per la ricezione e l'invio di fax un sistema di fax management, che consente l'acquisizione dei documenti in formato elettronico tramite caselle di posta elettronica dedicata. I documenti vengono protocollati ed inseriti nel sistema di gestione documentale.

Di norma al fax non segue mai l'originale. Qualora successivamente arrivasse anche l'originale del documento, a questo sarà attribuito lo stesso numero di protocollo.

4.8.6 Documenti di competenza di altre amministrazioni

Qualora pervengano all'Ente documenti di competenza di altre amministrazioni, questi vanno rifiutati con notifica di eccezione. Il documento deve essere rimandato al mittente (notifica di eccezione).

4.8.7 Corrispondenza degli irreperibili o senza fissa dimora:

Il servizio Anagrafe fornisce, a persone senza dimora presenti sul territorio del Comune di Vigevano, la residenza anagrafica in una via fittizia secondo quanto previsto dalla circolare ISTAT n.29 del 1992, consentendo loro di attivare i diritti di cittadinanza.

L'Ufficio Protocollo destinerà le raccomandate ricevute, senza protocollarle, alla Casa Comunale (Ufficio Messi).

La posta ordinaria non deve essere protocollata ma restituita all'ufficio postale. In quest'ultimo caso, qualora il cittadino fosse seguito dai Servizi Sociali, l'Ufficio Protocollo recapiterà la missiva all'assistente sociale di riferimento in modo tale che possa consegnarlo all'assistito.

4.8.9 Richieste di autocertificazioni e/o dichiarazioni sostitutive ed in genere scritti avulsi da qualsiasi procedimento amministrativo dell'Ente

Le richieste di autocertificazioni e/o dichiarazioni sostitutive ed in genere gli scritti avulsi da qualsiasi procedimento amministrativo dell'Ente non devono essere protocollati, *vedasi "Allegato 4- Documenti non soggetti a protocollazione - Registrazioni particolari"*.

CAPITOLO 5 – SMISTAMENTO, ASSEGNAZIONE, PRESA IN CARICO

5.1. Assegnazione dei documenti

L'assegnazione dei documenti ai servizi/uffici competenti, è effettuata dall'operatore addetto alla protocollazione che effettua l'assegnazione sulla base del funzionigramma *Allegato 2- Funzionigramma*.

Qualora sia necessario consegnare un documento analogico originale, questo dovrà essere consegnato all'ufficio che risulta assegnatario nel sistema di gestione documentale, mentre la scansione dello stesso ad eventuali altri assegnatari per conoscenza e competenza.

5.2. Modifica delle assegnazioni

Nel caso di assegnazione inesatta dei documenti, l'ufficio ricevente è tenuto a respingerlo con la dicitura "non di competenza" all'Ufficio mittente, inserendo la motivazione del rifiuto e possibilmente l'indicazione del corretto destinatario.

L'ufficio mittente provvederà alla corretta riassegnazione trasmettendolo al nuovo assegnatario.

La non accettazione del documento deve avvenire entro due giorni lavorativi.

Il sistema di gestione informatica dei documenti tiene traccia dei passaggi di cui sopra, memorizzando per ciascuno di essi l'identificativo dell'operatore, data e ora di esecuzione.

5.3 Presa in carico automatizzata

Il sistema di protocollo è configurato per evitare che i documenti smistati ai servizi/uffici competenti restino inevasi per mancata presa in carico o rifiuto e riassegnazione.

Trascorsi 30 giorni dalla mancata presa in carico da parte del destinatario, il software di protocollo attribuirà automaticamente il documento al destinatario stesso.

Il documento preso in carico automaticamente dal sistema è visibile a tutti gli operatori della struttura assegnataria solo nella gestione documentale e non più nella scrivania virtuale.

L'operatore deve trattare il documento e quindi *"eseguirlo"*.

5.4 Assegnazione alla Segreteria Generale di atti non smistabili

Raramente vengo trasmessi documenti di difficile assegnazione in quanto non sono chiare le competenze richieste.

In tal caso, quando le strutture organizzative più attinenti rifiutano tutto lo smistamento, l'Ufficio Protocollo provvede a smistare i documenti alla Segreteria Generale per la loro gestione.

CAPITOLO 6 - CLASSIFICAZIONE DEI DOCUMENTI

6.1 Classificazione dei documenti

La classificazione è l'operazione finalizzata all'organizzazione dei documenti secondo un ordinamento logico in relazione alle competenze, alle funzioni ed alle attività dell'amministrazione. Essa è eseguita sulla base del titolario di classificazione. *Allegato 5- Piano di classificazione dell'Ente.*

Tutti i documenti ricevuti o prodotti indipendentemente dal supporto sul quale sono formati, sono classificati in base al titolario dell'Ente.

Sono classificati anche gli atti preparatori interni, le minute o altri documenti che non vengono protocollati o che sono soggetti a registrazione particolare.

Il programma di protocollo informatico non permette la registrazione di documenti non classificati.

L'aggiornamento del Titolario compete al Responsabile della gestione documentale e ai Responsabili della conservazione nel pieno rispetto delle disposizioni contenute nella normativa vigente in materia di formazione e conservazione degli archivi.

Le modifiche devono essere comunicate a tutti i soggetti abilitati all'operazione di classificazione dei documenti d'archivio.

Tutti i documenti registrati nel sistema di protocollo informatico, indipendentemente dal supporto sul quale sono formati, devono essere classificati dall'unità protocollante e in seguito fascicolati dalla struttura assegnataria.

La classifica, come la fascicolazione sono dati essenziali ma modificabili post protocollazione. Esempio: modifica di una classificazione errata.

6.2 Creazione e identificazione dei fascicoli

Tutti i documenti, indipendentemente dal supporto sul quale vengono formati, sono riuniti in fascicoli come da articolo 64, comma 4, del TUDA che prevede: *“Le amministrazioni determinano autonomamente e in modo coordinato per le aree organizzative omogenee, le modalità di attribuzione dei documenti ai fascicoli che li contengono e ai relativi procedimenti, definendo adeguati piani di classificazione d'archivio per tutti i documenti, compresi quelli non soggetti a registrazione di protocollo”.*

L'operazione di creazione dei fascicoli deve essere effettuata all'inizio dell'anno solare ad esclusione dei fascicoli pluriennali o legati alla durata del procedimento relativo.

I fascicoli vanno regolarmente chiusi dalle strutture organizzative competenti quando l'ultima pratica al suo interno è conclusa, i fascicoli annuali devono essere chiusi entro i primi giorni dell'anno successivo all'apertura.

Nel corso dell'anno le strutture organizzative possono creare ulteriori fascicoli in aggiunta a quelli già aperti, qualora necessario.

I dati essenziali inseriti nel fascicolo sono: categoria e classe del titolare, numero del fascicolo, oggetto del fascicolo, data di apertura.

Il sistema di protocollo informatico aggiorna automaticamente l'elenco dei fascicoli.

6.3 Modifica delle assegnazioni dei fascicoli

La riassegnazione di un fascicolo è effettuata, su istanza scritta della struttura organizzativa che ha in carico il fascicolo, dal Ufficio Protocollo che provvede a riassegnarlo alla nuova struttura competente.

Le operazioni di riassegnazione vengono tracciate dal sistema di protocollo.

6.4 Fascicolo ibrido

Il fascicolo è composto da documenti formati su due supporti, quello cartaceo e quello informatico, afferenti ad un procedimento amministrativo che dà origine a due unità archivistiche di conservazione differenti; l'unitarietà del fascicolo è garantita dal sistema mediante l'indice di classificazione e il numero di repertorio che dovrà essere apposto identico su entrambe le unità archivistiche.

Operativamente deve essere fatta la stampa del numero di classifica e fascicolo (*stampa copertina*) da anteporre sulla cartella cartacea in cui vengono inseriti i documenti cartacei.

In presenza di documenti cartacei da inserire in fascicoli informatici, dovrà essere prodotta copia per immagine degli stessi conforme secondo la normativa vigente. L'originale cartaceo sarà conservato presso gli uffici/servizi dell'Ente.

6.2 Piano di conservazione dell'archivio

Il piano di conservazione dell'archivio dell'area organizzativa omogenea è riportato nell'*Allegato 8 - Piano di selezione, conservazione e scarto* ed è strettamente correlato al titolare di classificazione. In esso sono indicati i tempi di conservazione delle categorie di documenti e di atti, con l'indicazione "a conservazione permanente".

Il suo aggiornamento compete esclusivamente al responsabile della gestione documentale e ai responsabili della conservazione ed è assicurato quando se ne presenta la necessità, nel pieno rispetto delle disposizioni contenute nella normativa vigente in materia di formazione e conservazione degli archivi.

Dopo ogni modifica del piano di conservazione, i suddetti responsabili provvedono ad informare tutti i soggetti abilitati all'operazione di selezione e scarto dei documenti d'archivio e a darne loro le istruzioni per il corretto utilizzo.

CAPITOLO 7 – SPEDIZIONE

7.1 Spedizione documentazione analogica

La documentazione da spedire deve pervenire all'Ufficio Protocollo già imbustata a cura dell'ufficio mittente, il quale è responsabile della sua protocollazione, classificazione e fascicolazione.

Nel caso di spedizione di raccomandate devono essere accompagnate da apposita distinta elencante i soggetti destinatari, la città di destinazione, il numero di protocollo e la struttura mittente. Sono forniti alle strutture dell'Ente appositi modelli.

Spedizioni di grandi quantità di corrispondenza (posta massiva, intesa come spedizioni superiori ai 100 pezzi) ed eventuali spedizioni urgenti devono essere concordate con l'Ufficio Protocollo. La corrispondenza deve essere consegnata all'Ufficio Protocollo per la sua corretta gestione dall'orario di apertura al pubblico sino alle ore 10:30.

7.2 Spedizione dei documenti informatici

Per la spedizione dei documenti informatici soggetti alla registrazione di protocollo mediante l'utilizzo della posta elettronica l'ente si avvale di indirizzi di posta elettronica certificata e/o ordinaria (PEC istituzionale e PEC funzionali di cui al paragrafo 2.1 *Modello operativo adottato per la gestione dei documenti* del presente manuale).

I documenti vengono trasmessi, dopo essere stati classificati, fascicolati e protocollati, secondo le procedure all'indirizzo di posta elettronica dichiarato dai destinatari abilitati alla ricezione della posta per via telematica ovvero:

- in caso di spedizione di un documento al cittadino/utente, all'indirizzo di posta elettronica certificata comunicato in qualità di domicilio digitale.
- in caso di PA all'indirizzo pubblicato su IPA
- in caso di imprese e professionisti all'indirizzo pubblicato sull'Indice Nazionale degli Indirizzi PEC delle imprese e dei professionisti (INI PEC).

Le postazioni deputate ad effettuare l'invio telematico verificano l'avvenuto recapito dei documenti e il collegamento delle ricevute elettroniche alle registrazioni di protocollo.

I corrispondenti destinatari dell'Ente sono descritti in appositi elenchi costituenti l'anagrafica unica dell'Ente. In assenza del domicilio digitale l'Ente può predisporre le comunicazioni ai cittadini come documenti informatici sottoscritti con firma digitale ed inviare ai cittadini stessi, per posta ordinaria o raccomandata con avviso di ricevimento, copia analogica di tali documenti secondo la normativa vigente. L'Ente dovrà conservare l'originale digitale nei propri archivi; all'interno della copia analogica spedita al cittadino, deve essere riportata la dicitura che la copia originale del documento è conservata dall'Ente. La spedizione di documenti informatici, attraverso posta elettronica, al di fuori dei canali istituzionali descritti, è considerata una mera trasmissione di informazioni senza che a queste l'Ente riconosca un carattere giuridico-amministrativo che la impegni verso terzi.

7.3 Corrispondenza con più destinatari e copie per conoscenza

Tutte le comunicazioni che abbiano più destinatari e il medesimo contenuto, si registrano con un solo numero di protocollo. I destinatari sono indicati sulla registrazione di protocollo e vengono selezionati dall'anagrafica dell'IPA nel caso di pubbliche amministrazioni, dall'anagrafica dei beneficiari della contabilità o inseriti manualmente tramite apposito form.

Il canale di comunicazione preferenziale è quello della PEC, qualora disponibile.

7.4 Allegati

Tutti gli allegati devono essere trasmessi insieme al documento principale all'ufficio di protocollo per la registrazione. Su ogni allegato analogico è riportato il timbro della segnatura di protocollo.

Il sistema informatico provvede automaticamente a registrare gli allegati come parte integrante di un documento elettronico. Nel caso in cui una PEC contenga allegati illeggibili si dovrà chiedere chiarimenti al mittente in merito al documento allegato (notifica di eccezione).

7.5 Invio di documenti tra uffici dell'Ente - Protocollo interno

La comunicazione di natura giuridica probatoria o di rilevanza amministrativa della quale si vuole tenere traccia nel fascicolo relativo al procedimento cui si riferisce, deve essere protocollata tramite apposita funzione del sistema di protocollo informatico denominata "Protocollo Interno".

La protocollazione segue le stesse regole della protocollazione verso l'esterno, salvo l'individuazione del destinatario che nella fattispecie è un'unità organizzativa dell'Ente o uno specifico funzionario.

CAPITOLO 8 – ARCHIVIAZIONE DEI DOCUMENTI

8.1 Archiviazione dei documenti e dei fascicoli cartacei

I fascicoli cartacei dell'archivio corrente sono formati a cura dei responsabili dei procedimenti amministrativi e conservati presso gli uffici produttori.

I documenti sono conservati a cura delle strutture organizzative, secondo quanto previsto dal presente manuale. La documentazione corrente, relativa alle pratiche in corso non ancora terminate, è conservata a cura dei responsabili dei singoli uffici fino al trasferimento in archivio moderno, secondo quanto previsto dagli articoli dell'*Allegato 8 "Piano di selezione, conservazione e scarto"*.

8.2 Archiviazione dei documenti e dei fascicoli informatici

I documenti informatici sono memorizzati in modo non modificabile, contestualmente alle operazioni di registrazione e segnatura di protocollo.

Il Responsabile della conservazione informatica garantisce la corretta e puntuale esecuzione delle procedure di conservazione in modo da assicurare l'accesso al documento e la sua esibizione.

Il Responsabile del servizio di gestione documentale provvede a controllare periodicamente a campione (almeno ogni sei mesi) la leggibilità dei documenti conservati.

Il Comune di Vigevano ha individuato in PARER² (ex. IBACN), a seguito delle Deliberazioni di Giunta Comunale n. 199/2013 e n. 251/2018 e n.120/2019, la figura del Responsabile del servizio della conservazione dei documenti informatici con la sottoscrizione dell'*"Accordo di collaborazione per lo svolgimento della funzione di conservazione dei documenti digitali"* avvenuto in data 06/06/2019.

Il *Disciplinare tecnico per lo svolgimento della funzione di conservazione dei documenti informatici* elenca le tipologie documentarie inviate in conservazione e nello specifico:

Tipologia di unità documentaria	Sistema versante	Data di primo versamento
CONTRATTO SACER_VERSO, SACER_VERSO (per automi)	automa_sacer_verso,	06/08/2018
DECRETO SINDACALE	JSUITE (Ads)	20/03/2017

2 Servizio Polo Archivistico Regionale della Regione Emilia Romagna istituito con apposita Deliberazione di Giunta Regionale

Tipologia di unità documentaria	Sistema versante	Data di primo versamento
DELIBERA DI CONSIGLIO	JSUITE (Ads)	20/03/2017
DELIBERA DI GIUNTA	JSUITE (Ads)	20/03/2017
DETERMINAZIONE	JSUITE (Ads)	20/03/2017
DOCUMENTO PROTOCOLLATO	JSUITE (Ads)	22/03/2016
FATTURA ATTIVA	JSUITE (Ads)	11/07/2016
FATTURA PASSIVA	JSUITE (Ads)	11/07/2016
FLUSSO DISPONIBILITÀ LIQUIDE FLUSSO GIORNALE DI CASSA	JSUITE (Ads)	23/09/2019
FLUSSO ORDINATIVI	JSUITE (Ads)	23/09/2019
MANDATO MESSAGGIO ACK SIOPE	JSUITE (Ads)	23/09/2019
MESSAGGIO ESITO APPLICATIVO	JSUITE (Ads)	23/09/2019
MESSAGGIO RICEZIONE FLUSSO	JSUITE (Ads)	28/09/2020
MESSAGGIO RIFIUTO FLUSSO	JSUITE (Ads)	30/09/2020
ORDINANZA DIRIGENZIALE	JSUITE (Ads)	20/03/2017
ORDINANZA SINDACALE	JSUITE (Ads)	20/03/2017
REGISTRO GIORNALIERO	JSUITE (Ads)	23/03/2017

Le modalità di conservazione e accesso ai documenti, analogici o digitali, sono specificate con riferimento al Manuale di conservazione di PARER (*Allegato n. 9 – PARER – ManualeConservazione_ver2021fin e suoi allegati*).

8.3 Formati accettati

I formati accettati idonei alla conservazione sono specificati nell'*Allegato 10 – Formati accettati*.

8.4 Sistema informatico

Il sistema informatico, le misure di sicurezza fisica e logica, le procedure adottate per la gestione del sistema documentale sono descritte nel Piano della sicurezza informatica *Allegato 11 – Piano della sicurezza*.

ALLEGATI

Allegato 1 - Glossario dei Termini

Allegato 2 - Funzionigramma

Allegato 3 - Nomine

**Allegato 4 - Documenti non soggetti a protocollazione -
Registrazioni particolari**

Allegato 5 - Piano di classificazione dell'Ente

**Allegato 6 - Regolamento dell'accesso civico e dell'accesso
agli atti (approvato con deliberazione di Consiglio Comunale n. 69 del
11/10/2019)**

**Allegato 7- Procedura per l'attivazione del Registro di
Emergenza**

Allegato 8 - Piano di selezione, conservazione e scarto

Allegato 9 - PARER – ManualeConservazione_ver2021fin

Allegato 10 - Formati accettati

Allegato 11 – Piano della sicurezza



Allegato 1 – Glossario dei termini

Accesso: l'operazione che consente, a chi ne ha diritto, di prendere visione ed estrarre copia dei documenti.

Accreditamento facoltativo: riconoscimento del possesso, da parte del certificatore che lo richieda, dei requisiti del livello più elevato, in termini di qualità e sicurezza.

Affidabilità del sistema di gestione documentale: , la caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta;

Affare: complesso di documenti prodotti (spediti, ricevuti, allegati, ecc.) da un ente, relativi alla trattazione di un oggetto specifico di sua competenza; si chiama affare o anche pratica.

Albo pretorio: albo che espone al pubblico atti ufficiali.

Allegato: nota unita ad un documento o ad una pratica per prova, per chiarimento o integrazione di notizie, per memoria.

AOO (Area Organizzativa Omogenea): insieme definito di unità organizzative di una amministrazione, che usufruiscono, in modo omogeneo e coordinato, di comuni servizi per la gestione dei flussi documentali. In particolare una AOO utilizza per il servizio di protocollazione un'unica sequenza numerica, rinnovata ogni anno solare. Ogni comune costituisce un'unica AOO.

Archivio: il complesso dei documenti prodotti o comunque acquisiti da un ente durante lo svolgimento della propria attività e si divide in tre parti: archivio corrente, per la parte relativa agli affari in corso; archivio di deposito, per la parte di documentazione relativa agli affari esauriti; archivio storico, per la parte di documentazione relativa agli affari esauriti destinata alla conservazione perenne. L'archivio pur caratterizzandosi in tre momenti diversi è da considerarsi una sola unità. Con archivio si intende anche il luogo fisico di conservazione della documentazione.

Archivio informatico: archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche;

Archivio storico: il complesso di documenti relativi ad affari esauriti da 40 anni e destinati, previa operazioni di scarto, alla conservazione permanente per garantirne in forma adeguata la consultazione al pubblico;

Assegnazione: individuazione del servizio/ufficio competente per la trattazione dell'affare o procedimento amministrativo e della gestione dei documenti nella fase corrente.

Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico: la dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico;

Autenticità: la caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze;

Base di dati : (o banca dati; ing. database), raccolta di dati riguardanti uno stesso argomento, o più argomenti correlati tra loro archiviati su adeguati supporti secondo regole precise e generati in modo da poter essere consultati, manipolati e modificati agevolmente con l'impiego di un apposito linguaggio (chiamato Sql: Structured Query Language, vedi). La base di dati, oltre ai dati veri e propri, deve contenere anche gli elementi necessari alla loro rappresentazione (le informazioni sulla loro struttura e sulle relazioni che li legano). La funzionalità di un database dipende essenzialmente dalla sua progettazione: la corretta individuazione degli scopi dei database e quindi delle tabelle, da definire attraverso i loro campi e le relazioni che le legano, permette poi una estrazione dei dati più veloce e, in generale, una gestione più efficiente.

Carteggio: o epistolario, complesso delle lettere inviate e ricevute da una persona. L'espressione, propria della corrispondenza tra persone fisiche, si usa anche per intendere la parte dell'archivio di un ente relativa all'attività che si esplica mediante scambio di lettere e note con persone o con enti: così nell'archivio di un ente si potranno distinguere le serie di registri dalla serie del carteggio. (Fonte P. Carucci, *Le fonti archivistiche: ordinamento e conservazione*, Roma, Carocci, 2010.)

Casella istituzionale di posta elettronica (PEC): casella di posta elettronica, istituita da un'AOO, per la ricezione dall'esterno e per la spedizione all'esterno dei documenti da registrare a protocollo.

Categoria: partizione del titolario, contrassegnata da un simbolo costituito da un numero romano, o da un numero arabo, o da una lettera dell'alfabeto, oppure da un simbolo misto costituito da una lettera e un numero, ecc.

Certificati elettronici: attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche e confermare l'identità digitale dei titolari stessi.

Certificato elettronico qualificato: il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva n. 1999/93/ce, rilasciato da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva.

Certificatore: ai sensi dell'articolo 2, comma 1, lettera b del decreto legislativo 10/2002, il soggetto che presta servizi di certificazione delle firme elettroniche/digitali o che fornisce altri servizi connessi con queste ultime.

Certificazione: attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.

Chiusura del documento informatico: processo con cui la versione finale del documento viene memorizzata in modo definitivo su supporto informatico, con le informazioni necessarie per la sua rappresentazione ed individuazione. (ex Cnipa - AGID).

Client (it. Cliente): programma o computer che interagisce con un programma o computer remoto (server, vedi) permettendo di accedere a servizi e risorse da questi distribuite, normalmente via rete. (Sartini)

Classificazione: l'attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore;

Cloud della PA, l'ambiente virtuale che consente alle Pubbliche Amministrazioni di erogare servizi digitali ai cittadini e alle imprese nel rispetto di requisiti minimi di sicurezza ed affidabilità.

Codec: l'algoritmo di codifica e decodifica che consente di generare flussi binari, eventualmente imbustarli in un file o in un wrapper (codifica), così come estrarli da esso (decodifica);

Codice dell'amministrazione digitale (CAD): il d.lgs. 7 marzo 2005, n. 82, recante il Codice dell'amministrazione digitale.

Codice identificativo utente o user name o nome utente: il codice assegnato ai soggetti che, a diverso titolo, accedono ai documenti gestiti dall'Ente, per accedere dalla propria postazione di lavoro alle applicazioni informatiche, nonché ai dati e ai documenti da esse gestiti.

Condizionare, condizionatura condizionare un fondo significa sostituire i contenitori vecchi con buste nuove, o inserire in buste nuove unità archivistiche legate con lo spago, prive cioè di qualsiasi contenitore (Fonte P. Carucci, Le fonti archivistiche: ordinamento e conservazione, Roma, Carocci, 2010.)

Conservatore: il soggetto pubblico o privato che svolge l'attività di conservazione dei documenti informatici.

Conservazione: l'insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governare la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità e reperibilità dei documenti.

Conservazione sostitutiva, processo effettuato con le modalità di cui al decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013, recante "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, Autorità Nazionale Anticorruzione Versione 2.4 del 21 maggio 2020 Pag. 5 di 37 commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis.

Convenzioni di denominazione del file: l'insieme di regole sintattiche che definisce il nome dei file all'interno di un filesystem o pacchetto;

Coordinatore della gestione documentale: il soggetto responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'art. 50 comma 4 del DPR 445/2000 nei casi di Amministrazioni che abbiano istituito più AOO.

Copia: riproduzione di un documento originale eseguita a mano, a macchina o mediante apparecchio per fotocopiare. Non ha valore giuridico. La copia ha valore giuridico e si definisce autentica o autenticata quando è emessa da un ente che può rilasciare copie conformi all'originale e reca segni di autenticazione. Copia semplice: non ha forme legali che le diano valore di prova. Copia autentica: legittimata da sottoscrizione notarile. Copia vidimata: convalidata da autorità pubblica invece che da notai. Copia imitativa: riproduce, non per falsificazione, anche i caratteri grafici originali.

Copia analogica del documento informatico: il documento analogico avente contenuto identico a quello del documento informatico da cui è tratto.

Deposito: 1) locale nel quale un ente conserva la propria documentazione non più occorrente alla trattazione degli affari in corso. Si chiamano depositi anche i locali nei quali un archivio di concentrazione conserva gli archivi in esso confluiti. (Fonte P. Carucci, Le fonti archivistiche: ordinamento e conservazione, Roma, Carocci, 2010.)

Documento: una testimonianza di un fatto, non necessariamente di natura giuridica, compilata, su tipologie diverse di supporti e varie tecniche di scrittura, con l'osservanza di determinate forme che sono destinate a darle fede e forza di prova. Gli elementi essenziali del documento sono: autore, destinatario, testo, sottoscrizione, data; per la registrazione al protocollo questi elementi devono necessariamente essere presenti. Ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa.

Documento archiviato: documento informatico, anche sottoscritto, sottoposto al processo di archiviazione elettronica.

Documento conservato: documento sottoposto al processo di conservazione sostitutiva.

Documento informatico: la rappresentazione informatica di atti, fatti, o dati giuridicamente rilevanti.

Elenco: lista con indicazione più o meno sommaria della documentazione compresa in ciascuna busta e dei registri di un fondo non riordinato, secondo l'ordine in cui si trovano le singole unità.

E-mail: (posta elettronica), sistema di comunicazione elettronica attraverso messaggi.

Ente produttore di archivio: soggetto giuridico di natura pubblica o privata che, nello svolgimento della sua attività, forma, gestisce e conserva documenti.

Esibizione: operazione che consente di visualizzare un documento conservato e di ottenerne copia. La procedura che consente all'interessato o ai soggetti autorizzati dall'Ordinamento la consultazione di un documento informatico.

Evidenza informatica: una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.

Fascicolo: l'insieme dei documenti relativi a una determinata pratica (o affare), collocati, all'interno di una camicia (o copertina), in ordine cronologico; ne consegue che per ogni pratica (o affare) avremo il relativo fascicolo. L'insieme dei fascicoli costituisce la serie. I documenti sono collocati, all'interno del fascicolo, secondo l'ordine di archiviazione, pertanto il documento più recente è il primo aprendo la copertina e il più antico è l'ultimo.

Fatto giuridico: fatto che produce effetti giuridici; quindi ogni fatto dal quale una norma del diritto fa derivare qualche conseguenza.

Fax: apparecchio per la ricetrasmisione di documenti/informazioni tramite la rete telefonica; il documento/informazione ricevuta o trasmessa attraverso tale apparecchio; il contenuto del documento stesso.

Fibra ottica: filamento in fibra di vetro, utilizzato nelle telecomunicazioni in grado di trasmettere segnali digitali di alta velocità attraverso impulsi luminosi e con una capacità di trasmissione notevolmente superiore rispetto a quella dei tradizionali sistemi di trasmissione elettrica. Viene solitamente indicata come “accesa”, quando è effettivamente utilizzata, e “spenta” se invece non è collegata ad apparati.

Firma digitale: è un particolare di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica ed una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Firma elettronica: ai sensi dell'articolo 2, comma 1, lettera g, del decreto legislativo 10/2002, l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica.

Flusso documentale: movimento dei documenti all'interno dell'archivio (dalla fase di formazione dell'archivio corrente a quella di conservazione dell'archivio storico).

Funzione di hash: una funzione matematica che genera, a partire da una generica sequenza di simboli binari (bit), una impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari (bit) che la generi, ed altresì risulti di fatto impossibile determinare una coppia di sequenze di simboli binari per le quali la funzione generi impronte uguali.

Gestione dei documenti: l'insieme di attività finalizzate alla registrazione di protocollo e alla classificazione, organizzazione, assegnazione e reperimento dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato.

Impronta: la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash. Un'evidenza informatica di lunghezza predefinita ottenuta da un'altra evidenza informatica mediante un'opportuna funzione matematica

tale che risulti di fatto impossibile, a partire dall'impronta, ricostruire l'evidenza informatica che l'ha generata, ed altresì risulti di fatto impossibile determinare una coppia di evidenze informatiche per le quali la funzione generi impronte uguali.

Internet, rete di reti che collega milioni di persone in tutto il mondo. Nasce come evoluzione della rete americana ARPAnet.

Interoperabilità: possibilità di trattamento automatico, da parte del sistema di protocollo ricevente, delle informazioni trasmesse dal sistema di protocollo mittente, allo scopo di automatizzare le attività e i procedimenti amministrativi conseguenti (dPR 445/ 2000, art 55, comma 4 e dPCM 31/10/2000, art. 15).

Intranet: rete interna di una azienda realizzata utilizzando protocolli della famiglia TCP/IPP;

Inventario: è lo strumento fondamentale per eseguire le ricerche: descrive tutte le unità che compongono un archivio ordinato.

Manuale di conservazione: il documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti degli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture.

Manuale di gestione documentale: il documento informatico che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Marca temporale: un'evidenza informatica che consente la validazione temporale.

Massimario di scarto: lo strumento archivistico che indica, per ciascuna partizione del titolario di classificazione, quali documenti debbono essere conservati permanentemente e quali invece possono essere destinati al macero dopo un periodo di conservazione di 5, 10, 15 o più anni.

Metadati: i dati associati ad un documento informatico, ad un fascicolo informatico o ad un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura – così da permetterne la gestione nel tempo – in conformità a quanto definito nella norma ISO 15489- 1:2016 e, più nello specifico, dalla norma ISO 23081-1:2017.

Massimario di selezione: anche detto di scarto, il massimario di selezione è lo strumento che consente di coordinare razionalmente lo scarto archivistico (cioè la destinazione al macero) dei documenti prodotti dagli enti pubblici e dagli organi centrali e periferici dello Stato. Il massimario riproduce l'elenco delle partizioni (categorie) e sottopartizioni del titolario con una descrizione più o meno dettagliata delle competenze cui ciascuna partizione si riferisce e della natura dei relativi documenti; indica per ciascuna partizione quali documenti debbano essere conservati permanentemente (e quindi versati dopo quarant'anni dall'esaurimento degli affari nei competenti Archivi di Stato) e quali invece possono essere destinati al macero dopo cinque anni, dopo dieci anni, dopo venti anni, ecc.

Memorizzazione: processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici informatici, anche sottoscritti.

Mezzo di corredo: con questa espressione si intendono tutti gli strumenti che contengono la descrizione, analitica o sommaria, delle unità archivistiche o dei singoli documenti che compongono un archivio o un fondo archivistico: si tratta di inventari, elenchi, elenchi di consistenza, elenchi di versamento, regesti, indici, rubriche, schedari, ecc.

Microfilm: il microfilm rientra tra le tecniche reprografiche di riproduzione, quelle cioè che consentono di riprodurre l'originale in fac-simile (fotografia, fotocopia, xerografia, ecc)

Minuta: per ogni destinato ad essere spedito vengono compilati due esemplari, uno dei quali viene spedito e pertanto entra a far parte dell'archivio del destinatario, l'altro invece viene conservato dall'autore ed entra a far parte dell'archivio del mittente. Se lo scritto deve essere spedito a più destinatari, verranno compilati tanti esemplari quanti sono i destinatari più un esemplare che resta al mittente. L'esemplare che resta al mittente si chiama minuta.

Naming convention: convenzioni di denominazione utilizzate per identificare variabili, tipi, funzioni ed altre entità durante la stesura di codice sorgente.

Oggetto di conservazione: l'oggetto digitale versato in un sistema di conservazione;

Oggetto: in sede di formazione del documento l'oggetto è l'enunciazione sommaria, sintetizzata in poche parole, al massimo un paio di righe, dell'argomento di cui tratta il documento. L'oggetto viene scritto sul documento nello spazio apposito e deve essere riportato (talora con parole diverse) sia sul registro di protocollo dell'ente che scrive sia su quello dell'ente che riceve il documento.

Originale: è la stesura definitiva del documento, perfetto nei suoi elementi sostanziali e formali.

Pacchetto di archiviazione: il pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione;

Pacchetto di file: l'insieme di più file che costituiscono un contenuto informativo unitario ed auto-consistente.

Pacchetto di versamento: il pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.

Pacchetto informativo: il contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione.

Path: Un percorso (in lingua inglese "path" o "pathname"), in informatica, indica la posizione specifica di un elemento (file o cartella) all'interno di un archivio dati, con un certo file system strutturato ad albero. Il percorso consiste dunque in una stringa di caratteri che elenca,

ordinatamente, i diversi nodi del file system da visitare per raggiungere l'elemento in questione.
(Fonte: Wikipedia, l'enciclopedia libera)

Pathname: Un percorso (in lingua inglese "path" o "pathname"), in informatica, indica la posizione specifica di un elemento (file o cartella) all'interno di un archivio dati, con un certo file system strutturato ad albero. (Fonte: Wikipedia, l'enciclopedia libera)

Percorso: Un percorso (in lingua inglese "path" o "pathname"), in informatica, indica la posizione specifica di un elemento (file o cartella) all'interno di un archivio dati, con un certo file system strutturato ad albero. (Fonte: Wikipedia, l'enciclopedia libera)

Pezze: documenti giustificativi.

Piano di classificazione: vedi Titolario

Piano di conservazione: L'art. 68 del DPR 445/2000 prevede che ogni amministrazione debba dotarsi di un «piano di conservazione degli archivi, integrato con il sistema di classificazione, per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione dei documenti». (Fonte: Linee Guida sulla formazione, gestione e conservazione dei documenti informatici)

Piano della sicurezza del sistema di conservazione: il documento che, nel contesto del piano generale della sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi. (Fonte: Linee Guida sulla formazione, gestione e conservazione dei documenti informatici)

Piano della sicurezza del sistema di gestione informatica dei documenti: il documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi. (Fonte: Linee Guida sulla formazione, gestione e conservazione dei documenti informatici)

Posta Elettronica Certificata (PEC): ha lo stesso valore legale di una raccomandata tradizionale con avviso di ricevimento. Per certificare l'invio e la ricezione di un messaggio di PEC, il gestore di posta invia al mittente una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio e dell'eventuale documentazione allegata. Allo stesso modo, il gestore invia al mittente la ricevuta di avvenuta (o mancata) consegna del messaggio, con precisa indicazione temporale.
(Fonte: Agid)

Presa in carico: si indica l'assunzione di responsabilità rispetto al buon fine di un fatto (nuovo) richiesto. Nel caso della conservazione a norma si intende l'accettazione da parte del sistema di conservazione del pacchetto di versamento, conforme alle specifiche previste dal manuale di conservazione.

Protocollo informatico: il registro su supporto informatico sul quale vengono registrati quotidianamente i documenti spediti e ricevuti da un ente. La registrazione di protocollo costituisce elemento probante dell'autenticità del documento ed è l'operazione con cui un documento entra a far parte integrante di un archivio e della memoria di un ente, per cui un documento non protocollato è come se non fosse mai stato prodotto o ricevuto. Il protocollo è atto pubblico di fede

privilegiata fino a querela di falso¹; il protocollo è elemento essenziale per la gestione della memoria delle pubbliche amministrazioni in caso di mancanza del numero di protocollo il documento può perdere la sua efficacia².

Protocollo: il numero progressivo automatico apposto a un documento al momento della registrazione nel protocollo informatico.

Pubblico ufficiale: La definizione di pubblico ufficiale si ricava dall'art. 357 del c.p.. E' tale colui che esercita una funzione legislativa, amministrativa o giudiziaria con o senza rapporto di impiego con lo Stato, temporaneamente o permanentemente (come ad esempio i notai, i segretari comunali, etc.).

Quadro/Titolario di classificazione: lo strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni o attività dell'amministrazione interessata.

Registro: insieme di fogli rilegati sul quale si trascrivono o si registrano, per esteso o per sunto, documenti o minute di documenti.

Registro giornaliero di protocollo: registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti.

Registro particolare: un registro informatico individuato dalla Pubblica Amministrazione per memorizzare le informazioni relative a documenti soggette a registrazioni particolari di protocollo che non rientrano pertanto nel protocollo informatico dell'Ente.

Regolamento eIDAS: Il Regolamento eIDAS (electronic IDentification Authentication and Signature) - Regolamento UE n° 910/2014 sull'identità digitale - ha l'obiettivo di fornire una base normativa a livello comunitario per i servizi fiduciari e i mezzi di identificazione elettronica degli stati membri.

Repertorio: registro su cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni del titolario: il repertorio deve essere organizzato in maniera da riprodurre le suddivisioni del titolario.

Rete di accesso: l'insieme dei collegamenti che connettono l'utente con una rete per l'utilizzazione dei servizi.

Rete: l'insieme di infrastrutture che consentono di trasportare le informazioni generate da una sorgente a uno o più destinatari.

Riferimento temporale: informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici. (Fonte: Cnipa 11/04)

¹ Consiglio di Stato, 1993, I, 838; Foro amministrativo, 1993, 1494 e Giust. Civ.

² Commissione centrale imposte, sez. VI. 6 apr. 1982, n. 338.

Riproduzione digitale dei documenti informatici: il processo che trasferisce documenti informatici da un supporto di memorizzazione a un altro. (Cnipa).

Riproduzione sostitutiva: il processo che trasferisce documenti da un supporto analogico a un supporto digitale o che trasferisce documenti informatici adottando, tra quelli riconosciuti, un formato di rappresentazione informatica diverso dall'originale. (Cnipa)

Riversamento diretto: processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, non alterando la loro rappresentazione informatica. Per tale processo non sono previste particolari modalità. (Cnipa 11/04)

Riversamento sostitutivo: processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro modificando la loro rappresentazione informatica. Per tale processo sono previste le modalità descritte nell'art. 3, comma 2, e nell'art. 4, comma 4, della presente deliberazione. (Cnipa 11/04)

Rubrica: registro con i margini scalettati e contraddistinti con lettere dell'alfabeto, o schedario, su cui si registrano per materie, per nomi di enti o di persone o di luoghi, disposti in ordine alfabetico, i singoli documenti o le pratiche in base al loro contenuto: il documento o la pratica sarà richiamato in tutte le voci cui può essere riferito il contenuto.

Scarto: operazione con cui si destina al macero una parte della documentazione di un archivio.

Segnatura: si chiamano sottoscrizioni o signature le sottoscrizioni autografe o i segni rappresentativi (segni di cancelleria e segni di tabellionato) delle persone che hanno concorso con la loro opera o col loro consenso a comporre, autenticare e conferire pubblicità al documento (autore, consenzienti, testimoni, cancellieri, notai, ecc.). Si chiamano signature archivistiche le classificazioni e le numerazioni che contraddistinguono ciascuna unità archivistica.

Segnatura di protocollo: l'apposizione o l'associazione, all'origine del documento, in forma permanente e non modificabile delle informazioni riguardanti il documento stesso.

Selezione: operazione intellettuale di vaglio dei documenti tendente a individuare quelli da destinare alla conservazione permanente e quelli da destinare allo scarto.

Server: programma che gestisce, elabora e fornisce dati ad un client (vedi). Inoltre un server è un computer, dotato di una ingente memoria, uno o più dischi di grande capacità e grandi risorse di calcolo, che ospita risorse e fornisce servizi (accesso a banche dati, accesso condiviso e periferiche ecc.) ad altri computer (detti client). (Sartini)

Servizio archivistico: il servizio per la gestione informatica dei documenti, del protocollo, dei flussi documentali e degli archivi.

Sigillo elettronico: è equivalente a una firma elettronica qualificata, con la differenza che non afferisce a una persona fisica, bensì a una persona giuridica. In altri termini, mentre da una firma siamo in grado di individuare con certezza un soggetto attraverso il suo nome, cognome, codice

fiscale ecc., da un sigillo possiamo risalire con certezza ad una persona giuridica attraverso la sua denominazione, partita IVA o codice fiscale, ma non abbiamo alcun riferimento alla persona fisica che ha materialmente utilizzato le credenziali per generare tale sigillo. (Fonte: AGID)

Sistema di gestione informatica dei documenti: l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti.

Sistema per la conservazione dei documenti informatici: l'insieme delle procedure, degli strumenti informatici, degli apparati e delle regole di sicurezza utilizzato per le attività finalizzate alla conservazione dei documenti informatici. (ex Cnipa - AGID)

Sottofascicolo: ulteriore suddivisione del fascicolo che a sua volta può essere articolato in inserti: in questo caso i documenti saranno collocati in ordine cronologico l'interno di ciascun inserto. Il sottofascicolo ha la stessa classificazione e numero del fascicolo, a sua volta articolato in sottounità.

SQL (Structured Query Language it. linguaggio di interrogazione strutturato): linguaggio usato per la manipolazione e l'interrogazione di database relazionali e per l'accesso alle informazioni memorizzate in essi. (Sartini)

Supporto ottico di memorizzazione: mezzo fisico che consente la memorizzazione di documenti informatici mediante l'impiego della tecnologia laser (dischi ottici, magneto-ottici, DVD). (Cnipa 11/04)

Titolario: quadro di classificazione, costituito da un determinato numero di categorie (o titoli, o classi), articolate in sottopartizioni e contrassegnate da simboli numerici o alfabetici o misti.

Titolo: 1) indica una partizione del titolario: in questo senso è sinonimo di categoria o classe, a seconda dei termini usati da ciascun ente.

2) indica la definizione che raggruppa i fascicoli appartenenti a una serie. Esempio: «Nella stesura dell'inventario la serie viene indicata col titolo originario». 3) indica anche l'oggetto del fascicolo. 4) con la parola titolo si chiamano anche quegli atti che creano diritti o ne provano l'esistenza.

U.O.: unità organizzativa

Uffici utente: vedi U.O.

Unità archivistica: indica, al pari di pezzo, il documento o un insieme di documenti, rilegati o raggruppati secondo un nesso di collegamento organico, che costituiscono un'unità non divisibile: registro, volume, filza, mazzo o fascio, fascicolo.

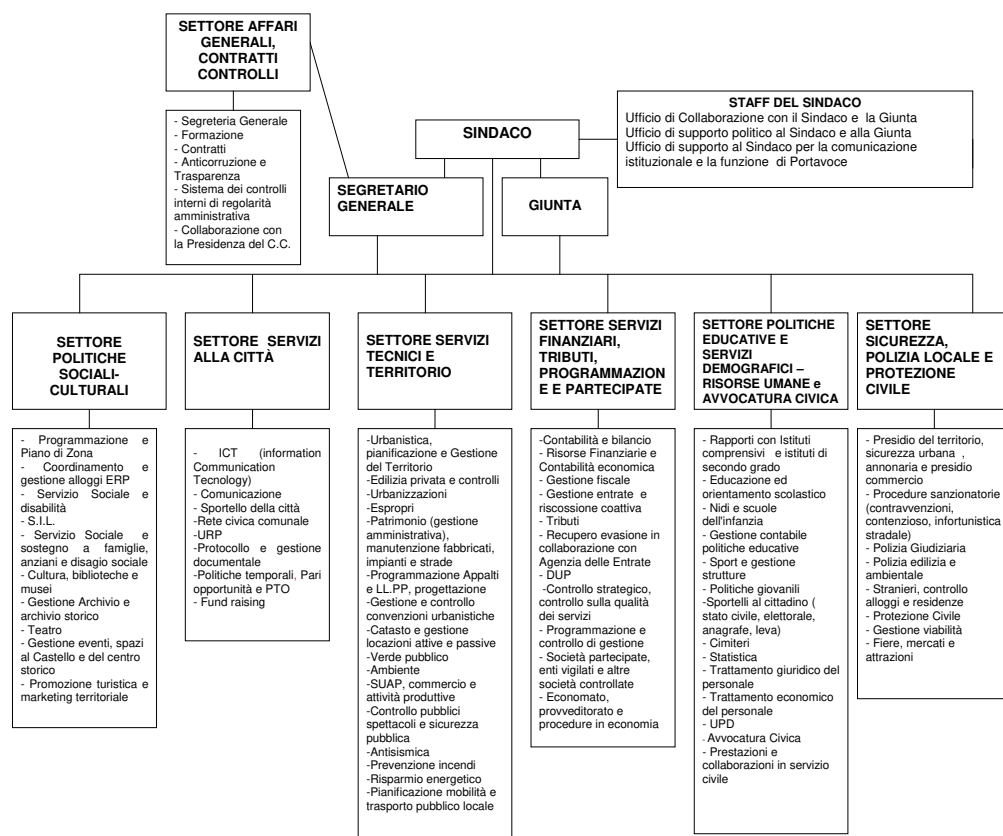
Unità di protocollazione: postazione di lavoro per la protocollazione dei documenti.

Versamento: è l'operazione con cui un ufficio, centrale o periferico, dello Stato, trasferisce periodicamente all'archivio di Stato deposito o storico competente per territorio la parte del proprio

archivio non più occorrente alla trattazione degli affari, dopo che siano state eseguite le operazioni di scarto. (Carucci)

Allegato 2 – Funzionigramma

Con deliberazione di G.C. n. 228 del 10/12/2020 e n. 21 del 04/02/2021 è stata approvata la revisione del funzionigramma connesso alla macrostruttura dell'Ente di seguito riportata:





**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Comunicazione dei dati di contatto del Responsabile della Protezione dei Dati - RPD

(art. 37, par. 7, RGPD e art. 28, c. 4 del D.Lgs. 51/2018)

A. Dati del soggetto che effettua la comunicazione

Il sottoscritto Cognome: Sacchi Nome: Daniela

E-mail: rtd@comune.vigevano.pv.it

nella sua qualità di

☐ rappresentante legale o ☒ delegato del rappresentante legale

Cognome: Ceffa Nome: Andrea

ai sensi dell'art. 37, par. 7, del RGPD comunica i seguenti dati e dichiara ☒ di aver preso visione dell'informativa sul trattamento dei dati personali e di essere consapevole che chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice in materia di protezione dei dati personali (*Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante*), salvo che ciò non costituisca più grave reato

A1. Tipo di comunicazione

Tipo di comunicazione dei dati di contatto del RPD:

☐ Nuova comunicazione

☒ Variazione di una comunicazione - Protocollo n.: 20180014022

☐ Revoca di una comunicazione - Protocollo n.:

B. Titolare/Responsabile del trattamento

1) Il Titolare/Responsabile del trattamento è:

- ☐ Censito nell'Indice nazionale dei domicili digitali delle imprese e dei professionisti
(INI-PEC www.inipec.gov.it - art. 6-bis Codice Amministrazione Digitale D.Lgs n. 82/2005)
- ☒ Censito nell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi
(IPA www.indicepa.gov.it - art. 6-ter Codice Amministrazione Digitale - D.Lgs n. 82/2005)
- ☐ Non censito in nessuno dei due precedenti indici

2) Dati del Titolare/Responsabile del trattamento:

Denominazione: Comune di Vigevano

Codice Fiscale: 85001870188

Stato: Italia

Provincia: Pavia

Comune: Vigevano CAP: 27029

Indirizzo: Corso Vittorio Emanuele II, 25

Telefono: 0381299247

E-mail:

PEC: protocollovigevano@pec.it

C. Responsabile della Protezione dei Dati

1) Tipo di designazione del Responsabile della Protezione dei Dati

☐ interno

☒ esterno

2) Il Responsabile della protezione dei dati è:

☒ persona fisica

☐ persona giuridica

3) Dati del Responsabile della Protezione dei Dati

Cognome: Ciappesoni

Nome: Andrea

P.IVA: 02468620139

4) Dati di contatto

Telefono: 0341700086

Cellulare:

E-mail: dpo@comune.vigevano.pv.it

PEC: ANDREA.CIAPPESONI@PEC.IT

D. Pubblicazione dei dati di contatto

I dati di contatto del RPD sono resi pubblici dal Titolare/Responsabile mediante:

- ☒ pubblicazione sul sito web (indicare l'indirizzo del sito su cui è possibile reperire l'informazione):
<https://www.comune.vigevano.pv.it/comune/amministrazione/responsabile-protezione-dati-rpd-dpo>
- ☐ Altro (specificare)



CITTÀ DI VIGEVANO

Provincia di Pavia

Verbale di deliberazione della Giunta Comunale n. 163 del 11/07/2019

L'anno duemiladiciannove, il giorno undici del mese di luglio alle ore 15:00 nella solita sala del Palazzo Municipale, osservate le modalità di legge, si è riunita la Giunta Comunale.

Presiede la seduta, nella sua qualità di Vice Sindaco, il Sig. CEFFA ANDREA che dichiara aperta la trattazione dell'oggetto sotto indicato.

OGGETTO:

NOMINA DEL RESPONSABILE PER LA TRANSIZIONE DIGITALE - ART. 17 DEL CODICE DELL'AMMINISTRAZIONE DIGITALE "CAD"

Risultano presenti alla trattazione dell'argomento in oggetto i Signori, dalle ore 15:50 alle ore 15:53

SALA ANDREA	Sindaco	Assente
CEFFA ANDREA	Vice Sindaco	Presente
ALESSANDRINO NUNZIATA	Assessore	Presente
AVALLE BRUNELLA	Assessore	Assente
GHIA RICCARDO	Assessore	Presente
MORESCHI ANTONIETTA	Assessore	Presente
PIGOLA LUIGI GIOVANNI MARIA	Assessore	Presente
ONORI GIULIO	Assessore	Presente

Presenti n. 6

Assenti n. 2

Partecipa il Segretario Generale SERGIO STEFANO.

LA GIUNTA COMUNALE

- Vista la proposta n. 2931 del 10/07/2019 di deliberazione relativa all'oggetto;
- Ritenuto di condividerne e farne propri i contenuti e le considerazioni ivi espressi;

Dato atto che:

- che ai sensi dell'art. 49 del D.Lgs 18 agosto 2000, n. 267, sono stati acquisiti ed allegati alla presente deliberazione di cui costituiscono parte integrante e sostanziale, i pareri favorevoli in ordine alla regolarità tecnica e contabile espressi rispettivamente dal Dirigente Responsabile del Settore Affari Generali, Contratti, Controlli e Advocatura Civica e dal Dirigente Responsabile del Settore Servizi Finanziari;

Visti:

- lo Statuto Comunale;
- il D.Lgs. n. 267/2000.

Con votazione unanime favorevole, espressa in forma palese

D E L I B E R A

1. Di approvare la proposta di deliberazione in premessa indicata, nel testo che si allega al presente provvedimento;
2. Di dare atto che nello stesso giorno in cui verrà pubblicato all'albo pretorio, il presente verbale sarà comunicato in elenco ai Capigruppo Consiliari ai sensi dell'art. 125 del D.Lgs. n. 267 del 18.08.2000;
3. Di demandare al Responsabile del Settore Affari Generali, Contratti, Controlli e Advocatura Civica tutti i successivi provvedimenti inerenti e conseguenti all'adozione del presente provvedimento;

Successivamente,

LA GIUNTA COMUNALE

• dichiara con successiva, separata ed unanime votazione favorevole il presente atto immediatamente eseguibile ai sensi dell'art. 134, comma 4, del D.Lgs. n. 267/2000

ALLEGATI:

- Proposta n. 2931 del 10/07/2019 del Settore Affari Generali, Contratti, Controlli e Advocatura Civica
- Parere regolarità tecnica ex art. 49 D.Lgs. n. 267/2000
- Parere regolarità contabile ex art. 49 D.Lgs. n. 267/2000

OGGETTO: NOMINA DEL RESPONSABILE PER LA TRANSIZIONE DIGITALE - ART. 17 DEL CODICE DELL'AMMINISTRAZIONE DIGITALE "CAD"

<i>Ufficio Proponente</i>	U.O.C. Segreteria Generale, Formazione, Sistema dei controlli interni di regolarità Amministrativa, Collaborazione con la Presidenza del C.C.
<i>Responsabile del procedimento</i>	Dott. Stefano Sergio
<i>Relatore</i>	Sindaco Andrea Sala

Premesso che il processo di riforma istituzionale avviato con Legge n. 124/2015 (cd Legge Madia) ha puntato sull'innovazione e digitalizzazione della Pubblica Amministrazione e in attuazione di ciò con D.lgs n.179/2016 è stato rivisto e aggiornato in modo significativo il Codice dell'Amministrazione Digitale CAD di cui al D.lgs n. 82/2005 e con D.lgs n. 217/2017 sono state previste ulteriori disposizioni integrative e correttive;

Dato atto che l'AGID (Agenzia per l'Italia Digitale) ha pubblicato il Piano Triennale per l'informatica nella Pubblica amministrazione 2017-2019, costruito sulla base di un modello strategico di evoluzione del sistema informativo della Pubblica amministrazione;

Visto che tale processo pone in capo ad ogni amministrazione pubblica la funzione di garantire l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione, centralizzando in capo ad un ufficio il compito di conduzione del processo di transizione alla modalità operativa digitale e dei correlati processi di riorganizzazione, nell'ottica di perseguire il generale obiettivo di realizzare un'amministrazione digitale e aperta, dotata di servizi facilmente utilizzabili e di qualità attraverso una maggiore efficienza ed economicità;

Visto in particolare l'art. 17 del CAD che disciplina la figura del Responsabile della transizione digitale, cui sono attribuiti importanti compiti di coordinamento e di impulso ai processi di reingegnerizzazione dei servizi;

Dato atto che alla figura in esame sono affidati i seguenti compiti:

- a) coordinamento strategico dello sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;
- b) indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;
- c) indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1;
- d) accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4;
- e) analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;
- f) cooperazione alla revisione della riorganizzazione dell'amministrazione ai fini di cui alla lettera e);

- g) indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;
- h) progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a soggetti giuridici mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;
- i) promozione delle iniziative attinenti l'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;
- j) pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità;

Dato atto che il Responsabile per la transizione alla modalità operativa digitale rappresenta il principale interlocutore di AgID per il monitoraggio e il coordinamento delle attività di trasformazione digitale e la norma prevede che sia dotato di adeguate competenze tecnologiche, di informatica giuridica e manageriali;

Ritenuta l'individuazione e la nomina del Responsabile per la transizione alla modalità operativa digitale un adempimento necessario e improrogabile;

Considerato che l'alta rilevanza dell'incarico in oggetto si connette necessariamente all'organizzazione dell'Amministrazione, assume significato strategico per l'attuazione delle direttive nazionali e comporta elevate responsabilità nei confronti dell'organo di vertice politico cui risponde direttamente (art. 17, comma 1-ter e 1-sexies CAD);

Considerato che in relazione al ruolo ricoperto nell'ente e alle capacità manageriali, necessarie per rivestire l'incarico, il Dirigente dott.ssa Daniela Sacchi, Responsabile del Settore Servizi alla Città che comprende il Servizio Informatico Comunale, rappresenta la figura idonea a rivestire il ruolo di Responsabile per la transizione digitale avvalendosi del supporto professionale del Funzionario Responsabile del SIC;

Considerato che in relazione alla complessità delle competenze richieste, il Responsabile della Transizione Digitale sarà supportato da tutti i dirigenti dell'Ente, e, ove occorra, coadiuvato da specifiche figure tecniche che consentano la copertura delle competenze richieste, lo svolgimento delle attività pianificate e che risponderà funzionalmente al Responsabile della Transizione Digitale, per le tematiche ed i compiti relativi alla transizione al digitale;

Dato atto che ai sensi dell'art. 49 del D.Lgs 18 agosto 2000, n. 267, sono stati acquisiti ed allegati alla presente proposta di cui costituiscono parte integrante e sostanziale, i pareri favorevoli in ordine alla regolarità tecnica e contabile espressi rispettivamente dal Dirigente Responsabile del Settore Affari Generali, Contratti, Controlli e Advocatura Civica e dal Dirigente Responsabile del Settore Servizi Finanziari;

Vista la circolare n. 3 del 1° ottobre 2018, adottata dal Ministro della Pubblica Amministrazione;

Visto il d.lgs. n. 267/2000 "Testo unico delle leggi sull'ordinamento degli enti locali";

Visto il vigente Statuto dell'Ente;

SI PROPONE ALLA GIUNTA COMUNALE DI DELIBERARE QUANTO SEGUE

1. le premesse formano parte integrante e sostanziale del presente provvedimento e vengono qui integralmente richiamate;
2. di nominare, ai sensi dell'art. 17, comma 1 del rinnovato D.Lgs 82/2005 - CAD – il Dirigente dott.ssa Daniela Sacchi, Responsabile del Settore Servizi alla Città, che comprende il Servizio Informatico Comunale (SIC), quale Responsabile per la transizione digitale, cui sono affidati i

compiti elencati nell'art. 17, comma 1 della medesima fonte di regolazione;

3. di demandare alla Dott.ssa Daniela Sacchi l'individuazione, con il supporto del Comitato dei Dirigenti, di figure tecniche anche appartenenti ad altri settori, con competenze idonee allo svolgimento delle attività che verranno programmate per la transizione alla modalità digitale e con modalità di volta in volta individuate;

4. di disporre che ai sensi dell'art. 17 comma 1 sexies il Responsabile della transizione alla modalità operativa digitale risponde al Sindaco, quale organo di vertice politico dell'amministrazione;

5. di disporre la pubblicazione del presente provvedimento all'Albo on line e nella Sezione Amministrazione Trasparente del sito web dell'Ente, ai sensi del d.lgs. n. 33/2013 e s.m.i. riguardante di obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni.

6. di disporre che il presente atto venga comunicato all'interessato e dallo stesso reso per accettazione.

CITTÀ DI VIGEVANO
Provincia di Pavia

Letto, approvato e sottoscritto digitalmente ai sensi dell'art. 21 D.L.gs n 82/2005 e s.m.i.

IL VICE SINDACO
CEFFA ANDREA

IL SEGRETARIO GENERALE
SERGIO STEFANO

DELIBERAZIONE DELLA G.C. N. 163 del 11/07/2019

Proposta N. 2019 / 2931

U.O.C. Segreteria Generale, Formazione, Sistema dei controlli interni di regolarità Amministrativa,
Collaborazione con la Presidenza del C.C.

OGGETTO: NOMINA DEL RESPONSABILE PER LA TRANSIZIONE DIGITALE - ART. 17 DEL
CODICE DELL'AMMINISTRAZIONE DIGITALE "CAD"

PARERE IN ORDINE ALLA REGOLARITA' TECNICA

Visto con parere FAVOREVOLE, art. 49 comma 1 del D.Lgs 267 del 18/08/2000.

Lì, 10/07/2019

IL DIRIGENTE
SERGIO STEFANO
(Sottoscritto digitalmente ai sensi
dell'art. 21 D.L.gs n 82/2005 e s.m.i.)

Proposta N. 2019 / 2931

U.O.C. Segreteria Generale, Formazione, Sistema dei controlli interni di regolarità Amministrativa,
Collaborazione con la Presidenza del C.C.

OGGETTO: NOMINA DEL RESPONSABILE PER LA TRANSIZIONE DIGITALE - ART. 17 DEL
CODICE DELL'AMMINISTRAZIONE DIGITALE "CAD"

PARERE IN ORDINE ALLA REGOLARITA' CONTABILE

Parere di regolarità contabile, FAVOREVOLE, art. 49 comma 1 del D.Lgs 267 del
18/08/2000.

Lì, 11/07/2019

IL DIRIGENTE
GENZINI LAURA
(Sottoscritto digitalmente ai sensi
dell'art. 21 D.L.gs n 82/2005 e s.m.i.)



CITTA' DI VIGEVANO

Unita' Operativa U.O.C. Segreteria Generale, Formazione, Sistema dei controlli interni di regolarità Amministrativa, Collaborazione con la Presidenza del C.C.

Certificato di Esecutività

Deliberazione N. 163 del 11/07/2019

Oggetto: NOMINA DEL RESPONSABILE PER LA TRANSIZIONE DIGITALE - ART. 17 DEL CODICE DELL'AMMINISTRAZIONE DIGITALE "CAD".

Si certifica che, ai sensi dell'art. 134, comma 4, del D.lgs. n. 267/2000 e s.m.i. la presente deliberazione è immediatamente eseguibile

Data Esecutività: 11/07/2019

Vigevano li, 02/08/2019

Sottoscritta
(ZANETTI MARCELLO)
con firma digitale



CITTÀ DI VIGEVANO

Certificato di Avvenuta Pubblicazione

Deliberazione della Giunta Comunale
N. 163 del 11/07/2019

Oggetto: NOMINA DEL RESPONSABILE PER LA TRANSIZIONE DIGITALE - ART. 17 DEL CODICE DELL'AMMINISTRAZIONE DIGITALE "CAD".

Si certifica che la presente deliberazione è stata pubblicata all'Albo Pretorio on-line di questo Comune per quindici giorni consecutivi a decorrere dal 17/07/2019 ai sensi del 1° comma dell'art. 124 del D.lgs. n. 267/2000 e s.m.i. e contestualmente comunicata ai Capigruppo Consiliari ai sensi dell'art. 125 del D.lgs. n. 267/2000 e s.m.i..

Li, 02/08/2019

L'INCARICATO DELLA PUBBLICAZIONE
ZANETTI MARCELLO
(Sottoscritto digitalmente
ai sensi dell'art. 21 D.L.gs. n. 82/2005 e s.m.i.)

Deliberazione di Giunta Comunale N. 163 del 11/07/2019

Allegato 4 – Documenti non soggetti a protocollazione e Registrazioni particolari

Alcune tipologie di documento non sono soggette a protocollazione.
Di seguito l'elenco:

- gazzette ufficiali
- bollettini ufficiali e notiziari della pubblica amministrazione
- note di ricezione delle circolari e altre disposizioni
- materiale statistico
- atti preparatori interni
- giornali, riviste, materiale pubblicitario, inviti a manifestazioni
- stampe varie, plichi di libri
- auguri per festività
- richieste di protocollazione di autocertificazioni e/o dichiarazioni sostitutive ed in genere di scritti avulsi da qualsiasi procedimento amministrativo di competenza dell'Ente

Registrazioni particolari

L'elenco seguente elenca i documenti soggetti a registrazione particolare soggetti ad appositi repertori che identificano univocamente l'atto, tramite un codice progressivo annuale.

Elenco registrazioni particolari

- Deliberazioni del Consiglio Comunale
- Deliberazione della Giunta Comunale
- Provvedimenti di diversa natura del Sindaco:
- ordinanze
- decreti
- ordini di servizio
- incarichi di direzione
- Determinazioni dirigenziali
- Decreti dirigenziali
- Ordinanze dirigenziali
- Impegni di spesa
- Atti pubblicati all'albo pretorio
- Atti depositati presso la casa comunale
- Notificazioni da parte di soggetti legittimati
- Determinazioni Posizioni Organizzative
- Contratti
- Iscrizione albo associazioni
- Autorizzazioni sanitarie

- Autorizzazioni all'attività
- Autorizzazioni di pubblica sicurezza
- Verbali, sopralluoghi e accertamenti
- verbali incidenti stradali
- Permessi temporanei di accesso alla ZTL
- Mandati di pagamento
- Reversali
- Disposizioni di liquidazione
- Pratiche SUAP in quanto tutti gli atti e documenti ricevuti ed inviati tramite lo Sportello Impresa in Un Giorno, sono assoggettate alla registrazione del protocollo informatico del portale governativo <http://www.impresainungiorno.gov.it>, conforme alle specifiche tecniche di cui al combinato disposto del Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 "Regole tecniche per il protocollo informatico" e del Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 "Registrazione di protocollo".

A Relativamente agli atti demografici, a seguito dell'attivazione di ANPR i movimenti Migratori AP4 sono protocollati solo se antecedenti al passaggio in ANPR (Anagrafe Nazionale Popolazione Residente).

Titolario

Classificazione		Dal	Al
01	AMMINISTRAZIONE GENERALE	28/12/2012	
01-01	LEGISLAZIONE E CIRCOLARI ESPLICATIVE	28/12/2012	
01-02	DENOMINAZIONE, TERRITORIO E CONFINI, CIRCOSCRIZIONI DI DECENTRAMENTO, TOPONOMASTICA	28/12/2012	
01-03	STATUTO	28/12/2012	
01-04	REGOLAMENTI	28/12/2012	
01-05	STEMMA, GONFALONE, SIGILLO	28/12/2012	
01-06	ARCHIVIO GENERALE	28/12/2012	
01-07	SISTEMA INFORMATIVO	28/12/2012	
01-08	INFORMAZIONI E RELAZIONI CON IL PUBBLICO	28/12/2012	
01-09	POLITICA DEL PERSONALE, ORDINAMENTO DEGLI UFFICI E DEI SERVIZI	28/12/2012	
01-10	RELAZIONI CON LE ORGANIZZAZIONI SINDACALI E DI RAPPRESENTANZA DEL PERSONALE	28/12/2012	
01-11	CONTROLLI ESTERNI	28/12/2012	
01-12	EDITORIA E ATTIVITA' INFORMATIVO-PROMOZIONALE INTERNA ED ESTERNA	28/12/2012	
01-13	CERIMONIALE, ATTIVITA' DI RAPPRESENTANZA, ONORIFICENZE E RICONOSCIMENTI	28/12/2012	
01-14	INTERVENTI DI CARATTERE POLITICO E UMANITARIO, RAPPORTI ISTITUZIONALI	28/12/2012	
01-15	FORME ASSOCIATIVE PER L'ESERCIZIO DI FUNZIONI E SERVIZI	28/12/2012	
01-16	AREA E CITTA' METROPOLITANA	28/12/2012	
01-17	ASSOCIAZIONISMO E PARTECIPAZIONE	28/12/2012	
02	ORGANI DI GOVERNO, GESTIONE, CONTROLLO, CONSULENZA E GARANZIA	28/12/2012	
02-01	SINDACO	28/12/2012	
02-02	VICE-SINDACO	28/12/2012	

Classificazione		Dal	Al
02-03	CONSIGLIO	28/12/2012	
02-04	PRESIDENTE DEL CONSIGLIO	28/12/2012	
02-05	CONFERENZA DEI CAPIGRUPPO E COMMISSIONI DEL CONSIGLIO	28/12/2012	
02-06	GRUPPI CONSILIARI	28/12/2012	
02-07	GIUNTA	28/12/2012	
02-08	COMMISSARIO PREFETTIZIO E STRAORDINARIO	28/12/2012	
02-09	SEGRETARIO E VICE-SEGRETARIO	28/12/2012	
02-10	DIRETTORE GENERALE E DIRIGENZA	28/12/2012	
02-11	REVISORI DEI CONTI	28/12/2012	
02-12	DIFENSORE CIVICO	28/12/2012	
02-13	COMMISSARIO AD ACTA	28/12/2012	
02-14	ORGANI DI CONTROLLO INTERNI	28/12/2012	
02-15	ORGANI CONSULTIVI	28/12/2012	
02-16	CONSIGLI CIRCOSCRIZIONALI	28/12/2012	
02-17	PRESIDENTI DEI CONSIGLI CIRCOSCRIZIONALI	28/12/2012	
02-18	ORGANI ESECUTIVI CIRCOSCRIZIONALI	28/12/2012	
02-19	COMMISSIONI DEI CONSIGLI CIRCOSCRIZIONALI	28/12/2012	
02-20	SEGRETARI DELLE CIRCOSCRIZIONI	28/12/2012	
02-21	COMMISSARIO AD ACTA DELLE CIRCOSCRIZIONI	28/12/2012	
02-22	CONFERENZA DEI PRESIDENTI DI QUARTIERE	28/12/2012	
03	RISORSE UMANE	28/12/2012	
03-01	CONCORSI, SELEZIONI, COLLOQUI	28/12/2012	
03-02	ASSUNZIONI E CESSAZIONI	28/12/2012	
03-03	COMANDI E DISTACCHI, MOBILITA'	28/12/2012	
03-04	ATTRIBUZIONE DI FUNZIONI, ORDINI DI SERVIZIO E MISSIONI	28/12/2012	
03-05	INQUADRAMENTI E APPLICAZIONE CONTRATTI	28/12/2012	

Riproduzione cartacea del documento informatico sottoscritto digitalmente da

Classificazione		Dal	Al
COLLETTIVI DI LAVORO			
03-06	RETRIBUZIONI E COMPENSI	28/12/2012	
03-07	ADEMPIMENTI FISCALI, CONTRIBUTIVI E ASSICURATIVI	28/12/2012	
03-08	TUTELA DELLA SALUTE E SICUREZZA SUL LUOGO DI LAVORO	28/12/2012	
03-09	DICHIARAZIONI DI INFERMITA' ED EQUO INDENNIZZO	28/12/2012	
03-10	INDENNITA' DI PREMIO DI SERVIZIO E TRATTAMENTO DI FINE RAPPORTO, QUIESCENZA	28/12/2012	
03-11	SERVIZI AL PERSONALE SU RICHIESTA	28/12/2012	
03-12	ORARIO DI LAVORO, PRESENZE E ASSENZE	28/12/2012	
03-13	GIUDIZI, RESPONSABILITA' E PROVVEDIMENTI DISCIPLINARI	28/12/2012	
03-14	FORMAZIONE E AGGIORNAMENTO PROFESSIONALE	28/12/2012	
03-15	COLLABORATORI ESTERNI	28/12/2012	
04	RISORSE FINANZIARIE E PATRIMONIALI	28/12/2012	
04-01	BILANCIO PREVENTIVO E PIANO ESECUTIVO DI GESTIONE (PEG)	28/12/2012	
04-02	GESTIONE DEL BILANCIO E DEL PEG (CON EVENTUALI VARIAZIONI)	28/12/2012	
04-03	GESTIONE DELLE ENTRATE: ACCERTAMENTO, RISCOSSIONE, VERSAMENTO	28/12/2012	
04-04	GESTIONE DELLA SPESA: IMPEGNO, LIQUIDAZIONE, ORDINAZIONE E PAGAMENTO	28/12/2012	
04-05	PARTECIPAZIONI FINANZIARIE	28/12/2012	
04-06	RENDICONTO DELLA GESTIONE: ADEMPIMENTI E VERIFICHE CONTABILI	28/12/2012	
04-07	ADEMPIMENTI FISCALI, CONTRIBUTIVI E ASSICURATIVI	28/12/2012	
04-08	BENI IMMOBILI	28/12/2012	
04-09	BENI MOBILI	28/12/2012	
04-10	ECONOMATO	28/12/2012	
04-11	OGGETTI SMARRITI E RECUPERATI	28/12/2012	

Riproduzione cartacea del documento informatico sottoscritto digitalmente da

Classificazione		Dal	Al
04-12	TESORERIA	28/12/2012	
04-13	CONCESSIONARI ED ALTRI INCARICATI DELLA RISCOSSIONE DELLE ENTRATE	28/12/2012	
04-14	PUBBLICITA' E PUBBLICHE AFFISSIONI	28/12/2012	
05	AFFARI LEGALI	28/12/2012	
05-01	CONTENZIOSO	28/12/2012	
05-02	RESPONSABILITA' CIVILE E PATRIMONIALE VERSO TERZI. ASSICURAZIONI	28/12/2012	
05-03	PARERI E CONSULENZE	28/12/2012	
06	PIANIFICAZIONE E GESTIONE DEL TERRITORIO	28/12/2012	
06-01	URBANISTICA: PIANO REGOLATORE GENERALE E VARIANTI	28/12/2012	
06-02	URBANISTICA: STRUMENTI DI ATTUAZIONE DEL PIANO REGOLATORE GENERALE	28/12/2012	
06-03	EDILIZIA PRIVATA	28/12/2012	
06-04	EDILIZIA PUBBLICA	28/12/2012	
06-05	OPERE PUBBLICHE	28/12/2012	
06-06	CATASTO	28/12/2012	
06-07	VIABILITA'	28/12/2012	
06-08	SERVIZIO IDRICO INTEGRATO, LUCE, GAS, TRASPORTI PUBBLICI, GESTIONE DEI RIFIUTI E ALTRI SERVIZI	28/12/2012	
06-09	AMBIENTE: AUTORIZZAZIONI, MONITORAGGIO E CONTROLLO	28/12/2012	
06-10	PROTEZIONE CIVILE ED EMERGENZE	28/12/2012	
07	SERVIZI ALLA PERSONA	28/12/2012	
07-01	DIRITTO ALLO STUDIO E SERVIZI	28/12/2012	
07-02	ASILI NIDO E SCUOLA MATERNA	28/12/2012	
07-03	PROMOZIONE E SOSTEGNO DELLE ISTITUZIONI DI ISTRUZIONE E DELLA LORO ATTIVITA'	28/12/2012	
07-04	ORIENTAMENTO PROFESSIONALE, EDUCAZIONE DEGLI ADULTI, MEDIAZIONE CULTURALE	28/12/2012	

Classificazione		Dal	Al
07-05	ISTITUTI CULTURALI (MUSEI, BIBLIOTECHE, TEATRI, SCUOLA COMUNALE DI MUSICA, ETC.)	28/12/2012	
07-06	ATTIVITA' ED EVENTI CULTURALI	28/12/2012	
07-07	ATTIVITA' ED EVENTI SPORTIVI	28/12/2012	
07-08	PIANIFICAZIONE E ACCORDI STRATEGICI CON ENTI PUBBLICI E PRIVATI E CON IL VOLONTARIATO SOCIALE	28/12/2012	
07-09	PREVENZIONE, RECUPERO E REINTEGRAZIONE DEI SOGGETTI A RISCHIO	28/12/2012	
07-10	INFORMAZIONE, CONSULENZA ED EDUCAZIONE CIVICA	28/12/2012	
07-11	TUTELA E CURATELA DI INCAPACI	28/12/2012	
07-12	ASSISTENZA DIRETTA E INDIRETTA, BENEFICI ECONOMICI	28/12/2012	
07-13	ATTIVITA' RICREATIVA E DI SOCIALIZZAZIONE	28/12/2012	
07-14	POLITICHE PER LA CASA	28/12/2012	
07-15	POLITICHE PER IL SOCIALE	28/12/2012	
08	ATTIVITA' ECONOMICHE	28/12/2012	
08-01	AGRICOLTURA E PESCA	28/12/2012	
08-02	ARTIGIANATO	28/12/2012	
08-03	INDUSTRIA	28/12/2012	
08-04	COMMERCIO	28/12/2012	
08-05	FIERE E MERCATI	28/12/2012	
08-06	ESERCIZI TURISTICI E STRUTTURE RICETTIVE	28/12/2012	
08-07	PROMOZIONE E SERVIZI	28/12/2012	
09	POLIZIA LOCALE E SICUREZZA PUBBLICA	28/12/2012	
09-01	PREVENZIONE ED EDUCAZIONE STRADALE	28/12/2012	
09-02	POLIZIA STRADALE	28/12/2012	
09-03	INFORMATIVE	28/12/2012	
09-04	SICUREZZA E ORDINE PUBBLICO	28/12/2012	

Riproduzione cartacea del documento informatico sottoscritto digitalmente da

Classificazione		Dal	Al
10	TUTELA DELLA SALUTE	28/12/2012	
10-01	SALUTE E IGIENE PUBBLICA	28/12/2012	
10-02	TRATTAMENTO SANITARIO OBBLIGATORIO	28/12/2012	
10-03	FARMACIE	28/12/2012	
10-04	ZOOPROFILASSI VETERINARIA	28/12/2012	
10-05	RANDAGISMO ANIMALE E RICOVERI	28/12/2012	
11	SERVIZI DEMOGRAFICI	28/12/2012	
11-01	STATO CIVILE	28/12/2012	
11-02	ANAGRAFE E CERTIFICAZIONI	28/12/2012	
11-03	CENSIMENTI	28/12/2012	
11-04	POLIZIA MORTUARIA E CIMITERI	28/12/2012	
12	ELEZIONI E INIZIATIVE POPOLARI	28/12/2012	
12-01	ALBI ELETTORALI	28/12/2012	
12-02	LISTE ELETTORALI	28/12/2012	
12-03	ELEZIONI	28/12/2012	
12-04	REFERENDUM	28/12/2012	
12-05	ISTANZE, PETIZIONI E INIZIATIVE POPOLARI	28/12/2012	
13	AFFARI MILITARI	28/12/2012	
13-01	LEVA	28/12/2012	
13-02	RUOLI MATRICOLARI	28/12/2012	
13-03	CASERME, ALLOGGI E SERVITU' MILITARI	28/12/2012	
13-04	REQUISIZIONI PER UTILITA' MILITARI	28/12/2012	
14	OGGETTI DIVERSI	28/12/2012	



Regolamento

dell'accesso civico e dell'accesso agli atti

In attuazione delle *Linee guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'articolo 5 comma 2 del d.lgs. 33/2013* (ANAC deliberazione 28 dicembre 2016 numero 1309)

Approvato con deliberazione di Consiglio Comunale n. 69 del 11/10/2019

SOMMARIO

TITOLO I – Principi generali	5
Articolo 1 - Oggetto	5
Articolo 2 – Trasparenza	5
TITOLO II – Accesso civico	6
Articolo 3 – Accesso civico semplice	6
Articolo 4 – Domanda di accesso semplice	6
Articolo 5 – Segnalazione del RPCT	6
TITOLO III – Accesso generalizzato.....	7
Articolo 6 – Accesso civico generalizzato	7
Articolo 7 – Domanda di accesso generalizzato	7
Articolo 8 – Domanda inammissibili.....	7
Articolo 9 - Esclusioni.....	8
Articolo 10 - Limiti a tutela di interessi pubblici	8
Articolo 11 - Limiti a tutela di interessi privati.....	8
Articolo 12 - Controinteressati	9
Articolo 13 - Domanda accolta	9
Articolo 14 - Domanda respinta.....	9
Articolo 15 - Domanda di riesame.....	10
Articolo 16 - Difensore civico	10
Articolo 17 - Ricorsi	10
Articolo 18 - Tutela dei controinteressati.....	10
Articolo 19 - Monitoraggio	11
Articolo 20 - Registro	11
TITOLO IV – Accesso agli atti.....	12
Articolo 21- Accesso agli atti amministrativi.....	12
Articolo 22 – Esclusioni e limitazioni	12
Articolo 23 – Domanda di accesso agli atti amministrativi.....	13
Articolo 24 – Controinteressati all’accesso agli atti	13
Articolo 25 - Accesso informale	14
Articolo 26 - Accesso formale.....	14
Articolo 27 – Domanda accolta e modalità di accesso.	14
Articolo 28 – Domanda respinta o differita.....	15
Articolo 29 - Tutele e ricorsi	15
TITOLO V – Norme finali.....	16
Articolo 30 - Rinvio dinamico	16
Articolo 31 - Entrata in vigore, abrogazioni e pubblicità	16

TITOLO I - Principi generali

Articolo 1 - Oggetto

1. Questo regolamento disciplina e organizza l'accesso civico semplice, l'accesso civico generalizzato, secondo l'articolo 5 commi 1 e 2 del decreto legislativo 33/2013 come modificato dal decreto legislativo 97/2016 (di seguito "*Decreto trasparenza*") e l'accesso agli atti amministrativi secondo gli articoli 22 e seguenti della legge 241/1990.

Articolo 2 - Trasparenza

1. La trasparenza è l'accessibilità totale ai dati e ai documenti detenuti dall'ente, allo scopo di tutelare i diritti dei cittadini, promuovere la partecipazione degli interessati all'attività amministrativa e favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche.

2. La trasparenza è realizzata attraverso la pubblicazione di informazioni, dati e documenti in "*Amministrazione trasparente*" e consentendo l'accesso civico e agli atti amministrativi.

TITOLO II – Accesso civico

Articolo 3 – Accesso civico semplice

1. Chiunque, indipendentemente dall'essere cittadino italiano o residente nel territorio dello Stato, ha il diritto di chiedere documenti, informazioni e dati che questo ente deve pubblicare in "*Amministrazione trasparente*" qualora sia stata omessa la pubblicazione.

Articolo 4 – Domanda di accesso semplice

1. La domanda di accesso civico semplice non è motivata ma deve identificare i dati, le informazioni o i documenti richiesti.
2. La domanda, presentata all'ufficio Protocollo dell'ente, in forma scritta o via PEC, è rivolta al responsabile della prevenzione della corruzione e della trasparenza.
3. Il procedimento deve concludersi entro trenta giorni con un provvedimento espresso e motivato del responsabile della prevenzione della corruzione e della trasparenza.
4. In caso di accoglimento, il responsabile della prevenzione della corruzione e della trasparenza sovrintende alla pubblicazione in "*Amministrazione trasparente*" delle informazioni e dei documenti omessi e comunica al richiedente l'avvenuta pubblicazione, indicandogli il relativo collegamento ipertestuale.

Articolo 5 – Segnalazione del RPCT

1. Qualora la domanda di accesso civico semplice sia fondata e, quindi, evidenzi un inadempimento, anche parziale, di obblighi di pubblicazione, il Responsabile della prevenzione della corruzione e della trasparenza valuta l'opportunità di segnalare l'accaduto all'ufficio competente per i procedimenti disciplinari, al sindaco e all'OIV.

TITOLO III – Accesso generalizzato

Articolo 6 – Accesso civico generalizzato

1. Chiunque, indipendentemente dall'essere cittadino italiano o residente nel territorio dello Stato, ha diritto di accedere ai dati e ai documenti detenuti da questo ente, ulteriori rispetto a quelli oggetto di pubblicazione obbligatoria, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti.
2. L'accesso civico generalizzato ha lo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico.

Articolo 7 – Domanda di accesso generalizzato

1. La domanda di accesso civico generalizzato non è necessariamente motivata, ma identifica i dati, le informazioni o i documenti richiesti.
2. La domanda, presentata all'ufficio Protocollo dell'ente, in forma scritta o via PEC, è rivolta all'ufficio che detiene i dati, le informazioni e i documenti. L'ufficio la inoltra, per conoscenza, al Responsabile della prevenzione della corruzione e della trasparenza.
3. Il rilascio di dati o documenti è gratuito, salvo il rimborso del costo sostenuto per la riproduzione su supporti materiali, come previsto dall'apposita deliberazione di Giunta Comunale di approvazione tariffe annuali.
4. Il procedimento deve concludersi entro trenta giorni con un provvedimento espresso e motivato del responsabile dell'ufficio che detiene i dati, le informazioni e i documenti.

Articolo 8 – Domanda inammissibili

1. Non sono ammissibili domande generiche che non individuino i dati, i documenti e le informazioni richieste con riferimento, almeno, alla loro natura e al loro oggetto¹.
2. Non sono ammissibili domande meramente esplorative volte semplicemente a scoprire di quali informazioni l'ente dispone.
3. Non sono nemmeno ammissibili domande di accesso per un numero manifestamente irragionevole di documenti, imponendo un carico di lavoro tale da paralizzare, o rallentare eccessivamente, il buon funzionamento dell'ente².
4. Resta escluso che, per rispondere alla richiesta di accesso civico generalizzato, l'ente abbia l'obbligo di formare, raccogliere o altrimenti procurarsi informazioni che non siano in suo possesso. L'ente non ha l'obbligo di rielaborare dati ai fini dell'accesso

¹ Si veda il paragrafo 4.2 della deliberazione ANAC 28 dicembre 2016 numero 1309 *Linee guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'articolo 5 comma 2 del d.lgs. 33/2013*.

² Corte di Giustizia UE, Tribunale prima sezione ampliata, 13 aprile 2005 causa T 2/03.

generalizzato, ma deve consentire l'accesso ai documenti nei quali siano contenute le informazioni già detenute e gestite dall'ente stesso³.

Articolo 9 - Esclusioni

1. L'accesso civico generalizzato è sempre *escluso* nei casi di segreto di Stato e negli altri casi di divieti di accesso o divulgazione previsti dalla legge, ivi compresi i casi in cui l'accesso è subordinato dalla disciplina vigente al rispetto di specifiche condizioni, modalità o limiti, inclusi quelli di cui all'articolo 24, comma 1, della legge 241/1990.

Articolo 10 - Limiti a tutela di interessi pubblici

1. L'accesso civico generalizzato è *rifiutato* se il diniego è necessario per evitare un pregiudizio concreto alla tutela di uno degli *interessi pubblici* inerenti a:

- a) la sicurezza pubblica e l'ordine pubblico;
- b) la sicurezza nazionale;
- c) la difesa e le questioni militari;
- d) le relazioni internazionali;
- e) la politica e la stabilità finanziaria ed economica dello Stato;
- f) la conduzione di indagini sui reati e il loro perseguimento;
- g) il regolare svolgimento di attività ispettive.

2. I limiti di cui sopra si applicano unicamente per il periodo nel quale la protezione è giustificata in relazione alla natura del dato. L'accesso non può essere negato ove, per la tutela degli interessi pubblici di cui sopra, sia sufficiente fare ricorso al differimento.

Articolo 11 - Limiti a tutela di interessi privati

1. L'accesso civico generalizzato è *rifiutato* se il diniego è necessario per evitare un pregiudizio concreto alla tutela di uno dei seguenti *interessi privati*:

- a) la protezione dei dati personali delle sole persone fisiche;
- b) la libertà e la segretezza della corrispondenza;
- c) gli interessi economici e commerciali di una persona fisica o giuridica, ivi compresi la proprietà intellettuale, il diritto d'autore e i segreti commerciali.

2. I limiti di cui sopra si applicano unicamente per il periodo nel quale la protezione è giustificata in relazione alla natura del dato. L'accesso non può essere negato ove, per la tutela degli interessi privati di cui sopra, sia sufficiente fare ricorso al differimento.

³ Previsione della deliberazione ANAC 28 dicembre 2016 numero 1309 paragrafo 4.2.

3. La domanda di accesso civico generalizzato è accolta oscurando i dati personali contenuti nei documenti richiesti⁴.

Articolo 12 - Controinteressati

1. Sono controinteressati coloro che dall'accoglimento della domanda di accesso civico generalizzato possono ricevere una lesione ad uno degli interessi privati elencati all'articolo precedente.
2. Qualora siano individuati dei controinteressati, l'ufficio procedente comunica loro copia della domanda d'accesso generalizzato, con raccomandata AR o via PEC.
3. Entro dieci giorni dalla ricezione della comunicazione, i controinteressati possono presentare una motivata opposizione, anche via PEC, alla richiesta di accesso.
4. Accertata la ricezione della comunicazione da parte dei controinteressati, decorso il termine di dieci giorni l'ufficio provvede comunque sulla richiesta.
5. A decorrere dalla comunicazione ai controinteressati, il termine di trenta giorni per concludere il procedimento rimane sospeso fino all'eventuale opposizione degli stessi.

Articolo 13 - Domanda accolta

1. Se la domanda di accesso generalizzato viene accolta, l'ufficio trasmette tempestivamente al richiedente i dati e i documenti.
2. Nel caso la domanda sia accolta nonostante l'opposizione di controinteressati, salvi i casi di comprovata indifferibilità, l'ufficio comunica la decisione motivata di accoglimento agli stessi controinteressati. Successivamente, ma non prima di quindici giorni dalla ricezione della comunicazione di accoglimento da parte dei controinteressati, l'ufficio trasmette al richiedente i dati e i documenti richiesti.

Articolo 14 - Domanda respinta

1. Se la domanda di accesso generalizzato è respinta o differita, la decisione deve essere motivata unicamente con riferimento alle cause di inammissibilità della domanda o di esclusione dell'accesso, oppure ai limiti a tutela di interessi pubblici e privati previsti dagli articoli precedenti e dal *Decreto trasparenza*.
2. L'ufficio trasmette tempestivamente e, comunque, entro il termine di conclusione del procedimento, il provvedimento di decisione al richiedente e ai controinteressati.

⁴ Si veda il paragrafo 8.1. pagina 21 della deliberazione ANAC 28 dicembre 2016 numero 1309.

Articolo 15 - Domanda di riesame

1. Nei casi di diniego totale o parziale dell'accesso o di mancata risposta entro il termine di conclusione del procedimento il richiedente può presentare richiesta di riesame al Responsabile della prevenzione della corruzione e della trasparenza.
2. Il Responsabile della prevenzione della corruzione e della trasparenza decide, in merito alla domanda di riesame, entro il termine di venti giorni con provvedimento motivato.
3. Se l'accesso civico generalizzato è stato negato o differito per tutelare dati personali, il Responsabile della prevenzione della corruzione e della trasparenza deve acquisire il parere preventivo del Garante per la protezione dei dati personali, il quale si pronuncia entro il termine di dieci giorni dalla richiesta.
4. A decorrere dalla comunicazione al Garante, il termine per l'adozione del provvedimento da parte del Responsabile della prevenzione della corruzione e della trasparenza rimane sospeso, fino alla ricezione del parere del Garante e comunque per un periodo non superiore ai predetti dieci giorni.

Articolo 16 - Difensore civico

1. Contro la decisione dell'ufficio o, in caso di richiesta di riesame, contro la decisione del Responsabile della prevenzione della corruzione e della trasparenza, il richiedente può presentare ricorso al Difensore civico regionale.
2. A norma di legge, il Difensore civico si pronuncia entro trenta giorni. Se il difensore civico ritiene illegittimo il diniego o il differimento, ne informa il richiedente e lo comunica all'ente.
3. Se l'ufficio non conferma il diniego o il differimento entro trenta giorni dal ricevimento della comunicazione del Difensore civico, l'accesso è consentito.

Articolo 17 - Ricorsi

1. A norma di legge, contro la decisione dell'ufficio o, in caso di richiesta di riesame, contro la decisione del Responsabile della prevenzione della corruzione e della trasparenza, il richiedente può sempre proporre ricorso al Tribunale amministrativo regionale.

Articolo 18 - Tutela dei controinteressati

1. I controinteressati dispongono delle stesse tutele che l'ordinamento riconosce al richiedente.
2. In caso di accoglimento della domanda di accesso, i controinteressati possono presentare richiesta di riesame al Responsabile della prevenzione della corruzione e della trasparenza, ricorso al difensore civico, oppure ricorso al Tribunale amministrativo regionale.

Articolo 19 - Monitoraggio

1. Gli uffici comunicano al Responsabile della prevenzione della corruzione e della trasparenza gli esiti delle domande di accesso generalizzato.
2. In ogni caso, il Responsabile della prevenzione della corruzione e della trasparenza può sempre verificare presso gli uffici l'esito delle istanze e le decisioni assunte.

Articolo 20 - Registro

1. E' istituito il *"registro delle domande di accesso: documentale, civico semplice e civico generalizzato"*.
2. Il registro reca, quali indicazioni minime essenziali: l'oggetto della domanda d'accesso generalizzato, la data di registrazione al protocollo, il relativo esito con indicazione della data.
3. Il registro è pubblicato, oscurando eventuali dati personali, e aggiornato ogni sei mesi in *"Amministrazione trasparente"*, *"Altri contenuti – accesso civico"*.

TITOLO IV - Accesso agli atti

Articolo 21- Accesso agli atti amministrativi

1. Tutti i soggetti privati, compresi quelli portatori di interessi pubblici o diffusi, che abbiano un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata a uno o più documenti amministrativi hanno il diritto di prendere visione e di estrarre copia di tali documenti.
2. A norma della legge 241/1990, l'accesso ai documenti amministrativi costituisce principio generale dell'attività amministrativa al fine di favorire la partecipazione e di assicurarne l'imparzialità e la trasparenza.

Articolo 22 - Esclusioni e limitazioni

1. Il diritto di accesso agli atti amministrativi è escluso:
 - a) per i documenti coperti da segreto di Stato e nei casi di segreto o di divieto di divulgazione espressamente previsti dalla legge, da regolamento governativo e dalle pubbliche amministrazioni;
 - b) nei procedimenti tributari, per i quali restano ferme le particolari norme che li regolano;
 - c) nei confronti dell'attività della pubblica amministrazione diretta all'emanazione di atti normativi, amministrativi generali, di pianificazione e di programmazione, per i quali restano ferme le particolari norme che ne regolano la formazione;
 - d) nei procedimenti selettivi, nei confronti dei documenti amministrativi contenenti informazioni di carattere psicoattitudinale relativi a terzi.
2. L'accesso ai documenti amministrativi non può essere negato qualora sia sufficiente fare ricorso al differimento.
3. Deve essere garantito ai richiedenti l'accesso ai documenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i loro interessi giuridici.
4. Nel caso di documenti contenenti categorie particolari di dati personali e dati relativi a condanne penali e reati, l'accesso è consentito nei limiti in cui sia strettamente indispensabile. Quando l'accesso concerne dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale⁵.

⁵ Si veda l'articolo 60 del decreto legislativo 196/2003 *Codice in materia di protezione dei dati personali*.

Articolo 23 – Domanda di accesso agli atti amministrativi

1. La domanda di accesso agli atti amministrativi è obbligatoriamente motivata, pena l'inammissibilità, e identifica i documenti richiesti.
2. Il diritto di accesso agli atti è esercitabile per i soli documenti amministrativi materialmente esistenti al momento della richiesta e detenuti dall'ente. Gli uffici non sono tenuti ad elaborare i dati in loro possesso al fine di soddisfare le richieste di accesso⁶.
3. Non sono ammissibili domande di accesso preordinate ad un controllo generalizzato dell'operato dell'ente.
4. La domanda può essere trasmessa anche per via telematica ed è presentata all'ufficio che detiene i dati, le informazioni e i documenti. L'ufficio la inoltra, per conoscenza, al Responsabile della prevenzione della corruzione e della trasparenza.
5. Il diritto di accesso si esercita mediante esame ed estrazione di copia dei documenti amministrativi.
6. L'esame dei documenti è gratuito. Il rilascio di copie è subordinato al rimborso del costo di riproduzione, salve le disposizioni vigenti in materia di bollo, nonché i diritti di ricerca e di visura, come previsto dall'apposita deliberazione di Giunta Comunale di approvazione tariffe annuali.
7. Il procedimento deve concludersi entro trenta giorni, preferibilmente con un provvedimento motivato del responsabile dell'ufficio che detiene i dati, le informazioni e i documenti. In caso di silenzio, decorso il termine di trenta giorni la domanda è respinta⁷.

Articolo 24 – Controinteressati all'accesso agli atti

1. Sono controinteressati alla domanda di accesso agli atti amministrativi tutti i soggetti, che, ai sensi dell'articolo 22 comma 1 lettera c) della legge 241/1990, individuati o facilmente individuabili, dall'esercizio dell'accesso vedrebbero compromesso il loro diritto alla riservatezza.
2. Qualora siano individuati controinteressati, l'ufficio procedente comunica loro copia della domanda d'accesso agli atti, con raccomandata AR o via PEC.
3. Entro dieci giorni dalla ricezione della comunicazione, i controinteressati possono presentare una motivata opposizione, anche via PEC, alla richiesta di accesso.
4. Accertata la ricezione della comunicazione da parte dei controinteressati, decorso il termine di dieci giorni, l'ufficio provvede comunque sulla richiesta.
5. A decorrere dalla comunicazione ai controinteressati, il termine di trenta giorni per concludere il procedimento rimane sospeso fino all'eventuale opposizione degli stessi.

⁶ Si veda l'articolo 2 comma 2 del DPR 184/2006 *Regolamento recante disciplina in materia di accesso ai documenti amministrativi*.

⁷ "Silenzio rifiuto" si veda l'articolo 25 comma 4 della legge 241/1990 e smi.

Articolo 25 - Accesso informale

1. Qualora, in base alla natura del documento richiesto, non risulti l'esistenza di controinteressati, il diritto di accesso può essere esercitato in via informale mediante richiesta, anche verbale, all'ufficio che detiene il documento.
2. Il richiedente deve indicare gli estremi del documento richiesto, oppure elementi che ne consentano l'individuazione, e comprovare l'interesse connesso all'oggetto della richiesta, dimostrare la propria identità e, ove occorra, i propri poteri di rappresentanza del soggetto interessato.
3. La richiesta, esaminata immediatamente e senza formalità, è accolta mediante indicazione del provvedimento contenente le notizie, esibizione del documento, estrazione di copie, ovvero altra modalità idonea.
4. La richiesta, ove provenga da una pubblica amministrazione, è presentata dal titolare dell'ufficio interessato o dal responsabile del procedimento amministrativo ed è trattata ai sensi dell'articolo 22, comma 5, della legge 241/1990.
5. Qualora l'ufficio, in base al contenuto del documento richiesto, riscontri l'esistenza di controinteressati, invita il richiedente a presentare domanda formale di accesso.

Articolo 26 - Accesso formale

1. Qualora non sia possibile accogliere la domanda in via informale, oppure sorgano dubbi sulla legittimazione del richiedente, sulla sua identità, sui suoi poteri rappresentativi, sulla sussistenza dell'interesse diretto concreto ed attuale, sull'accessibilità del documento o sull'esistenza di controinteressati, l'ufficio invita l'interessato a presentare richiesta d'accesso agli atti formale e ne rilascia ricevuta.
2. Il procedimento di accesso deve concludersi nel termine di trenta giorni, decorrenti dalla presentazione della domanda all'ufficio.
3. Qualora la domanda sia irregolare o incompleta, l'ufficio entro dieci giorni ne dà comunicazione al richiedente con raccomandata AR o via PEC. Il termine del procedimento ricomincia a decorrere dalla presentazione della richiesta corretta.

Articolo 27 - Domanda accolta e modalità di accesso.

1. L'accoglimento della domanda di accesso a un documento comporta la facoltà di accedere agli altri documenti nello stesso richiamati e appartenenti al medesimo procedimento, fatte salve le eccezioni di legge o di regolamento.
2. L'esame dei documenti avviene presso l'ufficio indicato nell'atto di accoglimento, nelle ore di ufficio, alla presenza se necessaria di personale addetto.
3. I documenti sui quali è consentito l'accesso non possono essere asportati dal luogo presso cui sono dati in visione, o comunque alterati in qualsiasi modo.
4. L'esame dei documenti è effettuato dal richiedente o da persona da lui incaricata, con l'eventuale accompagnamento di altra persona di cui vanno specificate le generalità, che

devono essere poi registrate in calce alla richiesta. L'interessato può prendere appunti e trascrivere in tutto o in parte i documenti presi in visione.

Articolo 28 - Domanda respinta o differita

1. Il rifiuto, la limitazione o il differimento dell'accesso agli atti formale sono motivati, con riferimento specifico alla normativa vigente e, in particolare, alle categorie di cui all'articolo 24 della legge 241/1990, ed alle circostanze di fatto per cui la richiesta non può essere accolta così come proposta.
2. Il differimento dell'accesso è disposto se è sufficiente per assicurare una temporanea tutela agli interessi di cui all'articolo 24, comma 6, della legge 241/1990, o per salvaguardare specifiche esigenze dell'amministrazione, specie nella fase preparatoria dei provvedimenti, in relazione a documenti la cui conoscenza possa compromettere il buon andamento dell'azione amministrativa.
3. Il provvedimento che dispone il differimento dell'accesso ne indica la durata.

Articolo 29 - Tutele e ricorsi

1. Interessati e controinteressati all'accesso agli atti amministrativi dispongono delle tutele previste dall'articolo 25 comma 4 della legge 241/1990.

TITOLO V - Norme finali

Articolo 30 - Rinvio dinamico

1. Le disposizioni del presente regolamento si intendono modificate per effetto di sopravvenute norme nazionali, regionali o di prescrizioni inderogabili dell'Autorità Nazionale Anticorruzione. Nelle more dell'adeguamento del presente regolamento si applica immediatamente la normativa sopravvenuta.

Articolo 31 - Entrata in vigore, abrogazioni e pubblicità

1. Questo regolamento entra in vigore il giorno in cui diviene esecutiva la deliberazione consiliare d'approvazione.
2. Sono abrogate tutte le norme regolamentari di questo ente che normano il diritto di accesso o che siano in contrasto con il presente.
3. Il presente è pubblicato sul sito internet dell'ente.

Allegato 7 – Procedura per l'attivazione del Registro di Emergenza

L'attivazione del Registro di protocollo di emergenza avviene se si verificano tre condizioni, non necessariamente concomitanti:

- 1 Guasto al software di protocollazione Informatica o sua indisponibilità per mancanza di connettività
- 2 Guasto al sistema informatico dell'Ente
- 3 Mancanza di energia elettrica

Quando si verifica la condizione 1 si deve attivare un registro di emergenza su supporto informatico.

Quando si verificano le condizioni 2 o 3 si deve attivare un registro di emergenza cartaceo.

Procedura di attivazione

Attività da eseguire per l'attivazione del Registro di protocollo di emergenza:

- a) Il Responsabile del Servizio Gestione documentale deve predisporre apposito provvedimento per l'attivazione del Registro e redigere il verbale di attivazione;
- b) il personale dell'Ufficio Protocollo deve compilare il Registro di emergenza (su supporto informatico o manuale a seconda dei casi)
- c) Il Responsabile del Servizio Gestione documentale da comunicazione alle strutture organizzative dell'Ente dell'attivazione di dell'apposito registro e successivamente comunica alla Soprintendenza archivistica l'attivazione del registro

Procedura di chiusura dell'emergenza

Al termine dell'emergenza:

- a) Il Responsabile del Servizio Gestione documentale deve predisporre apposito provvedimento per la chiusura del Registro e redigere il verbale di chiusura dell'emergenza;
- b) deve versare le registrazioni di emergenza nel protocollo informatico dell'Ente seguendo le procedure del programma di cui alla guida della specifica funzionalità
- c) deve dare comunicazione alle strutture organizzative dell'Ente della revoca dell'emergenza
- d) deve comunicare alla Soprintendenza archivistica il ripristino delle funzionalità del registro di protocollo informatico.

La numerazione del registro di emergenza è unica per l'intero anno e ricomincia dal numero successivo all'ultimo generato per ogni attivazione.

Nel caso di attivazione del Registro di Emergenza Manuale si possono utilizzare fogli singoli con numerazione indicata nel margine destro, in modo tale che più operatori possano lavorare contemporaneamente.

La numerazione indicata deve essere riportata per ogni documento registrato.

Registro manuale di emergenza

Di seguito un'immagine di esempio del registro manuale di emergenza:

Numero Registr. emergenza	Data	Tipo	Mittente/Destinatrio	Oggetto	Classificazione			
					Cat	Classe	Sotto classe	n. Fascicolo

Allegato 8 - Piano di selezione, conservazione e scarto

Il presente piano di selezione, conservazione e scarto è basato sul vigente Titolario d'archivio.

Selezione

La selezione è l'attività che consente di suddividere la documentazione, su qualunque supporto sia stata prodotta, fra quella da archiviare in modo definitivo, quella da archiviare provvisoriamente, e quella da eliminare con diverse tempistiche, in base ai massimari di conservazione e scarto anch'essi allegati al Manuale di gestione e redatti in base alla normativa vigente. Tali massimari possono essere modificati in base alle esigenze dell'Amministrazione, purché non in contrasto con la normativa.

L'attività di selezione è di competenza dei diversi Servizi/Uffici dell'Ente che devono effettuare le attività.

Archiviazione e conservazione

I documenti dell'amministrazione, su qualsiasi formato siano stati prodotti, sono conservati a cura dei diversi Servizi/Uffici dell'Ente, secondo quanto previsto dal manuale di gestione. La documentazione corrente, relativa alle pratiche in corso non ancora terminate, è conservata a cura dei responsabili dei singoli uffici fino al trasferimento in archivio moderno, secondo quanto previsto dagli articoli del presente piano.

Formato dei documenti elettronici

Per la predisposizione dei documenti informatici si adottano formati che possiedono i requisiti minimali di leggibilità, interscambiabilità, non alterabilità durante le fasi di accesso e conservazione, immutabilità nel tempo del contenuto e della struttura.

Trasferimento all'archivio di deposito

Si trasferisce all'archivio moderno (o di deposito) tutta la documentazione relativa ad affari o procedimenti chiusi durante l'anno precedente il trasferimento, nonché tutti i fascicoli annuali e i fascicoli del personale cessato. L'operazione di versamento è curata dal responsabile del singolo Servizio/Ufficio. Presso tale archivio la documentazione rimane per 40 anni; il termine di conservazione decorre dalla data dell'ultimo documento che esaurisce la trattazione dell'affare ovvero dalla conclusione del procedimento amministrativo.

Il trasferimento avviene dopo che i singoli uffici abbiano prodotto un elenco di tutti i fascicoli e registri da versare; il responsabile del Servizio conservazione verifica la correttezza degli elenchi e la loro corrispondenza con il repertorio dei fascicoli, cura la formazione e la conservazione di un elenco di tutti i fascicoli e delle serie trasferite nell'archivio di deposito (art.67 *testo unico*).

Il responsabile del Servizio conservazione provvede altresì a concordare con i responsabili degli uffici il piano della fascicolazione per l'anno successivo in base al quadro di classificazione. Durante l'anno è possibile aggiungere al piano della fascicolazione ogni fascicolo che si renda necessario secondo quanto stabilito dal manuale di gestione.

In questa fase avviene la prima operazione di scarto relativa al materiale di immediata eliminazione (cosiddetto *scarto in itinere*).

Trasferimento alla sezione separata (archivio storico)

Come previsto dalla normativa vigente, tutti i documenti anteriori all'ultimo quarantennio e destinati alla conservazione definitiva vengono versati dall'archivio di deposito presso la sezione separata (archivio storico).

In questa fase avvengono, a cura del responsabile del Servizio conservazione, le ulteriori operazioni di verifica del materiale di conservazione provvisoria, come previsto negli allegati massimari. E' possibile depositare anche documentazione più recente, qualora non rivesta più un preminente carattere giuridico-amministrativo per l'ente, sotto la responsabilità del suddetto Servizio di conservazione.

Gestione dei documenti della sezione separata

La gestione dei documenti versati presso l'archivio storico, considerato il fine essenzialmente storico che essi ricoprono e della necessità di trattamento distinto dalla documentazione dell'archivio moderno, è regolata da apposito **Regolamento** allegato al Manuale.

Conservazione dei documenti informatici

Il Responsabile del Servizio Informatico in collaborazione col Responsabile del Servizio Protocollo e Gestione documentale e con il supporto della tecnologia disponibile, provvede a conservare i documenti informatici selezionati per la conservazione perenne e a controllare periodicamente a campione (almeno una volta all'anno) la leggibilità dei documenti stessi.

Scarto

Per scarto s'intende l'eliminazione, previa selezione, del materiale documentario ritenuto inutile o superfluo ai bisogni ordinari dell'amministrazione e non necessario ai fini della ricerca storica. Lo scarto è attuato sotto la sorveglianza della Soprintendenza Archivistica per la Lombardia, come previsto dal d.lgs. 42/2004 "Codice dei beni culturali e del paesaggio".

Lo scarto avviene secondo un massimario costituito dagli elenchi di cui alla voce "Documentazione da scartare" del presente allegato, che prevedono selezioni e tempistiche differenti in base alla tipologia della documentazione.

Gli elenchi dei documenti selezionati per l'eliminazione sono inviati per il nulla osta alla competente Soprintendenza archivistica per la Lombardia; ottenuta l'approvazione, il responsabile del Servizio di conservazione predispose l'atto dirigenziale relativo allo scarto e porta a termine la distruzione fisica dei documenti cartacei.

Consultazione dei documenti

Gli uffici possono richiedere in ogni momento, per consultazione, fascicoli inviati in archivio di deposito o nella sezione separata; l'accesso va concordato con il responsabile del Servizio di conservazione.

Si deve tenere traccia delle operazioni effettuate in relazione alla movimentazione dei fascicoli, della richiesta di prelevamento e dei tempi stabiliti per la restituzione.

Aggiornamento

Ogni anno il responsabile del Servizio di conservazione valuta la congruità del piano di scarto e lo aggiorna in base alle necessità riscontrate. Comunica, con i mezzi che ritiene più idonei, ai membri dell'amministrazione con funzioni di responsabili nonché ai dirigenti gli aggiornamenti al piano.

Documentazione da archiviare e conservare senza limiti di tempo

La documentazione da archiviare sotto elencata si intende in originale, o in copia qualora l'originale sia indisponibile, sia su supporto cartaceo che digitale.

- Tutta la corrispondenza protocollata prodotta nel corso dell'espletamento dell'attività dell'Amministrazione (se non è compresa nelle voci di materiale da scartare)

Amministrazione generale

- Protocollo generale
- Piani di classificazione della corrispondenza, repertori, strumenti d'archivio
- Convenzioni e protocolli d'intesa
- Statuti, Regolamenti
- Registri albo pretorio e notifiche
- Pianta organica aggiornata e piani occupazionali

Organi di governo, gestione, controllo

- Delibere di Consiglio e Giunta
- Decreti e ordinanze del Sindaco
- Decreti e Determinazioni dirigenziali
- Elenchi trasmissione delibere organi di controllo
- Ordini del giorno e verbali di Consiglio e Giunta
- Interpellanze e mozioni dei consiglieri
- Istanze, petizioni, esposti
- Verbali commissioni consiliari e altre commissioni
- Fascicoli amministratori e membri delle commissioni
- Contratti e capitolati

Personale e risorse umane

- Verbali delle commissioni per espletamento di concorsi e selezioni (in caso di concorsi con pochi partecipanti, è possibile conservare tutta la pratica con le prove di concorso anche per fini storici)
- Fascicoli personale di ruolo (in servizio e in pensione)
- Ruoli e matricole personale

Affari legali

- Pratiche legali

Servizi sociale e servizi alla persona

- Piani di intervento in campo sociale
- Fascicoli assistiti

Polizia locale e sicurezza pubblica

- Registri e verbali incidenti stradali
- Registri e verbali infrazioni Polizia Municipale

Risorse finanziarie e patrimoniali

- Verbali delle commissioni per aggiudicazione forniture varie
- Schede tecniche delle forniture
- Albi aggiornati dei fornitori
- Concessioni permanenti
- Plateatico e concessione suolo pubblico a qualunque titolo (fiere, mercati, spettacoli, aree cimiteriali e loculi)
- Inventari aggiornati beni mobili e immobili
- Bilanci e conti consuntivi
- Mandati e reversali
- Libri mastri e contabili
- Ruoli delle imposte e tasse

Elezioni e iniziative popolari

- Verbali commissioni elettorali
- Albi, liste elettorali aggiornate

Lavori Pubblici e Assetto del territorio

- Piani regolatori e commerciali
- Lavori pubblici: progetti, verbali, contratti, conti
- Manutenzione fabbricati e immobili
- Piani aggiornati trasporto pubblico
- Concessioni edilizie

Attività economiche

- Fascicoli e autorizzazioni esercizi commerciali, pubblici esercizi, società, spettacoli

Servizi demografici

- Verbali commissioni elettorali
- Liste di leva
- Registri anagrafici
- Contratti cimiteriali

All'elenco va aggiunta inoltre tutta la eventuale documentazione per la quale sia prevista per legge una conservazione illimitata

In generale vanno conservati i registri che riportino dati e informazioni ricavate dal cartaceo che si intende eliminare.

Resta sempre a discrezione del responsabile dello scarto valutare se del materiale possa rivestire, in previsione futura, dell'interesse storico, e quindi decidere per l'archiviazione anche se non rientra nelle categorie previste.

Vanno conservati gli atti che riportino dati riassuntivi e statistici.

In caso di documentazione non prevista nelle tipologie sopra indicate, occorre individuare quella più affine.

Documentazione da scartare

1) Scarto in itinere (immediato)

La seguente documentazione può essere eliminata all'atto del trasferimento delle carte dall'archivio corrente all'archivio di deposito:

- Copie bilanci e relazioni
- Copie progetti e atti contabili
- Buste vuote corrispondenza
- Registri in bianco e modulistica
- Manifesti

Riviste, pubblicazioni, Gazzette Ufficiali, possono essere scartate senza richiesta di autorizzazione alla Soprintendenza Archivistica.

2) Scarto dopo 5 anni:

Questo materiale deve essere eliminato nel periodo di giacenza presso l'archivio moderno.

- Circolari interne
- Bollettari, matrici, blocchetti vari
- Bolle di accompagnamento
- Avvisi e ricevute di pagamento

Titolo I: AMMINISTRAZIONE GENERALE

- Registri di spese postali
- Compiuta giacenza, destinatari irreperibili e reperibili non ritirati, richieste di pagamento enti richiedenti

Titolo II: ORGANI DI GOVERNO, GESTIONE, CONTROLLO, CONSULENZA E GARANZIA

- Avvisi di convocazione Giunta, Consiglio, Commissioni

Titolo III: RISORSE UMANE

- Cartellini e tabulati presenze personale
- Registri e richieste ferie, permessi, assenze, tabulati e permessi orari, turni, straordinari, visite fiscali
- Cedolini e tabulati CPDL – INPS - Gescal – variazione stipendi

Titolo IV: RISORSE FINANZIARIE E PATRIMONIALI

- Richieste dagli uffici di forniture economiche
- Solleciti di pagamento

Titolo XI: SERVIZI DEMOGRAFICI

- Richieste certificati nascita – comunicazioni e direttrici di trascrizione morte, nascita e matrimonio
- Certificati assistenza al parto
- Autorizzazioni trasporti salme

3) Scarto dopo 10 anni

Questo materiale deve essere eliminato nel periodo di giacenza presso l'archivio moderno e in ogni caso prima del trasferimento della massa documentaria alla sezione separata di archivio storico.

Titolo I: AMMINISTRAZIONE GENERALE

- Corrispondenza interna
- Minute e fatture relative a pratiche varie
- Manuali e relazioni non più aggiornati

Titolo II: ORGANI DI GOVERNO, GESTIONE, CONTROLLO, CONSULENZA E GARANZIA

- Copie delibere Giunta e Consiglio
- Copie determinazioni dirigenziali

Titolo III: RISORSE UMANE

- Stipendi: Copia modelli 740
- Personale: Ordini di servizio, piante organiche, valutazione personale
- Personale: Concorsi e selezioni: domande, prove, atti preparatori (da archiviare i verbali; diplomi originali da conservare per 40 anni)

Titolo IV: RISORSE FINANZIARIE E PATRIMONIALI

- Economato: Offerte e preventivi forniture varie (in archivio i verbali, contratti)
- Economato: Inventari patrimoniali (se sostituiti con altri aggiornati)
- Economato: domande ed elenchi fornitori
- Ragioneria: Copie mandati, reversali, fatture, distinte di liquidazione, mastri fornitori, registri sezionali IVA, ritenute d'acconto, spese economali
- Tributi: Censimento TRSU, schede AGIAP, avvisi di pagamento imposte varie

Titolo VI: PIANIFICAZIONE E GESTIONE DEL TERRITORIO

- Lavori Pubblici: carteggio manutenzione beni mobili e immobili, strade, verde, caldaie, ascensori
- Lavori Pubblici: Concessioni provvisorie rotture per lavori stradali - Permessi temporanei viabilità - Richieste immissioni precarie fognatura
- Lavori Pubblici: Copie progetti e atti contabili, Ampliamenti illuminazione pubblica – installazioni telefoniche – carteggi acquisto materiale vario, Copie delibere ASM
- Lavori Pubblici: Censimenti caldaie e distributori

Titolo VII: SERVIZI ALLA PERSONA

- Servizi Sociali: domande di concessione tributi o esenzioni
- Servizi Sociali: pratiche assistite (contributi, richieste di pagamento e atti interni)
- Servizi Sociali: gare di affidamento servizi e progetti scaduti
- Servizi scolastici: Buoni libro, schede e domande iscrizione nidi e materne, presenze personale e minori nidi e materne
- Servizi scolastici: Domande riduzione ed esenzione rette, Comitati scolastici, relazioni e programmazione, servizi e pasti erogati, richieste trasporti
- Politiche abitative: bandi scaduti

Titolo VIII: ATTIVITÀ ECONOMICHE

- Sportello attività produttive: Licenze commercio ritirate e respinte – modifiche turni di chiusura, ferie
- Sportello attività produttive: Autorizzazioni saldi, promozioni, feste, spettacoli viaggianti, fiere, occupazioni temporanee (in archivio fascicoli commercio fisso, pubblici esercizi, società)

Titolo IX: POLIZIA LOCALE E SICUREZZA PUBBLICA

- Polizia Municipale: verbali contravvenzioni a codice strada e regolamenti
- Polizia Municipale Richieste occupazione suolo pubblico – permessi carico e scarico - Permessi temporanei transito zona traffico limitato

Titolo XI: SERVIZI DEMOGRAFICI

- Demografico: Fascicoli e schede giudici popolari Corte d'Assise e di Appello
- Demografico: Schede rilevazione statistiche varie
- Demografico: Mutazioni stato civile – rettifiche allo schedario – adozioni, emancipazioni, morte presunta, legittimazioni
- Demografico: Cartellini carte d'identità

Titolo XII: ELEZIONI E INIZIATIVE POPOLARI

- Elettorale: Liste sezionali
- Elettorale: Minute e copie verbali commissione elettorale (in archivio originali verbali)
- Elettorale: Elezioni: statistiche, stampati, nomine presidenti e scrutatori, circolari, allestimento seggi, consegne materiale, verbali sezionali

MANUALE DI CONSERVAZIONE

<i>Codice documento</i>	ManualeConservazione
<i>Versione</i>	1.1

	<i>Data</i>	<i>Nominativo</i>	<i>Funzione</i>
<i>Redazione</i>	22/122021	Giovanni Galazzini	Consulente
		Cristiano Casagni	Responsabile sviluppo e manutenzione del sistema
<i>Verifica</i>	28/12/2021	Gabriele Bezzi	Responsabile funzione archivistica di conservazione
<i>Approvazione</i>	28/12/2021	Marco Calzolari	Responsabile del servizio

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

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	Produttore	26
4.3	Utente	27
4.4	Ente conservatore.....	28
4.5	Organismi di tutela e vigilanza.....	30
5	STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE	33
5.1	Organigramma della Regione Emilia-Romagna	33
5.2	Struttura organizzativa del Servizio Polo Archivistico (ParER).....	33
6	OGGETTI SOTTOPOSTI A CONSERVAZIONE	40
6.1	Oggetti conservati.....	40
6.1.1	Unità archivistiche e Unità documentarie.....	43
6.1.2	Formati.....	45
6.1.3	Metadati.....	46
6.2	Pacchetto di versamento (SIP).....	47
6.3	Pacchetto di archiviazione (AIP)	48
6.4	Pacchetto di distribuzione (DIP)	49
7	PROCESSO DI CONSERVAZIONE	50
7.1	Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico	50
7.1.1	Preacquisizione	52
7.1.2	Acquisizione	53
7.2	Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti.....	53
7.3	Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico	54
7.4	Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie	55
7.4.1	Monitoraggio	55
7.4.2	Gestione delle anomalie	56
7.5	Preparazione e gestione del Pacchetto di archiviazione.....	58
7.6	Preparazione e gestione del Pacchetto di distribuzione (DIP) ai fini dell'esibizione.....	61
7.7	Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti	62
7.8	Scarto dei pacchetti di archiviazione	62
7.9	Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori	63

8	IL SISTEMA DI CONSERVAZIONE.....	65
8.1	Componenti logiche.....	65
8.2	Componenti tecnologiche	67
8.2.1	SacER.....	68
8.2.2	VersoO	71
8.2.3	PING	71
8.2.4	DPI.....	72
8.2.5	Interfacce di Acquisizione e di Recupero (Web Service)	72
8.2.6	TPI	72
8.2.7	DIPS.....	73
8.2.8	SIAM	73
8.2.9	Sacerlog	74
8.2.10	Componenti di supporto	74
8.3	Componenti fisiche.....	76
8.3.1	Schema generale	76
8.3.2	Caratteristiche tecniche dei Sistemi	78
8.4	Procedure di gestione e di evoluzione	82
8.4.1	Gestione dell'Esercizio.....	82
8.4.2	Gestione delle utenze	82
8.4.3	Gestione dei Malfunzionamenti.....	83
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	89
9	MONITORAGGIO E CONTROLLI.....	91
9.1	Procedure di monitoraggio	91
9.2	Funzionalità per la verifica e il mantenimento dell'integrità degli archivi	91
9.3	Soluzioni adottate in caso di anomalie	92
9.4	Verifica periodica di conformità a normativa e standard di riferimento.....	94
9.5	Audit e gestione delle Non Conformità	94
9.6	Controlli di sicurezza	96
10	TRATTAMENTO DEI DATI PERSONALI.....	97
11	DOCUMENTI DI RIFERIMENTO E ALLEGATI	100

INDICE DELLE FIGURE

<i>Figura 1 - Sistema e attori</i>	<i>25</i>
<i>Figura 2 - Struttura organizzativa di ParER</i>	<i>36</i>
<i>Figura 3 - Modello di ordinamento di archivio derivato da ISAD</i>	<i>40</i>
<i>Figura 4 - Pacchetto informativo (da OAIS)</i>	<i>43</i>
<i>Figura 5 - Struttura dell'Unità documentaria</i>	<i>44</i>
<i>Figura 6 - Schema logico del Sistema di conservazione</i>	<i>65</i>
<i>Figura 7 - Flussi di dati nel Sistema di conservazione</i>	<i>67</i>
<i>Figura 8 - Schema Tecnologico del Sistema di conservazione</i>	<i>68</i>
<i>Figura 9 - Schema Infrastrutturale del Sistema di conservazione</i>	<i>77</i>
<i>Figura 10 - Schema dei Sistemi di ParER</i>	<i>79</i>
<i>Figura 11 - Schema del Sito Primario</i>	<i>80</i>
<i>Figura 12 - Procedura di Gestione utenze</i>	<i>83</i>
<i>Figura 13 - Procedura di Gestione delle Richieste di Informazioni, Reclami e Segnalazioni</i>	<i>84</i>
<i>Figura 14 - Procedura di Gestione incidenti di sicurezza</i>	<i>85</i>
<i>Figura 15 - Procedura di Gestione richieste di cambiamento</i>	<i>86</i>
<i>Figura 16 - Procedura di Progettazione e realizzazione di software applicativo</i>	<i>88</i>
<i>Figura 17 - Procedura di Gestione dei rilasci</i>	<i>89</i>
<i>Figura 18 - Procedura di Audit del SGI</i>	<i>95</i>
<i>Figura 19 - Gestione delle Non Conformità</i>	<i>95</i>
<i>Figura 20 - Procedura di Verifiche Tecniche e VA/PT</i>	<i>96</i>

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. E' predisposto dal Servizio Polo archivistico e gestione documentale (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 convenzionati. 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 convenzione o 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 citate fonti 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.

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 che accede ai servizi o alle risorse di un'altra componente detta 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*. [da **OAIS**]

Contenuto informativo: l'insieme delle informazioni che costituisce l'obiettivo originario della *conservazione*. E' composto dall'**Oggetto-dati** e dalle **Informazioni di rappresentazione**. [da **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 prevede riflessioni anche su persone, siti, risorse e fornitori dell'organizzazione.

Convenzione: accordo tra il *Produttore* e ParER, che regola i rapporti di servizio, e più precisamente: la natura dei servizi offerti, la responsabilità delle parti e le condizioni economiche, oltre agli strumenti di consultazione e controllo. Con il termine Convenzione si intendono sia le convenzioni propriamente dette, sottoscritte con gli Enti del territorio dell'Emilia-Romagna, sia gli accordi di collaborazione sottoscritti con Enti di altri territori nazionali.

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: Una 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*.

Ente Produttore (o Produttore): *titolare dell'oggetto della conservazione* che affida la conservazione dei propri documenti informatici alla Regione Emilia-Romagna

Esito versamento: documento in formato XML prodotto al termine delle verifiche in fase di **versamento**, memorizzato nel *Sistema di conservazione* ed 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 una 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*. [da **OAIS**]

Informazioni sulla rappresentazione: informazioni che associano un **Oggetto-dati** a concetti più significativi. [da **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**. [da **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 SpA)

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 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. [da **OAIS**]

Raccolta di archiviazione (AIC): Un 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. [da **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)

ParER: Servizio Polo archivistico e gestione documentale della Direzione Generale Risorse, Europa, Innovazione e Istituzioni della Regione Emilia-Romagna

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 oppure 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

Produttore (o Ente produttore): *titolare dell'oggetto della conservazione* che affida la conservazione dei propri documenti informatici alla Regione Emilia-Romagna

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)

Regione: Regione Emilia-Romagna, nelle sue articolazioni di Giunta regionale, comprese le Agenzie senza personalità giuridica, e 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.

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**;
- a ragione di qualche altra relazione derivante dalle modalità della loro produzione, acquisizione o uso.

(fonte: **ISAD**)

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)

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) e il Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

SIDDT (Servizio ICT – Servizio Innovazione Digitale, dei Dati e della Tecnologia): struttura organizzativa della Regione Emilia-Romagna deputata, in base a quanto previsto dalla Delibera di Giunta n. 771/2021, a gestire le infrastrutture informatiche, a fissare gli standard informatici e di rete, a progettare, sviluppare e gestire i sistemi informativi "centrali", a gestire la sicurezza informatica degli strumenti informatici ed apparati di rete utilizzati per le attività della Regione e degli Enti / Agenzie che fruiscono a vario titolo dei servizi informatici e di rete regionali

SIEM (Security Information and Event Management): le soluzioni rientranti in questa categoria di sistemi sono contraddistinte dalla capacità di effettuare analisi 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)

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***.

Storage: dispositivo per memorizzare i dati in formato digitale; sono considerati storage sia i dispositivi a cassette che i dispositivi a disco.

Struttura versante (o Struttura): ripartizione dell'Ente produttore identificativa della specifica area di produzione dei documenti versati, in genere coincidente con l'*area 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 gestisce e registra delle liste di richieste di assistenza o di problemi, organizzato secondo le necessità di chi offre il servizio. [...] Un ticket o biglietto, serve per tenere il filo di una richiesta. Ad ogni biglietto corrisponde un identificativo univoco, che ne consente l'archiviazione e la consultazione in qualunque momento, da parte del personale coinvolto nella sua chiusura. I biglietti 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***. [da ***ISAD***]

Unità di archiviazione (AIU): Un Pacchetto di archiviazione (AIP) elementare, il cui contenuto informativo non è ulteriormente decomposto in altri contenuti informativi. Definisce un AIP di Unità documentaria. [da ***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. [da **ISAD** e da **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 della 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 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 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.

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, 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 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 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 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 altresì 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 apposita convenzione, 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 il Servizio Polo Archivistico e gestione documentale di una specifica struttura tecnologica ed un organico con professionalità qualificate che assommano conoscenze di natura archivistica, informatica, organizzativa e giuridica⁴.

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".

⁴ Tra le competenze del Servizio, così come ridefinite dalla delibera di Giunta regionale del 24 maggio 2021, n. 771 figurano: la responsabilità dello svolgimento dei processi di conservazione sostitutiva e di riversamento sostitutivo dei Documenti informatici della Regione e degli Enti convenzionati o con accordo; la cura delle modalità di trasferimento, accesso e fruizione del patrimonio documentario e informativo conservato; la promozione dell'adesione degli enti del sistema regionale; il supporto all'azione dei responsabili del protocollo informatico presso gli Enti produttori per la messa a punto degli strumenti archivistici, organizzativi e software per le esigenze di conservazione dei documenti digitali, nonché per l'adeguamento al *Sistema di conservazione* digitale di ParER; la progettazione, lo sviluppo e la manutenzione del sistema di conservazione, garantendone l'aggiornamento in conformità agli standard internazionali di riferimento, ai cambiamenti normativi e alle evoluzioni della piattaforma tecnologica (hardware e software); la gestione ed erogazione di servizi per il trattamento e la trasmissione tra PA dei documenti informatici (e dei documenti multimediali) per la Regione e gli enti convenzionati o con accordo.

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 modello Open Archival Information System (**OAIS**), certificato standard ISO 14721 nel 2003 e recentemente aggiornato (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 PDV*), **Utente** (o *Utente abilitato*), **Responsabile della conservazione** o **Conservatore**.

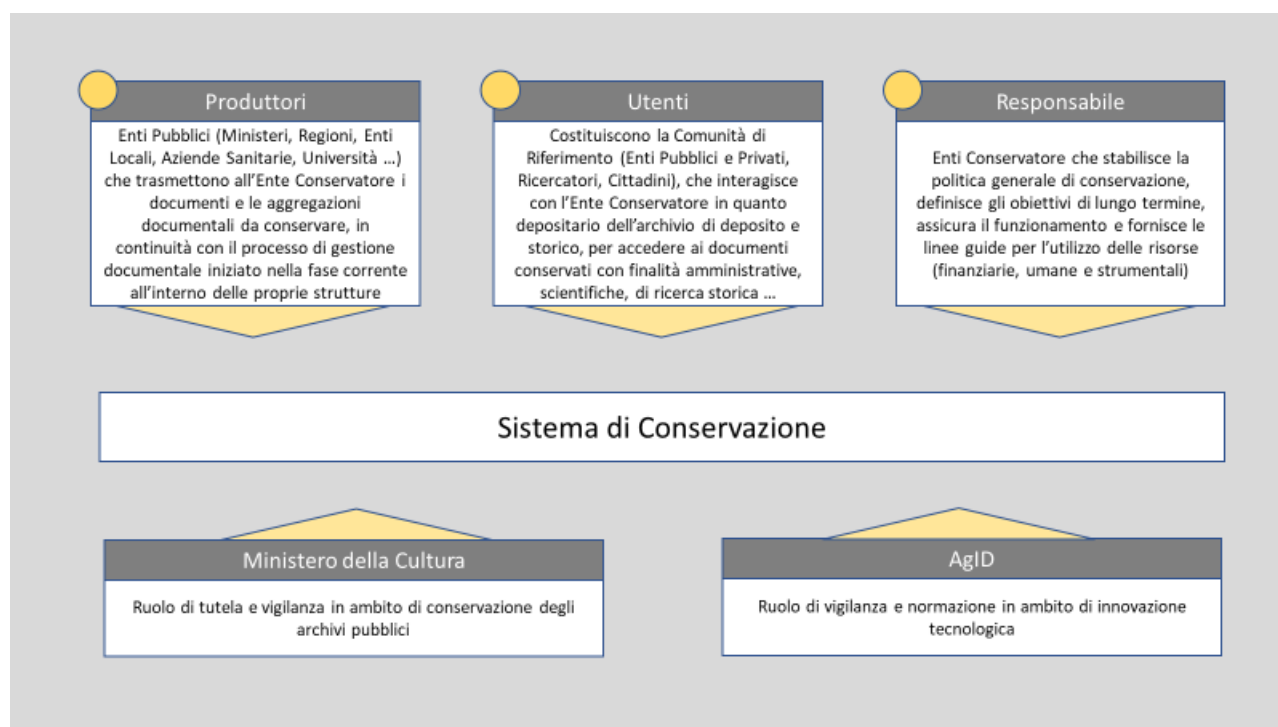


Figura 1 - Sistema e attori

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

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 nella **Convenzione** Ente Produttore.

Nel ruolo del *Produttore* possono essere definiti tutti gli enti pubblici convenzionati, 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: la **Convenzione** e il **Disciplinare tecnico**⁵.

La **Convenzione**, o 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. Le attuali **Convenzioni** 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 nella **Convenzione**, 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*.

⁵ 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 Convenzione 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.

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.

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 genericamente 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 Produttore 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 identifica 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 Conservatore

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*.

Il modello organizzativo precedentemente descritto, ai sensi dell'articolo 34, comma 1 bis, lettera b) del CAD, prevede che il 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 come Responsabile del servizio di conservazione il Responsabile di ParER.

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 e 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 coinvolto nelle operazioni quotidiane di amministrazione del sistema che sono totalmente a carico del soggetto incaricato della sua gestione, cioè il Servizio Polo Archivistico e gestione documentale, comunemente noto come ParER, 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.⁶

Di fatto, quindi (come definito dal testo della **Convenzione**, 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 del Servizio Polo Archivistico e gestione documentale (ParER) della Regione Emilia-Romagna. Nello svolgimento di tali attività è coadiuvato dal *Responsabile della funzione archivistica di conservazione*, che svolge anche il ruolo di *Responsabile della Conservazione* per la Regione.

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 opportunamente 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 Dirigente Responsabile del Servizio Polo archivistico regionale dell'Emilia-Romagna (ParER), quale Responsabile del servizio di conservazione; il titolare della Posizione organizzativa di presidio della funzione archivistica di conservazione, a cui, in quanto Responsabile della Conservazione, sono assegnate in particolare le funzioni di sottoscrizione previste nell'ambito

⁶ Da Relazione sulle attività realizzate per gli anni 2009 – 2012 approvata dalla Delibera di Giunta regionale Emilia-Romagna del 01 ottobre 2012, n. 1428.

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 la **Convenzione** 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.

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

4.5 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 42/2004⁷.

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)

⁷ 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

- al trasferimento di archivi informatici ad altri soggetti giuridici, nell'ottica della conservazione permanente sia del documento sia del contesto archivistico.⁸

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 **Convenzione**;
- 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 nella **Convenzione**, 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 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.

⁸Dal sito della Soprintendenza archivistica per l'Emilia-Romagna, <http://www.sacro.archivi.beniculturali.it/index.php?id=21>

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 potrà 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 della Regione Emilia-Romagna

La Regione Emilia-Romagna è organizzata in Direzioni Generali: all'interno di una di esse, la gestione del *Sistema di conservazione* è in carico a uno dei Servizi in cui si articola. Infatti, la Regione Emilia-Romagna ha attivato il Servizio Polo archivistico regionale dell'Emilia-Romagna (ParER) come struttura dirigenziale a livello di Servizio.

Con la Delibera di Giunta n. 771 del 24 maggio 2021 il Servizio è stato denominato Servizio Polo archivistico e gestione documentale e fa parte della Direzione Generale risorse, Europa, Innovazione e Istituzioni (DGREII)

A ParER sono state attribuite diverse competenze, tra le quali in primis la responsabilità dello svolgimento del *processo di conservazione* dei *Documenti informatici* della Regione e degli altri enti convenzionati, e la cura delle modalità di trasferimento, *accesso* e fruizione del patrimonio documentario e informativo conservato.

ParER cura inoltre l'evoluzione tecnologica e l'aggiornamento o la **migrazione** del *Sistema di conservazione*.

In una prospettiva di promozione della dematerializzazione e della conservazione digitale, ParER coordina l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione delle pubbliche amministrazioni previste dal Codice dell'amministrazione digitale in raccordo con la Direzione generale competente della Giunta regionale; supporta l'azione dei responsabili della gestione documentale presso i *Produttori*, in particolare in vista dell'adeguamento dei sistemi al *Sistema di conservazione*; promuove l'adesione degli enti del sistema regionale; si raccorda con analoghe iniziative a livello nazionale ed europeo.

5.2 Struttura organizzativa del Servizio Polo Archivistico (ParER)

All'interno di ParER, si situano le responsabilità relative al Servizio di Conservazione di seguito dettagliate.

Responsabile del Servizio: dirigente con responsabilità dei procedimenti / processi / progetti di ParER. E' il dirigente responsabile del Servizio Polo archivistico e gestione documentale (ParER). È responsabile dei progetti e delle attività di ParER, della definizione e attuazione delle politiche complessive del Sistema di conservazione, nonché del governo della gestione del Sistema di conservazione e della gestione amministrativa del personale assegnato, con responsabilità sulle differenti posizioni organizzative afferenti al servizio e sulla relativa definizione del personale e delle risorse di cui avvalersi per l'attuazione delle attività, sulla pianificazione annuale delle attività assegnate e dell'organizzazione del lavoro all'interno del servizio. Ha l'obbligo di definire i fabbisogni professionali ordinari e straordinari, le proposte di piani di sviluppo del personale e le conseguenti azioni e valutazioni dei risultati. È responsabile della definizione dei requisiti e delle specifiche del Sistema di conservazione, sulla base della

normativa vigente, e dell'erogazione del servizio ai *Produttori*, oltre che della gestione delle Convenzioni.

Responsabile della sicurezza dei sistemi per la conservazione: è il soggetto al quale compete la definizione delle soluzioni tecniche e organizzative in attuazione delle disposizioni in materia di sicurezza, nonché la verifica del rispetto e il monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza. È tenuto a segnalare eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.

Responsabile della funzione archivistica di conservazione: è il funzionario titolare della Posizione Organizzativa responsabile del presidio della funzione archivistica di conservazione ed opera a stretto contatto con il Responsabile del Servizio, nello svolgimento delle funzioni di *Responsabile della Conservazione* per Regione. Nella struttura organizzativa del paragrafo successivo va identificato con il Responsabile dell'Area funzione archivistica di conservazione. Rientrano tra le sue mansioni e responsabilità, come da specifica designazione:

- la definizione e gestione del processo di conservazione, incluse le modalità di trasferimento, descrizione archivistica, esibizione, accesso e fruizione del patrimonio documentario e informativo conservato;
- la verifica sistematica dell'aderenza del processo e del sistema di conservazione alla normativa e standard di riferimento e ai loro aggiornamenti;
- la definizione dei requisiti degli accordi e/o Convenzioni dal punto di vista archivistico, con la definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici, anche mediante l'analisi e l'identificazione dell'articolazione strutturale dei Produttori e delle modalità di registrazione e classificazione della documentazione da essi adottate;
- il monitoraggio del processo di conservazione con la verifica delle modalità di versamento e l'eventuale presenza di errori, la verifica di integrità e la descrizione archivistica dei documenti e delle Aggregazioni documentali informatiche trasferite;
- l'analisi archivistica per lo sviluppo di nuove funzionalità del Sistema di conservazione;
- la collaborazione con l'azione del responsabile della gestione documentale del Produttore ai fini del trasferimento in conservazione e della selezione;
- la gestione dei rapporti con gli enti convenzionati e con la Soprintendenza archivistica per l'Emilia-Romagna (ora Soprintendenza archivistica e bibliografica dell'Emilia-Romagna) e altre articolazioni del MiC per quanto di competenza;
- la sottoscrizione con firma digitale dei Pacchetti di archiviazione secondo le modalità descritte nel presente Manuale
- l'eventuale sottoscrizione di Pacchetti di distribuzione e di attestazioni di conformità di copie cartacee di Documenti informatici conservati.

Responsabile dei sistemi informativi per la conservazione: individuato nella struttura organizzativa del paragrafo successivo con il Responsabile dell'Area gestione servizi e infrastrutture di ParER. Rientrano tra le sue mansioni:

- la gestione dell'esercizio delle componenti hardware e software del Sistema di conservazione;
- la responsabilità della corretta erogazione dei servizi di conservazione, della verifica e del mantenimento dei relativi livelli di servizi;
- il monitoraggio, d'intesa con il Responsabile della Sicurezza del servizio di conservazione, della sicurezza fisica e logica dell'impianto tecnologico di ParER;

- il coordinamento tecnico dei rapporti con i fornitori di data center e supporto tecnologico ai progetti di conservazione digitale;
- la pianificazione, di concerto con i fornitori, dello sviluppo dell'architettura tecnologica a disposizione per le attività di conservazione e quelle di servizio;
- il controllo e verifica dei livelli di servizio erogati dai fornitori (SLA), la segnalazione delle eventuali difformità e la pianificazione delle necessarie contromisure;
- il coordinamento nell'assegnazione, nell'installazione e nella manutenzione delle attrezzature informatiche individuali, nonché nell'assistenza agli operatori, con il supporto dei collaboratori assegnati a tale attività;
- la collaborazione nelle attività inerenti alla protezione dei dati personali; la predisposizione delle procedure di acquisto di beni e servizi in area informatica;
- il supporto di rete telematica alle attività di ParER.

Responsabile dello sviluppo e della manutenzione del sistema di conservazione:

individuato nella struttura organizzativa del paragrafo successivo con la Posizione Organizzativa di Capo Progetto dell'Area tecnologia e sviluppo sistemi di conservazione. E' responsabile del coordinamento e della gestione dei rapporti con i fornitori per le attività di pianificazione strategica e operativa finalizzate alla progettazione e allo sviluppo del *Sistema di conservazione* di ParER e per le attività di monitoraggio e di verifica delle operazioni di implementazione del *Sistema di conservazione* e di personalizzazione e implementazione di nuove funzionalità dei sistemi informatici. Tra i suoi compiti rientrano:

- il monitoraggio dello sviluppo dei progetti informatici e la cura della rispondenza allo standard dei parametri e dei requisiti definiti;
- il coordinamento delle attività di verifica e di implementazione dei progetti;
- l'analisi e la progettazione delle nuove procedure informatiche in base alle necessità dell'utenza, agli standard e alla rispondenza ai criteri di qualità e sicurezza individuati per l'insieme del sistema informativo regionale;
- l'interfaccia con i Produttori, in riferimento agli applicativi di gestione, ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche;
- l'individuazione di soluzioni di personalizzazione e manutenzione delle soluzioni applicative in relazione alle diverse tipologie di Produttori e degli oggetti conservati o da conservare e alle esigenze di evoluzione tecnologica;
- la definizione delle caratteristiche e dei requisiti del Sistema di conservazione (componenti architetturali, applicative, delle risorse e dei servizi);
- la progettazione e organizzazione del sistema (informativo, informatico, telematico) con riferimento ai diversi processi di sviluppo, di test e rilascio in produzione e di conduzione a regime;
- la gestione dell'intero ciclo di sviluppo di siti web e portali connessi al servizio di conservazione;
- il supporto alla verifica dell'aderenza del processo e del sistema di conservazione alla normativa e standard di riferimento e ai loro aggiornamenti.

Le figure sopracitate svolgono inoltre le azioni indicate nel Piano della Sicurezza in merito alla definizione ed alla attuazione degli indirizzi e delle attività necessarie per assicurare la sicurezza delle informazioni conservate.

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

ParER è organizzato secondo la struttura riportata in figura.

Le aree indicate svolgono le attività di seguito descritte in dettaglio; il Responsabile della Sicurezza coincide attualmente con il Responsabile del servizio e il Responsabile della Qualità coincide con il Responsabile dell'Area funzioni di supporto.

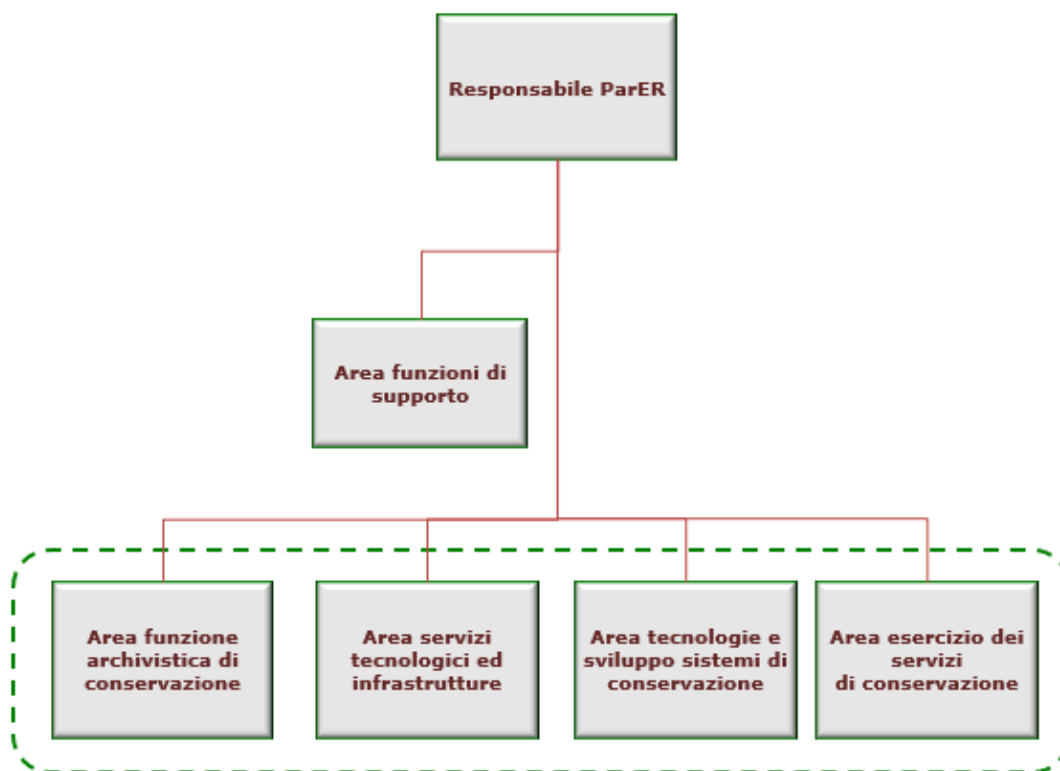


Figura 2 - Struttura organizzativa di ParER

AREA FUNZIONI DI SUPPORTO, per la gestione dei processi amministrativi interni al servizio. In particolare, è in capo a quest'area la responsabilità nella gestione dei rapporti giuridico-amministrativi e nella redazione degli atti di impegno e delle convenzioni con la pubblica amministrazione, degli atti di liquidazione e dei contratti con i fornitori e della gestione delle **Convenzioni** con gli enti per l'avvio del rapporto con ParER, l'analisi e gli adempimenti organizzativi relativi all'applicazione della normativa in materia di protezione dei dati personali; la gestione contabile dei capitoli di spesa di competenza di ParER e il relativo monitoraggio; la gestione della procedura amministrativa inerente le **Convenzioni** per la funzione di conservazione dei *Documenti informatici* da sottoscrivere con i *Produttori* (enti locali e vari enti pubblici), la gestione dei processi di certificazione e di accreditamento, le gestione della Qualità. Il Responsabile di quest'area è rappresentato dal **Responsabile di Gestione Qualità**, che ha il compito di verificare sia la redazione che l'aggiornamento dei documenti del Sistema di Gestione Integrato (**SGI**) rispetto ai requisiti ISO 9001. Una volta definita, è responsabile della distribuzione della documentazione approvata, della definizione dei template e standard documentali, della loro revisione nel caso di cambiamenti e modifiche. Relativamente al suo ambito, è responsabile degli Audit al fine di verificare la corretta applicazione delle procedure e

dei requisiti prescritti dalla normativa e analizzare le Non conformità di processo e di sistema in modo da evidenziare eventuali scostamenti, di conseguenza concorda con gli altri Responsabili l'applicazione di adeguate Azioni Correttive. Rileva gli indici di Qualità ed effettua il riesame per verificare l'adeguatezza e l'efficacia del sistema integrato, focalizzandosi sull'ambito della qualità.

AREA FUNZIONE ARCHIVISTICA DI CONSERVAZIONE, con funzioni di gestione del protocollo, gestione e verifica della conservazione digitale, gestione dell'archivio di deposito e storico analogico della Regione Emilia-Romagna.

Quest'area ha la responsabilità generale del processo di conservazione, e in particolare garantisce l'aderenza del processo alla normativa e standard di riferimento e ai loro aggiornamenti.

Si occupa di fornire le linee guida su tutti gli aspetti archivistici del servizio e ne verifica l'applicazione; ciò si applica in particolare alle **Convenzioni**, ai **Disciplinari tecnici**, alla definizione dei modelli di *pacchetti informativi*, Alla definizione degli aspetti non operativi delle procedure, alla gestione della documentazione interna al servizio.

Quest'area si occupa inoltre del monitoraggio complessivo del processo di conservazione e ne garantisce la correttezza, provvedendo alla sottoscrizione digitale dei *pacchetti informativi*.

Dal punto di vista delle nuove applicazioni quest'area contribuisce alla definizione dei requisiti funzionali, garantendone la coerenza con le esigenze del processo di conservazione.

Infine, quest'area mantiene le relazioni con gli enti convenzionati e con gli organismi di sorveglianza e di indirizzo (MiC, Soprintendenze archivistiche, AgID), nonché con altri soggetti interessati a sviluppare azioni comuni nell'ambito della conservazione.

AREA SERVIZI TECNOLOGICI E INFRASTRUTTURE, con funzione di presidio della gestione dei servizi di conservazione e dell'infrastruttura informatica di ParER. Il Responsabile di tale area svolge le attività quale Responsabile dei sistemi informativi per la conservazione in base alle mansioni indicate in precedenza.

L'infrastruttura tecnologica che ospita il *Sistema di conservazione*, nonché tutti i servizi necessari al suo funzionamento, è in parte ospitata presso i **data center** della Regione Emilia-Romagna uno contenente il sito primario e l'altro il sito di **disaster recovery**.

Ambedue i **data center**, descritti in dettaglio nel capitolo 8, sono situati sul territorio nazionale, per cui deve considerarsi applicabile la normativa nazionale.

AREA TECNOLOGIE E SVILUPPO DEI SISTEMI DI CONSERVAZIONE, con le funzioni di presidio dei sistemi informatici e di gestione dei rapporti con i fornitori dei servizi tecnologici agli enti, per l'interfacciamento di ParER.

In quest'area è prevista la figura di un Responsabile dello sviluppo e della manutenzione del *Sistema di conservazione*, con le mansioni e i compiti indicati in precedenza, per i quali è supportato dalle figure dell'Area.

Sono inoltre previste altre figure: analista informatico (o "analista di sistemi informativi"), analista funzionale (o "Analista di business") e tecnico informatico (o "Analista Programmatore"). L'analista informatico è il gestore delle relazioni con i fornitori degli enti che si vogliono interfacciare con ParER e del supporto tecnico per la definizione delle specifiche tecniche, la progettazione e la validazione delle funzionalità ed evoluzioni del software di conservazione, ivi incluse le problematiche di autenticazione e di sicurezza informatica.

L'analista funzionale è responsabile delle attività di analisi dei requisiti e delle funzionalità che il *Sistema di conservazione* deve garantire nel tempo per poter erogare il servizio richiesto, partecipando alle diverse fasi di progettazione delle funzionalità del *Sistema di conservazione* e delle sue evoluzioni, dallo studio di fattibilità alle fasi di analisi e realizzazione, rilascio e collaudo; la rilevazione e l'analisi critica delle esigenze di evoluzione del sistema; il coinvolgimento nella

reingegnerizzazione dei processi legati alla conservazione e nella scelta dell'evoluzione dell'architettura e delle funzionalità del sistema.

I tecnici informatici sono i soggetti addetti allo sviluppo e all'evoluzione del *Sistema di conservazione*. Tra le loro mansioni figurano la traduzione delle analisi dei requisiti e delle funzioni in specifiche tecniche del *Sistema di conservazione*; lo sviluppo delle evoluzioni software del *Sistema di conservazione*; la realizzazione dei test e della messa in esercizio delle nuove versioni dell'applicativo di conservazione; la realizzazione delle attività di verifica, manutenzione e aggiornamento del *Sistema di conservazione* in uso; lo sviluppo e la manutenzione delle componenti di sicurezza dell'applicativo di conservazione.

Il personale addetto allo sviluppo opera anche nella manutenzione del sistema in esercizio, quando se ne presente la necessità, in base a piani di lavoro che tengono conto sia delle esigenze di nuovi sviluppi che delle esigenze di manutenzione del sistema in esercizio.

AREA ESERCIZIO DEI SERVIZI DI CONSERVAZIONE, con funzioni di gestione operativa dei servizi di conservazione.

Prevede al suo interno la figura di un Responsabile, con mansioni di coordinamento delle attività operative a supporto del processo di conservazione. Il Responsabile si occupa di coordinare le attività delle risorse dell'area, in modo tale da garantire adeguati livelli di servizio agli Enti che conservano presso ParER. Oltre a gestire il ciclo di pianificazione, esecuzione e controllo delle attività, si occupa di definire i processi e le procedure operative del servizio, in coerenza con le linee guida emesse dall'Area Funzione Archivistica di Conservazione; nel caso di nuovi sviluppi applicativi fornisce i requisiti di massima del servizio e verifica i documenti prodotti dall'Area Tecnologia e Sviluppo dei Sistemi di Conservazione.

All'interno dell'area 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

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	Resp. Sicurezza dei Sistemi	Resp. Funzioni di Supporto e Qualità	Resp. Funzione Archivistica Conservazione	Resp. Esercizio di conservazione	Resp. Servizi Tecnologici Infrastrutture	Resp. Tecnologie e Sviluppo dei Sistemi	Resp. Trattamento Dati Personali
Gestione delle Convenzioni	A		R	C	C			
Attivazione del servizio di conservazione	A			C	R			
Gestione del processo di conservazione				A	R			
Chiusura del servizio di conservazione	A			C	R			
Gestione Infrastruttura	I			I	I	A, R	I	
Sviluppo e manutenzione del sistema	I			I	I	I	A, R	
Monitoraggio del servizio di conservazione	A			R	R	R		
Gestione del Sistema di Qualità	C		A, R	C	C	C	C	C
Verifica di conformità a norme e std di conservazione			I	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	A, R	I	I	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**.

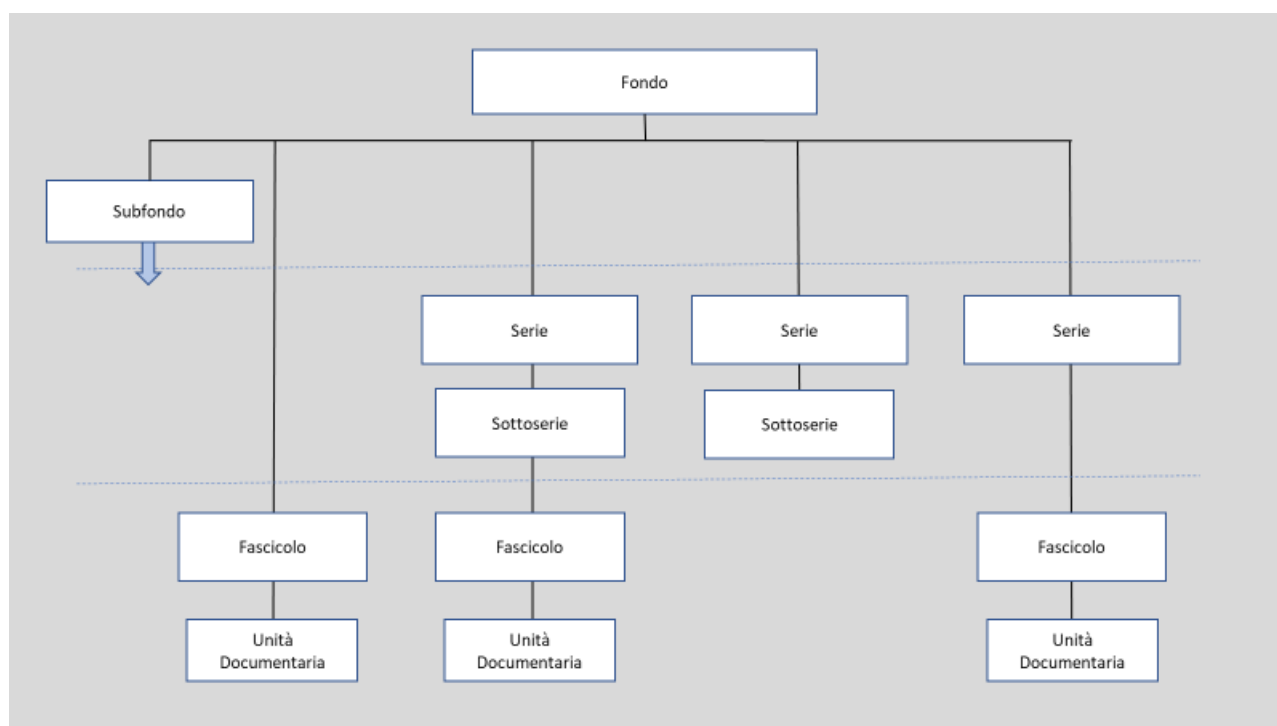


Figura 3 - Modello di ordinamento di archivio derivato da ISAD

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**, l'Area 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.

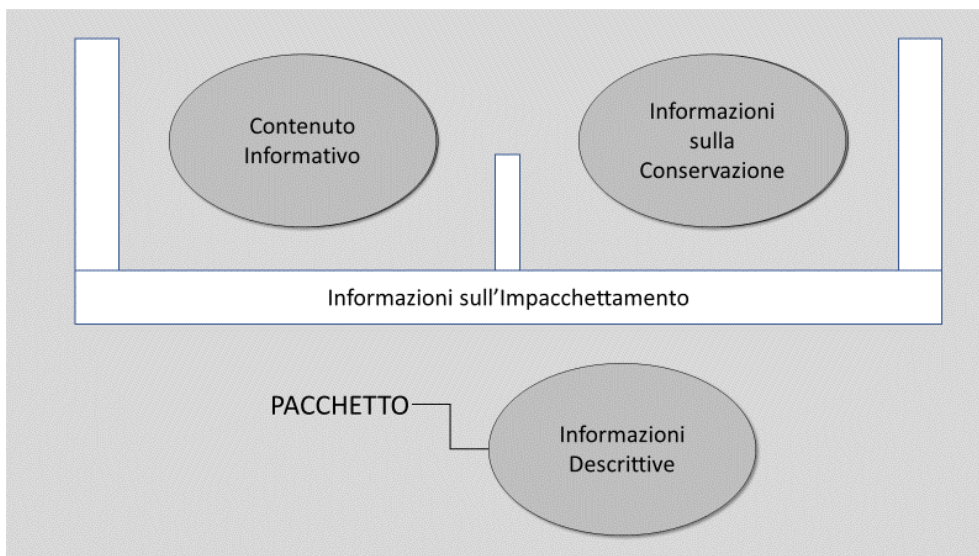


Figura 4 - Pacchetto informativo (da OAIS)

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 successiva).

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.

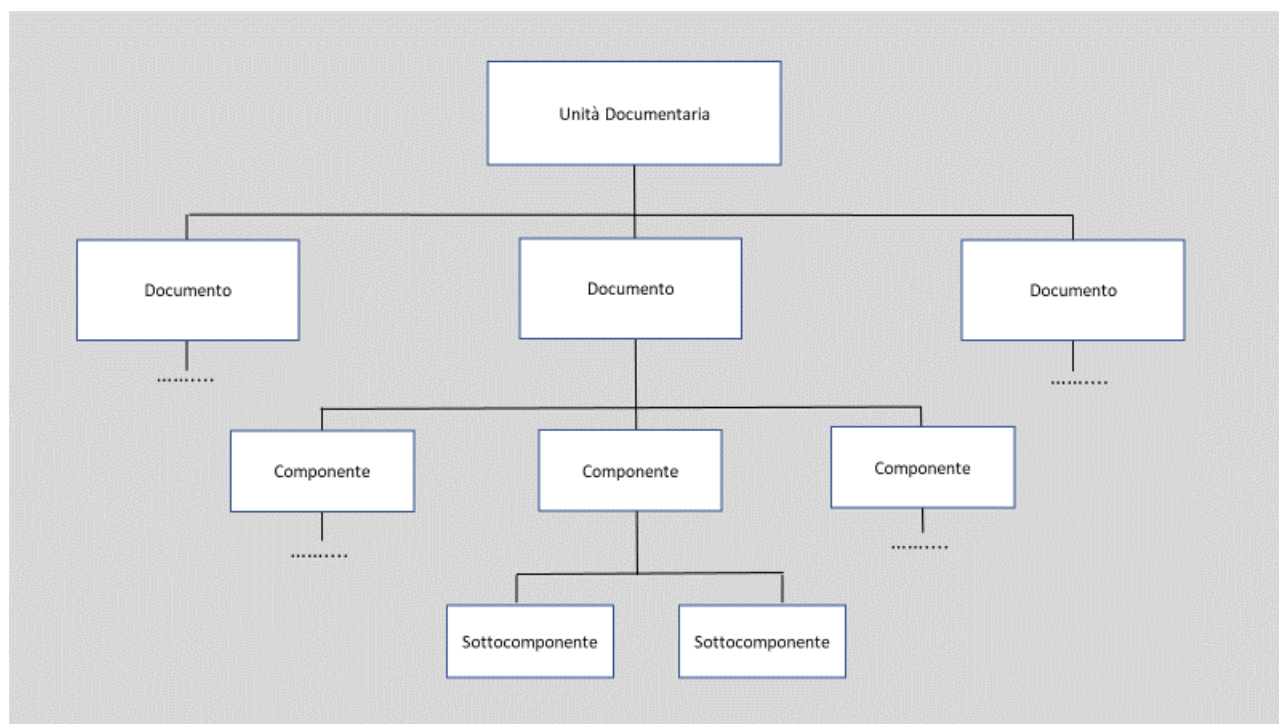


Figura 5 - Struttura dell'Unità documentaria

in un momento successivo rispetto a quello del **Documento principale**, per fornire 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 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** 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**. Normalmente tale contenuto 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 idonee 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 da ogni *Produttore* e 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 vari 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 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> .
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> .

Elemento del pacchetto informativo	Articolazione dell'elemento	Descrizione
Informazioni su l'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'essa 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 della **Convenzione** tra il *Produttore* e la Regione Emilia-Romagna con le modalità indicate nella **Convenzione** stessa e dettagliate nel **Disciplinare tecnico**. La **Convenzione** medesima disciplina anche la chiusura del servizio in caso di recesso o scadenza della **Convenzione** stessa, 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 su una logica di conservazione caratterizzata dal **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.

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".

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 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 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 una serie di verifiche automatiche. Nel caso in cui le verifiche abbiano successo, il **versamento** viene accettato, il SIP acquisito per la sua *presa in carico* e generato in modo automatico dal Sistema 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 si avvia 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 una serie di 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 una serie di 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 *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;
- **i controlli di coerenza e 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 questo frangente, sono illustrati nel documento "Specifiche tecniche dei servizi di versamento".

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

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

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 elencate 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 e a effettuare 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 risolubili: nel caso in cui un **versamento** sia stato rifiutato per la presenza di anomalie che il *Produttore* giudica non risolubili, il **versamento** può essere marcato come non risolubile 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.).	Produttore 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 gestibile dal <i>Sistema di conservazione</i> .	Il <i>Produttore</i> segnala il problema a ParER, che si attiverà per la sua risoluzione.

Tipo anomalia	Descrizione	Modalità di gestione
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 ad 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 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.

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

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.

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 del 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, relative 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.

L'AIP dell'**Unità documentaria** prodotto viene firmato dal Responsabile della funzione di archivistica di conservazione.

La firma 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 firma 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 firmata, è inserita negli AIP delle singole **Unità documentarie**.

Nel caso di **Versamento in archivio**, invece, la firma degli AIP delle **Unità documentarie** avviene attraverso la firma 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 firmati dal Responsabile della funzione archivistica di conservazione 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*.

Con la firma 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 apposite 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, con periodicità quadrimestrale, 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, ognuno 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**, PI SIP, **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 apposite 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 specifiche funzionalità dell'interfaccia web del Sistema o utilizzando 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. e trasmesso dal *Produttore* all'Autorità di vigilanza che, in base alle norme vigenti, deve fornire il nulla-osta 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 riscontrasse 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

La **Convenzione** 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**.

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 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 comprendendo le copie 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 prelevare 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.

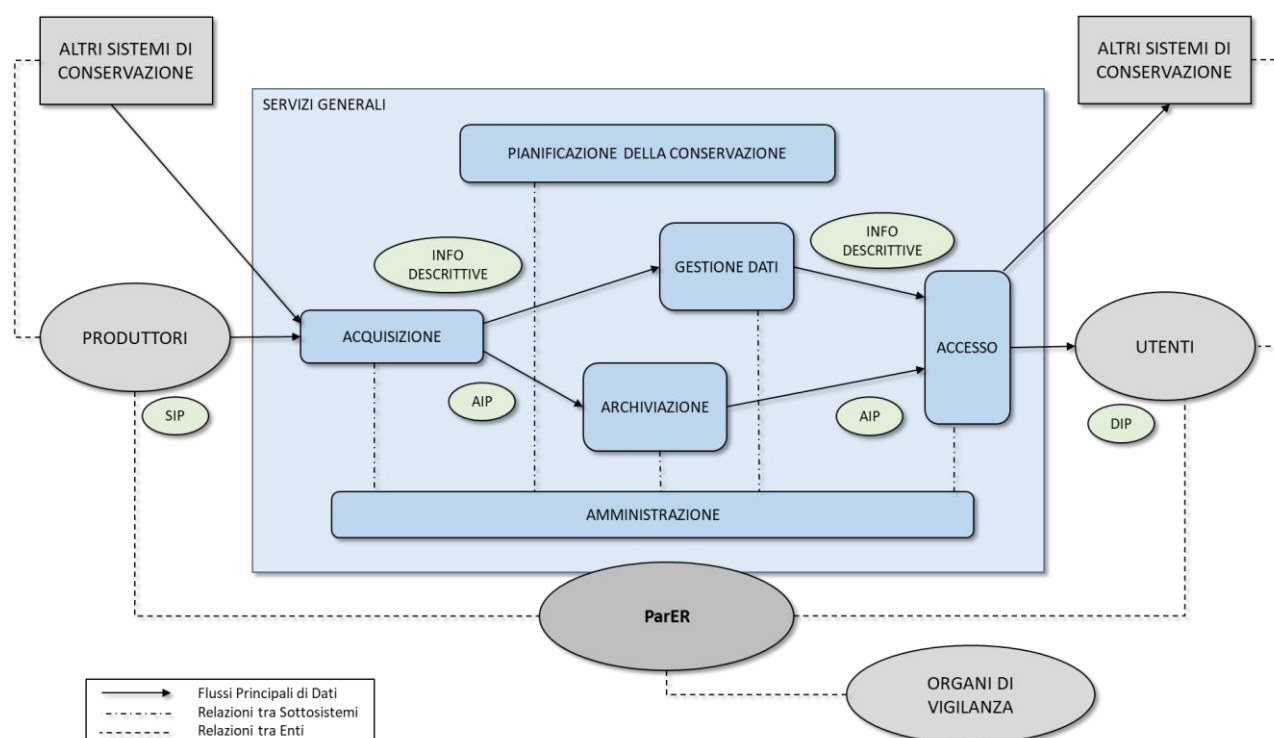


Figura 6 - Schema logico del Sistema di conservazione

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, configurandosi 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, nei test su nuovi componenti hardware, e in altro ancora.

Normalmente 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): 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.

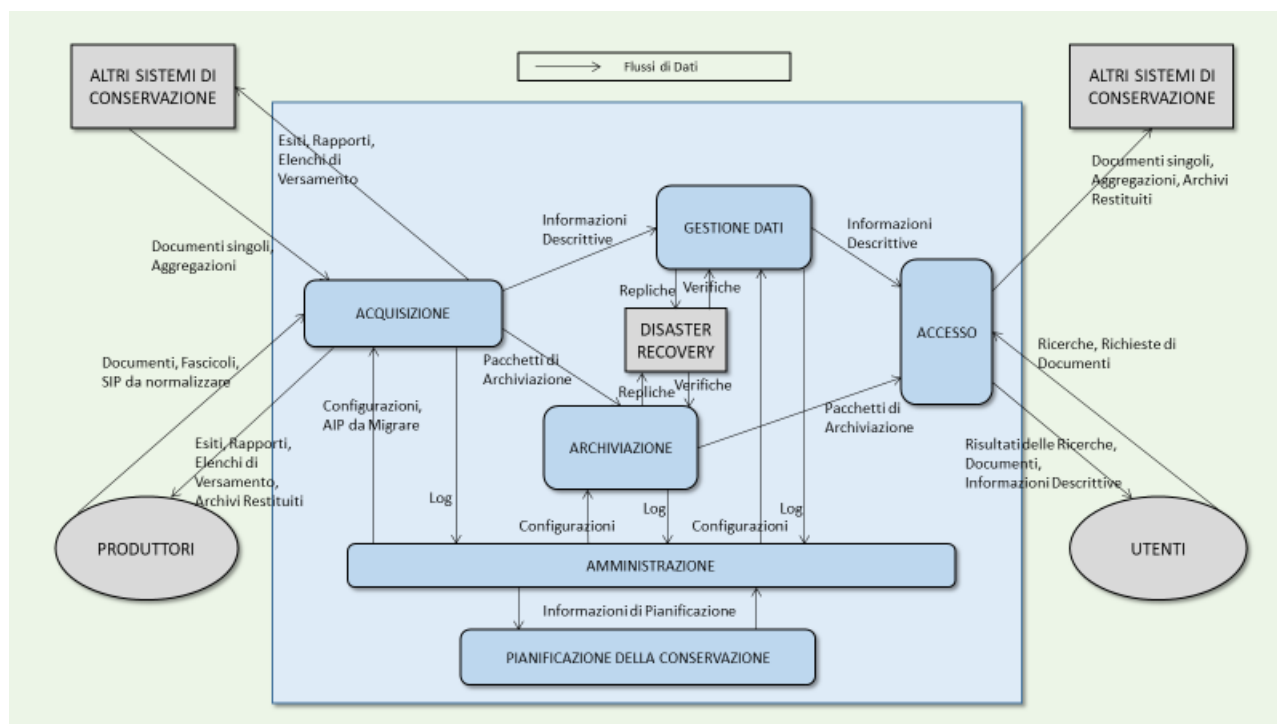


Figura 7 - Flussi di dati nel Sistema di conservazione

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 di vari livelli 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.

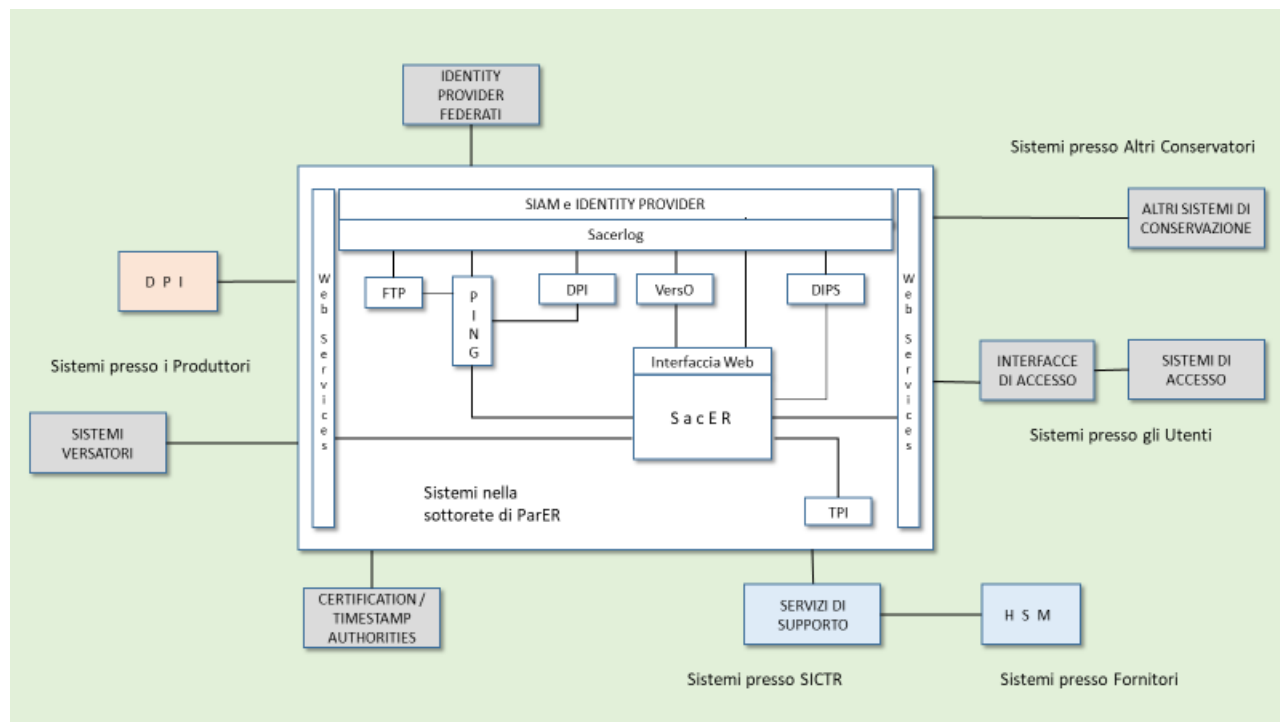


Figura 8 - Schema Tecnologico del Sistema di conservazione

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 da ParER direttamente o tramite il **SIDDT** della 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'impackettamento, 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 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 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 al Piano di Sicurezza;
- 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 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 determinate 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, tramite 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. Utilizza un'interfaccia web e quindi non richiede l'installazione di alcun software sulla stazione di lavoro del *Produttore*.

Il suo utilizzo tipico è per 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 un **IdP** federato, 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 richieda 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 sono state definite durante nella 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 per conoscere a quale punto del processo è giunto il SIP da un operatore tramite interfaccia web o dal sistema versante tramite opportuno **Web Service**.

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, 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.

In particolare, 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 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 secondario 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 può accettare anche l'autenticazione effettuata su altri **IdP** opportunamente federati nel rispetto delle logiche di sicurezza richieste dalle Politiche della Sicurezza di ParER.

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 altri sistemi federati.

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

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, ogniquale volta 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.iien.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 SIDDT 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 dei malfunzionamenti, 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** open source RT (Request Tracker) messo a disposizione dal SIDDT;
- 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 utile 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;

- 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;
- SELF, sistema di e-Learning federato 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 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 ed 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 **S3**, mentre il sistema di gestione dello **storage** su cassetta (TMS) 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 a Parma, ma gestito per i sistemi di ParER dal SIDDIT, che ha lo scopo di subentrare come sito di **Disaster recovery** nel caso di caduta irreparabile del sito primario.

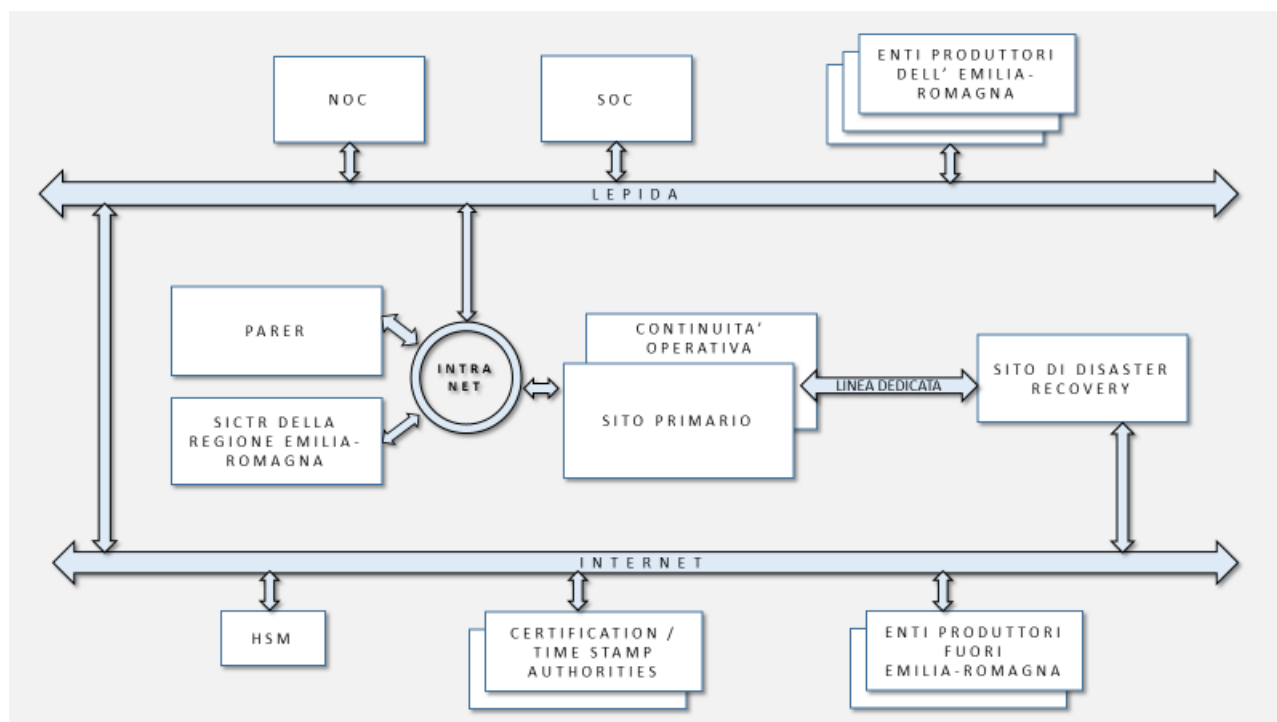


Figura 9 - Schema Infrastrutturale del Sistema di conservazione

Il sito primario e il sito di Parma sono gestiti dal SIDDIT della 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.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** del SIDDIT; 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 del SIDDIT 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, inclusi quelli installati nella sottorete del SIDDIT, 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** 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 (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** del SIDDT.

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**.

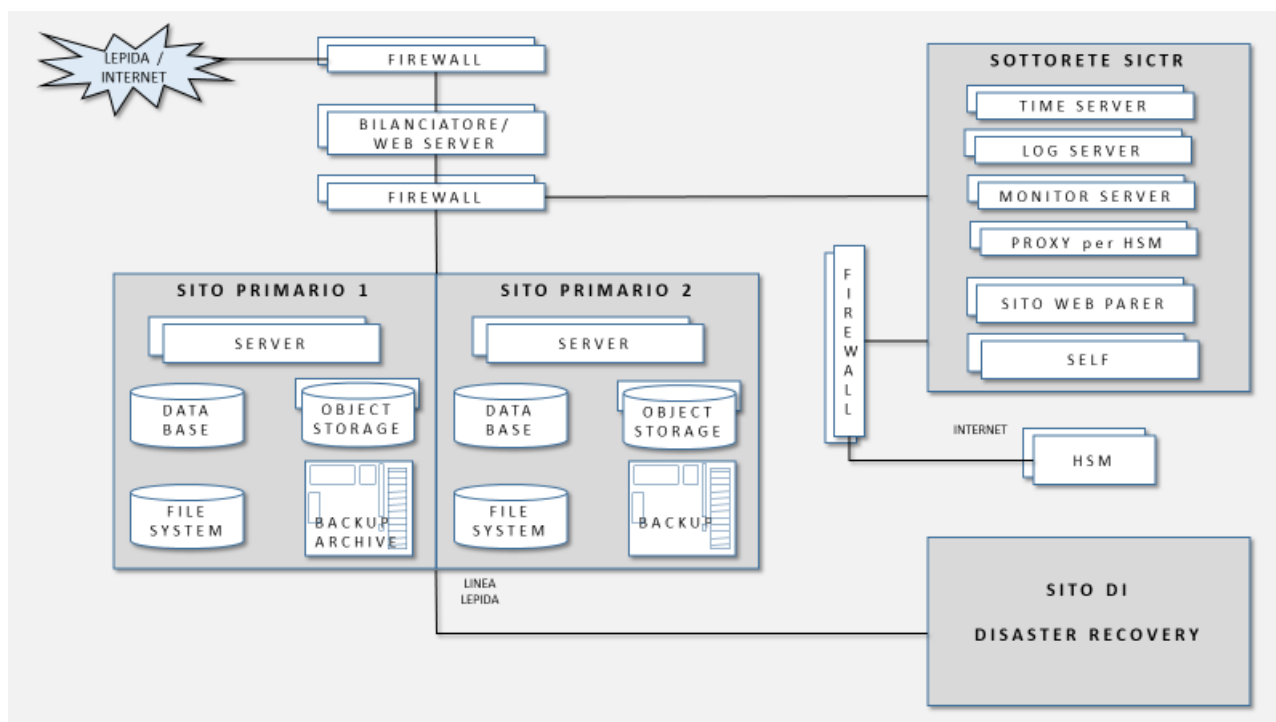


Figura 10 - Schema dei Sistemi di ParER

I servizi ausiliari, in quanto di interesse di tutta l'infrastruttura regionale, sono ospitati su server della sottorete del SICTR; 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.iien.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.

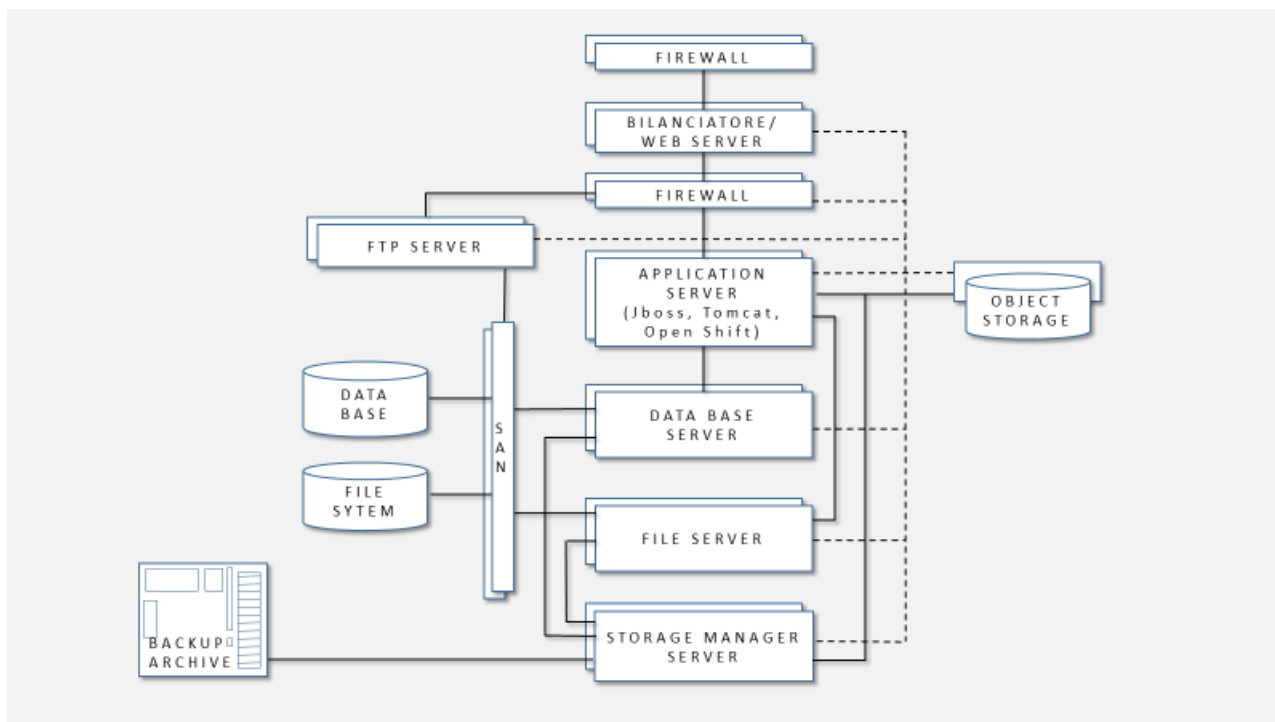


Figura 11 - Schema del Sito Primario

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 Management System (TMS), 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;
- Storage Manager Tivoli (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 il framework JPA 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 secondario 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 TMS 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 ParER si occupa di garantire la cancellazione sicura delle informazioni presenti nel sistema; a tal fine negli accordi con i gestori dell'infrastruttura ParER richiede esplicitamente l'impegno ad adottare idonei accorgimenti e misure per la distruzione dei supporti di memorizzazione dei dati, una volta dismessi.

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

8.4 Procedure di gestione e di evoluzione

La gestione del *Sistema di conservazione* è affidata a diversi gruppi di operatori di ParER, 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, 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'Area Esercizio dei Servizi di Conservazione di ParER presidia le attività descritte nello specifico punto del paragrafo 5.2.

L'Area di Gestione dei Servizi e delle Infrastrutture di ParER 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; è suo compito indirizzare le attività di gestione che sono svolte dal SIDDT della Regione Emilia-Romagna ai fini della gestione del sito primario incluso il sito di **Continuità Operativa** e verificarne il buon funzionamento; infine si occupa di verificare il buon funzionamento dell'infrastruttura di **Disaster Recovery**.

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

8.4.2 Gestione delle utenze

La procedura riportata nel documento "Gestione utenze" e schematizzata in figura descrive le modalità con cui viene garantita la corretta gestione dei soggetti che hanno accesso al sistema

di conservazione, con particolare riguardo alla sicurezza dei dati e delle informazioni conservate, nel rispetto della politica generale di controllo degli accessi di ParER.

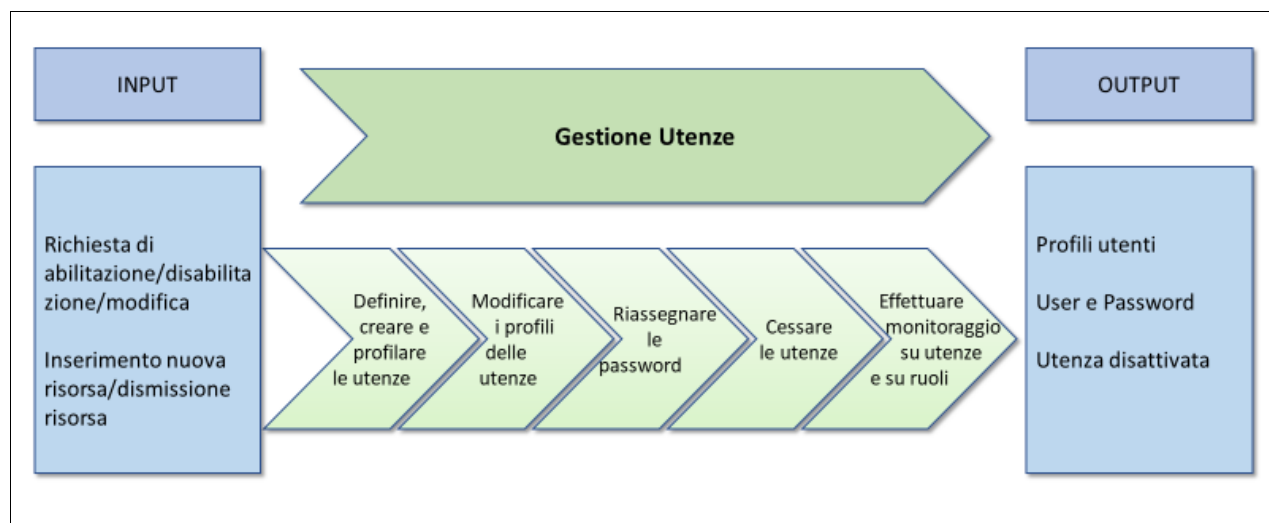


Figura 12 - Procedura di Gestione utenze

La procedura descrive inoltre il metodo seguito per la gestione delle password in coerenza con quanto descritto nella *Politica sulla sicurezza delle informazioni del servizio di Conservazione*.

In particolare, in caso di Creazione di nuovo utente, Riattivazione e Reset di password il sistema genera casualmente le password, le memorizza in forma criptata e le presenta temporaneamente a video in modo che l'operatore possa comunicarle all'utente.

L'operatore di Help Desk di ParER provvede a creare l'utenza nel sistema inviando tramite due e-mail separate lo user-id e la password, che l'utente deve necessariamente cambiare al primo accesso.

Nel caso in cui l'utente abbia dimenticato la password il suo Referente può chiederne la riassegnazione (reset) inviando l'opportuna richiesta tramite una comunicazione formale. L'operatore di Help Desk di ParER (o del gestore esterno) provvede a caricare la richiesta in riferimento alla comunicazione, desumendo le informazioni dal testo della comunicazione o dal file allegato.

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 accreditamento.

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

8.4.3 Gestione dei Malfunzionamenti

La procedura riportata nel documento "Gestione delle Richieste di Informazioni, Reclami e Segnalazioni" e schematizzata in figura descrive la maniera in cui ParER tratta le richieste di informazioni, i malfunzionamenti e gli eventuali reclami da parte degli utenti del sistema.

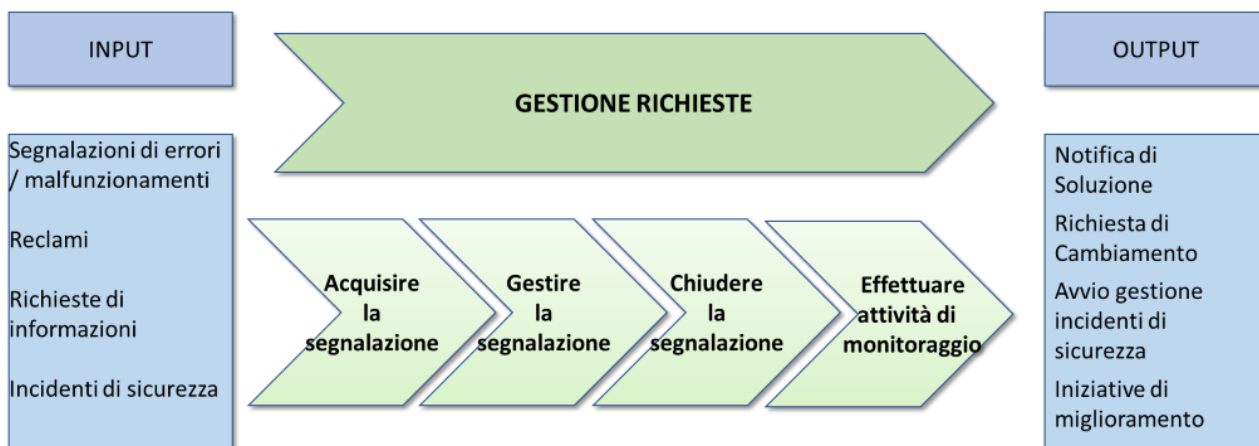


Figura 13 - Procedura di Gestione delle Richieste di Informazioni, Reclami e Segnalazioni

La gestione dei malfunzionamenti può coinvolgere diverse strutture di ParER, 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'Area Esercizio dei Servizi di Conservazione, dall'Area Funzione Archivistica di Conservazione di ParER o dall'Area Tecnologia e Sviluppo Sistemi di Conservazione, mentre malfunzionamenti di natura tecnica possono essere segnalati dall'Area di Gestione dei Servizi e delle Infrastrutture del ParER dal SIDDT della Regione Emilia-Romagna.

Allo stesso modo diverse possono essere le strutture che intervengono nella soluzione del malfunzionamento: l'Area Esercizio dei Servizi di Conservazione è normalmente in grado di risolvere i malfunzionamenti che non sono dovuti a problemi tecnici, eventualmente coinvolgendo il 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 di Gestione dei Servizi e delle Infrastrutture, che coordina gli interventi del; l'Area Tecnologie e sviluppo 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 di ParER e il SIDDT 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 delle informazioni del sistema di conservazione* di ParER.

La procedura riportata nel documento "Gestione incidenti di sicurezza" e schematizzata in figura 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:

- gestire gli eventi;

- gestire gli incidenti di sicurezza;
- gestire le attività post-incidente.

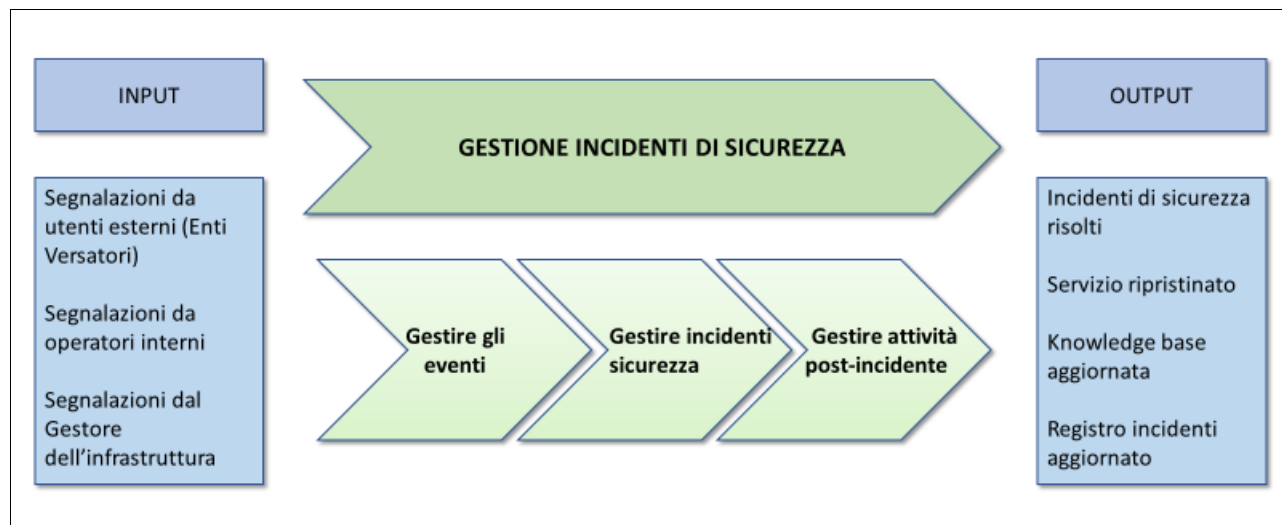


Figura 14 - Procedura di Gestione incidenti di sicurezza

All'interno della Procedura, ParER ha definito le responsabilità nell'ambito della gestione degli incidenti di sicurezza.

In particolare,

- gli Enti convenzionati 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;
 - notificare tempestivamente agli Enti convenzionati 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, 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 all'Area Esercizio dei Servizi di Conservazione, SAL per l'evoluzione degli applicativi, cui partecipano i responsabili delle diverse aree di ParER e i responsabili dei fornitori dello sviluppo e, quando necessario, SAL per l'evoluzione dell'infrastruttura, cui partecipano anche i responsabili del SIDDT. 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).

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

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" e la cui procedura è schematizzata in figura.

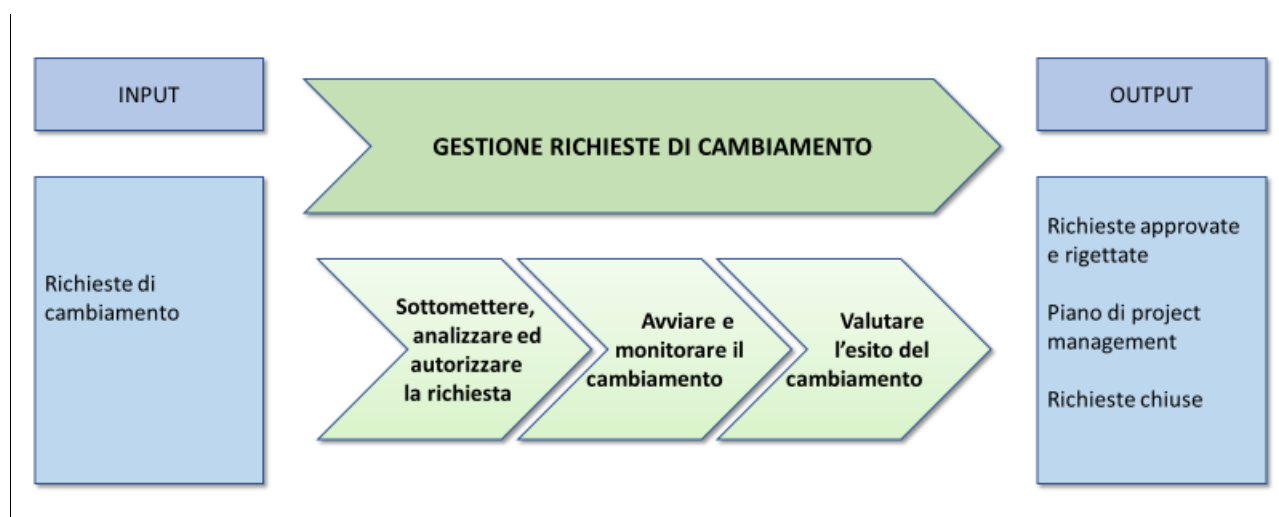


Figura 15 - Procedura di Gestione richieste di cambiamento

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 nell'area 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 delle diverse Aree 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" e schematizzata in figura 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'Area Tecnologie e Sviluppo dei 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.

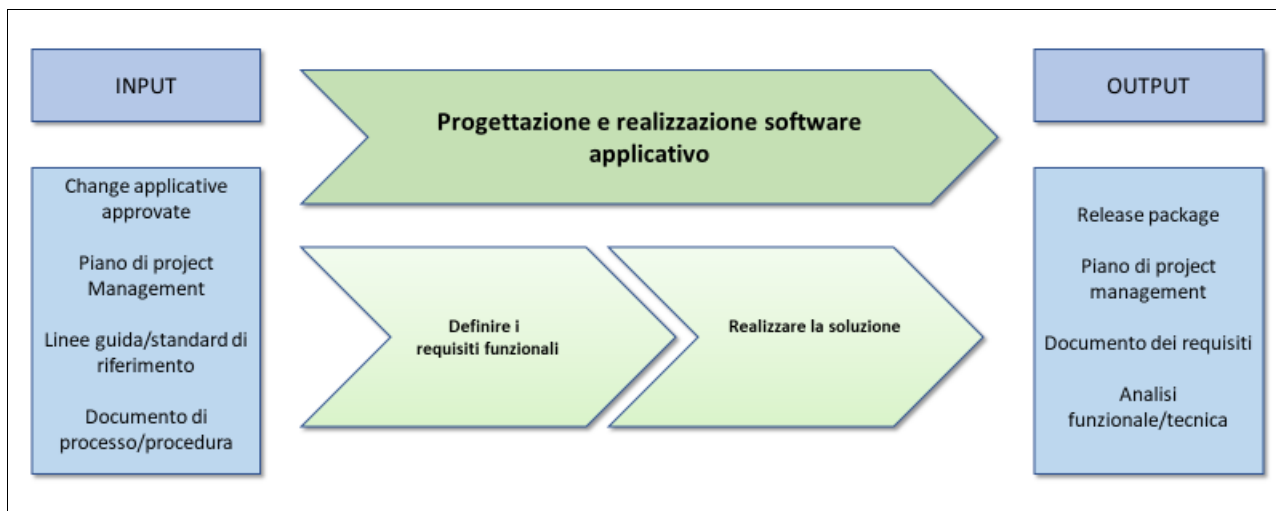


Figura 16 - Procedura di Progettazione e realizzazione di software applicativo

I test della nuova **release** vengono condotti nell'ambiente di Test sulla base del piano di test sotto responsabilità dell'Area Tecnologie e Sviluppo con il supporto dell'Area Esercizio dei Servizi Archivistici. 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 il personale dell'Area Tecnologie e Sviluppo dei Sistemi di Conservazione e il personale dell'Area Esercizio Servizi di Conservazione, 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.

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

8.4.8 Gestione dei Rilasci

Prima di effettuare il rilascio in preproduzione e produzione, L'Area Tecnologie e Sviluppo 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'Area Tecnologie e Sviluppo concorda con l'Area di Gestione dei Servizi e delle Infrastrutture e con l'Area Esercizio dei Servizi di Conservazione il

piano di rilascio della nuova **release** nell'ambiente di preproduzione e successivamente nell'ambiente di produzione, e richiede al SIDDT 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".

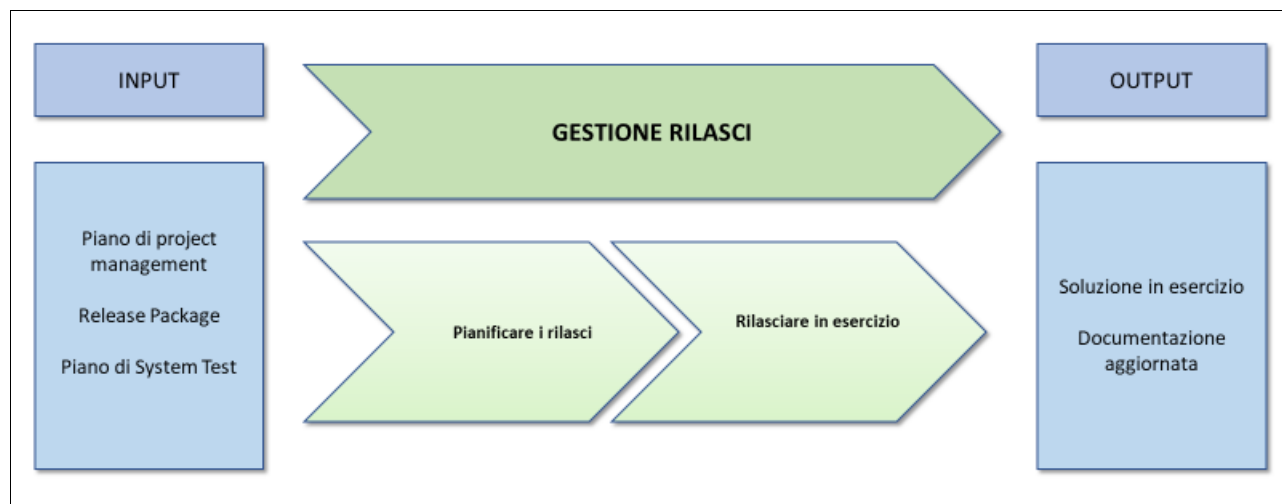


Figura 17 - Procedura di Gestione dei rilasci

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, Gestore dell'infrastruttura e Outsourcer) 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 al Gestore dell'infrastruttura e all'Outsourcer e garantendo il rispetto dei tempi pianificati.

Il SIDDT 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 sistema di log (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 del SIDDT, in quanto si ritiene dopo tale periodo di tempo abbiano esaurito la loro utilità.

I 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.

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

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 del **SIDDT**, che provvede a produrre e rendere disponibili periodicamente all'Area Gestione dei servizi e delle infrastrutture di ParER report di controllo di tutte le aree infrastrutturali (rete, server, **storage**, database, **backup**). Si tratta di report tra loro eterogenei, ottenuti per rielaborazione e integrazione delle informazioni prodotte per via automatica dal software di base dei sistemi e dal software di monitoraggio tecnico installato sui medesimi e dai log delle attività svolte dal personale tecnico. Analoghi report vengono prodotti dalla gestione del **Disaster recovery**.

Periodicamente i report di monitoraggio tecnico vengono esaminati congiuntamente dall'Area Gestione dei servizi e delle infrastrutture di ParER e dall'Area Tecnologie e sviluppo sistemi di conservazione, con lo scopo di individuare eventuali aree di miglioramento negli aspetti tecnici dell'applicativo.

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

9.2 Funzionalità per la verifica e il mantenimento dell'integrità degli archivi

Le procedure di monitoraggio illustrate 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 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 secondario

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 si occupa di gestire tutti i metadati trattati nel Sistema. La gestione sistemistica del Data Base è effettuata 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 si occupa di gestire tutti i **Componenti** (files) che transitano nel Sistema, a parte i file memorizzati

temporaneamente nel **file system** e definitivamente nello storage a cassette, è effettuata 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** 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 è effettuata tramite prodotti certificati da IBM, ed è tracciata nel *log di sistema*;
- per quanto attiene invece ai **Componenti** memorizzati su storage a cassette, l'integrità nel singolo sito è garantita da funzionalità intrinseche del modulo di archiving di TMS per tutti i dati archiviati su cassetta; queste ultime 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 la copia del file dal **Blob** del Data Base all'**object storage**.

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 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* 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 secondario (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.

Ambito del sistema	Misure adottate
	Le procedure di recupero debbono essere 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 TMS)

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

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'Area Esercizio del Sistema di Conservazione, 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
- Accreditamento dei Conservatori secondo le modalità definite da AgID con la circolare n.65/2014
- Qualificazione nel Cloud Marketplace di AgID.

Gli audit interni costituiscono momento fondamentale per il conseguimento e il mantenimento delle certificazioni ISO, dell'accreditamento e della qualificazione.

ParER si impegna a fornire su richiesta dei propri Enti convenzionati (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 convenzionati.

Dall'altra parte, ParER in tutte le convenzioni con i fornitori di infrastruttura, si riserva la possibilità di effettuare a sua volta Audit mirati allo scopo di verificare il mantenimento delle condizioni contrattuali stabilite.

La procedura riportata nel documento "Audit del SGI" e schematizzata in figura descrive l'insieme di attività e responsabilità legate alla pianificazione, conduzione e documentazione degli Audit di ParER.

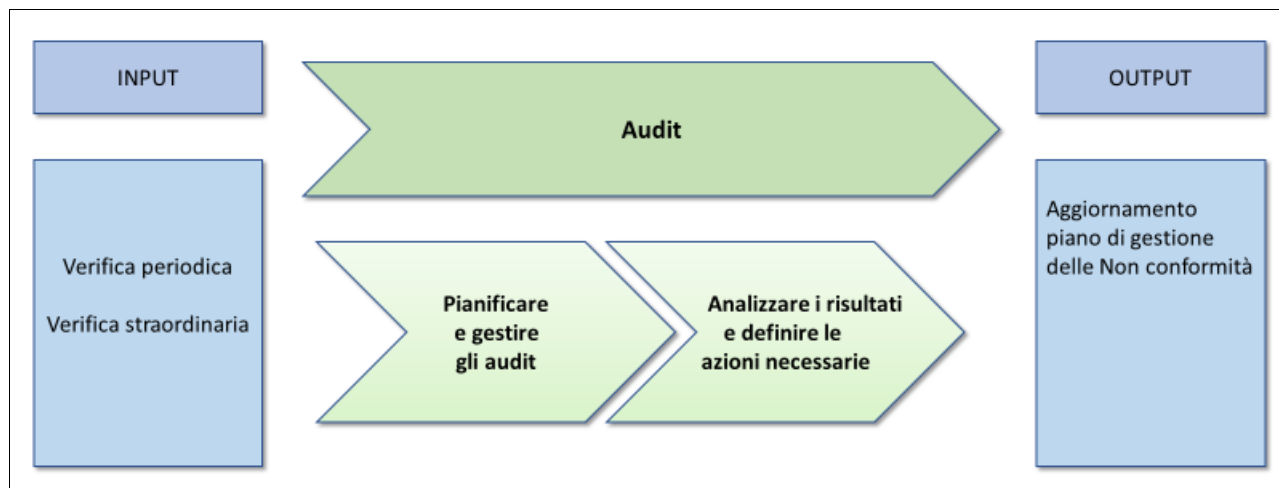


Figura 18 - Procedura di Audit del SGI

Gli Audit vengono eseguiti su base periodica, o in modo straordinario, se i Responsabili lo richiedono, per valutare il grado di applicazione e di efficacia di quanto indicato nella "Politica di sicurezza del sistema di conservazione", nella "Politica per la qualità" e nei documenti ad esso collegati e per orientare la successiva gestione delle Non Conformità riscontrate.

Gli ambiti di verifica sono sia i processi interni che i processi esterni (outsourcing).

Le eventuali non conformità rilevate nei processi di audit vengono gestite seguendo la procedura descritto nel documento "Gestione delle Non Conformità" e schematizzata in figura.

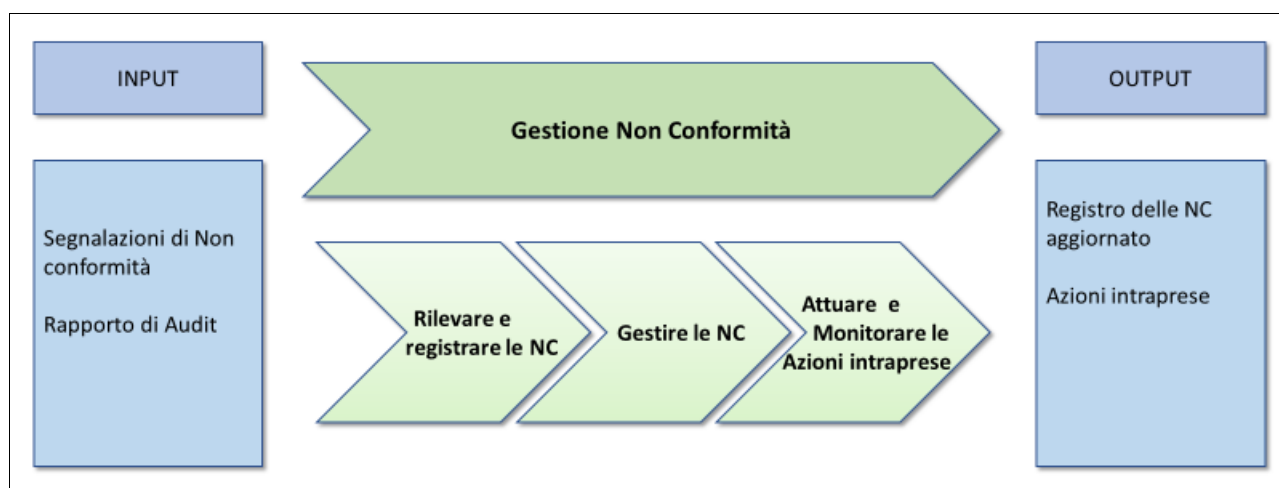


Figura 19 - Gestione delle Non Conformità

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 sulla sicurezza delle informazioni del servizio di Conservazione" 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.

Di seguito in figura viene rappresentato un quadro di sintesi della procedura relativa alle Verifiche Tecniche e VA/PT (Vulnerability Assessment / Penetration Test), che si implementa nell'ambito dei sistemi e degli applicativi in esercizio.

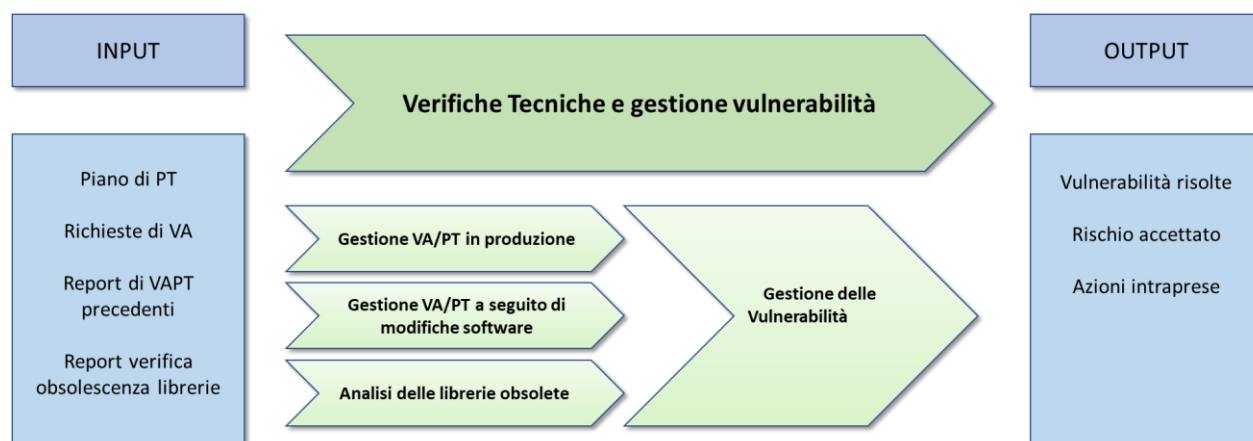


Figura 20 - Procedura di Verifiche Tecniche e VA/PT

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.

Con deliberazione di Giunta regionale n. 2169 del 20 dicembre 2017, ai sensi dell'art. 37 del GDPR, è stato designato il Responsabile della protezione dei dati (DPO - Data Protection Officer), nella persona del dirigente regionale Dott. Ing. Alessandro Zucchini, specificandone le caratteristiche organizzative e i compiti assegnati. I compiti e le responsabilità del DPO sono stati poi ulteriormente dettagliati nell'allegato A della deliberazione di Giunta regionale n. 1123 del 16 luglio 2018. Tali compiti sono svolti anche per tutte le strutture della Giunta regionale e delle Agenzie e Istituti regionali ai sensi della lettera b), comma 3 bis, art. 1, L.R. 43/2001.

Con successiva deliberazione della Giunta regionale n. 2329 del 22 novembre 2019, a seguito del collocamento a riposo del Dott. Ing. Alessandro Zucchini, dal 1° gennaio 2020 il Responsabile della protezione dei dati (DPO) per le strutture della Giunta e dell'Assemblea Legislativa della Regione Emilia-Romagna e delle Agenzie e Istituti regionali ai sensi della lettera b), comma 3 bis, art. 1, L.R. 43/2001, è stato designato tramite contratto di servizio con la Società LEPIDA S.C.P.A., che lo ha individuato nella persona di Sergio Duretti. Tale designazione esterna del DPO ha durata triennale, salvo mutate condizioni organizzative interne all'Amministrazione che permettano di procedere alla nomina interna del DPO

Il DPO funge da punto di contatto per l'autorità di controllo per questioni connesse al trattamento dei dati personali.

Nel succitato 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 o convenzioni 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 Responsabili di Servizio nonché 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/convenzioni) 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 Servizio Polo Archivistico dott. Ing. Marco Calzolari, opportunamente delegato, 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 convenzione 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 della **Convenzione/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 **Convenzione/Accordo** sottoscritta con i *Produttori*.

Coerentemente a quanto espresso, il Responsabile del Servizio 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.

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 Servizio 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 del servizio di Conservazione	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 sulla sicurezza delle informazioni del servizio di Conservazione	pubblicata nel sito di ParER: https://poloarchivistico.regione.emilia-romagna.it , in "Documentazione"
Piano della Sicurezza	share ParER Doc / Area riservata
Piano di Continuità Operativa	share ParER Doc / Policy
DPIA	Share regionale / Area riservata
Gestione incidenti di sicurezza	share ParER Doc / Procedure / Supporto
Gestione richieste di cambiamento	share ParER Doc / Procedure / Supporto
Progettazione e realizzazione di software applicativo	share ParER Doc / Procedure / Supporto
Gestione dei rilasci	share ParER Doc / Procedure / Supporto
Audit del SGI	share ParER Doc / Procedure / Supporto
Gestione delle Non Conformità	share ParER Doc / Procedure / Supporto
Verifiche tecniche e VA/PT	share ParER Doc / Procedure / Supporto
Registro dei formati	SacER
Gestione utenze	share ParER Doc / Procedure / Realizzazione del Servizio
Procedura di restituzione dell'archivio	share ParER Doc / Procedure / Realizzazione del Servizio
Gestione di richieste e malfunzionamenti	share ParER Doc / Procedure / Supporto

Si riporta l'elenco dei documenti allegati al presente Manuale:

- **Allegato 1 "Normativa e standard di riferimento"**
- **Allegato 2 "Registro dei responsabili"**

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

Allegato 10 – Formati accettati

Nella Tabella 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 da parte dell'Ente conservatore PARER.

In base all'idoneità in relazione alla conservazione a lungo termine i formati sono classificati come segue:

- **IDONEI:** sono i formati che per le loro caratteristiche di standardizzazione, di apertura, di sicurezza, di portabilità, di immodificabilità, di staticità e di diffusione reputati idonei alla conservazione a lungo termine;
- **GESTITI:** sono i formati non ritenuti idonei per la conservazione a lungo termine ma che possono essere opportunamente migrati in Formati idonei;
- **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

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/octet-stream	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
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

Formato versato ammesso	Mimetype	Idoneità alla conservazione
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
CSV.P7M	text/plain	IDONEO
CSV.P7S	text/plain	IDONEO
DAT	application/vnd.ms-tnef	DEPRECATO
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
DER.ASICE	application/x-x509-ca-cert	GESTITO
DER.ASICS	application/x-x509-ca-cert	GESTITO
DER.P7M	application/x-x509-ca-cert	GESTITO
DER.P7S	application/x-x509-ca-cert	GESTITO
DIB	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
DOCX	application/ vnd.openxmlformats-officedocument.wordprocessingml	

Formato versato ammesso	Mimetype	Idoneità alla conservazione
	.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	

Formato versato ammesso	Mimetype	Idoneità alla conservazione
	.template	
GESTITO		
DTD	text/plain	IDONEO
DTD.ASICE	text/plain	IDONEO
DTD.ASICS	text/plain	IDONEO
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
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
EML.ASICS	message/rfc822	IDONEO
EML.P7M	message/rfc822	IDONEO
EML.P7S	message/rfc822	IDONEO
EMLX	message/x-xml	GESTITO
EMLX.ASICE	message/x-xml	GESTITO
EMLX.ASICS	message/x-xml	GESTITO
EMLX.P7M	message/x-xml	GESTITO
EMLX.P7S	message/x-xml	GESTITO
EMZ	application/x-gzip	DEPRECATO
ENC	application/octet-stream	DEPRECATO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
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
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
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
JPE	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
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	GESTITO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
M7M	multipart/mixed	IDONEO
MDB	application/x-msaccess	DEPRECATO
MHT	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
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

Formato versato ammesso	Mimetype	Idoneità alla conservazione
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
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

Formato versato ammesso	Mimetype	Idoneità alla conservazione
PDF.P7M	application/pdf	IDONEO
PDF.P7M.P7M	application/pdf	IDONEO
PDF.P7M.TSD	application/pdf	IDONEO
PDF.P7M.TSR	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
POT	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.sldshow	
IDONEO		
PPSX.ASICE	application/ vnd.openxmlformats-officedocument.presentationml.sldshow	
IDONEO		
PPSX.ASICS	application/ vnd.openxmlformats-officedocument.presentationml.sldshow	
IDONEO		
PPSX.P7M	application/ vnd.openxmlformats-officedocument.presentationml.sldshow	
IDONEO		
PPSX.P7S	application/ vnd.openxmlformats-officedocument.presentationml.sldshow	
IDONEO		
PPT	application/vnd.ms-powerpoint	GESTITO
PPT.ASICE	application/vnd.ms-powerpoint	GESTITO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
PPT.ASICS	application/vnd.ms-powerpoint	GESTITO
PPT.P7M	application/vnd.ms-powerpoint	GESTITO
PPT.P7S	application/vnd.ms-powerpoint	GESTITO
PPTM	application/ vnd.ms-powerpoint.presentation.macro-enabled.12	
GESTITO		
PPTM.ASICE	application/ vnd.ms-powerpoint.presentation.macro-enabled.12	
GESTITO		
PPTM.ASICS	application/ vnd.ms-powerpoint.presentation.macro-enabled.12	
GESTITO		
PPTM.P7M	application/ vnd.ms-powerpoint.presentation.macro-enabled.12	
GESTITO		
PPTM.P7S	application/ vnd.ms-powerpoint.presentation.macro-enabled.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
PSD	image/vnd.adobe.photoshop	GESTITO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
PSD.ASICE	image/vnd.adobe.photoshop	GESTITO
PSD.ASICS	image/vnd.adobe.photoshop	GESTITO
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	application/x-rar-compressed	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
RTF	application/rtf	GESTITO
RTF.ASICE	application/rtf	GESTITO
RTF.ASICS	application/rtf	GESTITO
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

Formato versato ammesso	Mimetype	Idoneità alla conservazione
SGP.ASICE	text/plain	IDONEO
SGP.ASICS	text/plain	IDONEO
SGP.P7M	text/plain	IDONEO
SGP.P7S	text/plain	IDONEO
SHP	application/octet-stream	GESTITO
SHP.ASICE	application/octet-stream	GESTITO
SHP.ASICS	application/octet-stream	GESTITO
SHP.P7M	application/octet-stream	GESTITO
SHP.P7S	application/octet-stream	GESTITO
SHX	application/octet-stream	GESTITO
SHX.ASICE	application/octet-stream	GESTITO
SHX.ASICS	application/octet-stream	GESTITO
SHX.P7M	application/octet-stream	GESTITO
SHX.P7S	application/octet-stream	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
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

Formato versato ammesso	Mimetype	Idoneità alla conservazione
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
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/unknown	DEPRECATO
VCF	text/x-vcard	GESTITO
VCF.ASICE	text/x-vcard	GESTITO
VCF.ASICS	text/x-vcard	GESTITO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
VCF.P7M	text/x-vcard	GESTITO
VCF.P7S	text/x-vcard	GESTITO
WMV	video/x-ms-wmv	DEPRECATO
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
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-	GESTITO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
	excel.sheet.binary.macroenabled.12	
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		
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/	

Formato versato ammesso	Mimetype	Idoneità alla conservazione
	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
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
XSLT	application/xslt+xml	IDONEO
XSLT.ASICE	application/xslt+xml	IDONEO
XSLT.ASICS	application/xslt+xml	IDONEO

Formato versato ammesso	Mimetype	Idoneità alla conservazione
XSLT.P7M	application/xslt+xml	IDONEO
XSLT.P7S	application/xslt+xml	IDONEO
ZIP	application/zip	IDONEO
ZIP.ASICE	application/zip	IDONEO
ZIP.ASICS	application/zip	IDONEO
ZIP.P7M	application/zip	IDONEO
ZIP.P7M.TSD	application/zip	IDONEO
ZIP.P7S	application/zip	IDONEO

Allegato 11 – Piano della sicurezza

Il presente Piano della Sicurezza (PdS) descrive l'implementazione del Sistema di Gestione della Sicurezza Informatica (SGSI) del Comune di Vigevano esclusivamente per quanto attiene le attività di conservazione documentale ex DPCM 3 dicembre 2013 e, quindi, inerenti quanto definito nell'ambito del Codice dell'Amministrazione Digitale (D.Lgs. 7 marzo 2005, n. 82 e successive modificazioni). Pertanto, ogni indicazione contenuta nel PdS è da intendersi riferita, ove altrimenti non indicato, esclusivamente alle predette attività di conservazione documentale.

Esso è sottoposto a verifica ed aggiornamento e deve considerare almeno i seguenti aspetti: analisi dei rischi, politiche di sicurezza ed interventi operativi.

Nel PdS sono state incluse le misure atte a garantire la corretta gestione e conservazione delle copie di sicurezza dell'archivio informatico.

NORMATIVA E STANDARD DI RIFERIMENTO

- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD) e in particolare art. 50 bis;
- Decreto del Presidente del Consiglio dei Ministri 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 Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale ex al Decreto Legislativo n. 82 del 2005;
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82;
- "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" emanate da AGID entrate in vigore il 10 settembre 2020 ed attuate il 7 giugno 2021

ORGANIZZAZIONE DEL SISTEMA DI GESTIONE DOCUMENTALE

Di seguito viene descritta l'organizzazione del Sistema di gestione documentale, sotto il profilo dei ruoli, delle responsabilità e della produzione-diffusione di policy e procedure.

Il Sistema Documentale è lo strumento che permette la gestione dei flussi documentali all'interno dell'Amministrazione.

L'accesso degli utenti al Sistema Documentale è regolato in funzione delle competenze che caratterizzano gli operatori, basate principalmente sul ruolo e sulla struttura organizzativa di appartenenza.

La visualizzazione delle varie parti del Sistema Documentale potrà essere diversa da utente a utente, in base al ruolo attribuitogli dal Servizio ICT in base alle autorizzazioni pervenute da parte dei Dirigenti/Responsabili di Settore/Servizio preposti.

Ruoli e Responsabilità

- Responsabile gestione documentale – predispone il manuale di gestione, gestisce il servizio di gestione documentale dell'Ente, predispone il Piano della sicurezza informatica in collaborazione con il Responsabile ICT.
- Responsabile Servizio ICT cura l'implementazione, la gestione e la sicurezza dell'Infrastruttura ICT
- Responsabile della sicurezza perimetrale dell'Ente – Nominato quale esperto in sicurezza dell'aggiudicatario del Servizio externalizzato di Assistenza sistemistica e sicurezza perimetrale dell'Ente.
- Servizio di Help desk – Servizio strutturato su due livelli: livello 1 – help desk externalizzato per la gestione delle Postazioni di lavoro, livello 2 – help desk effettuato da personale specializzato interno all'Ente per risoluzione di problematiche complesse.
- Soggetto privato che implementa e gestisce il software applicativo su cui poggia il sistema di Protocollo Informatico in uso. Il software fornito in modalità SaaS su cloud certificato AGID rispetta tutte le norme di sicurezza previste in materia.
- Polo Archivistico Regionale Emilia Romagna: soggetto privato che implementa e gestisce la conservazione digitale dei documenti informatici soggetti a protocollazione, nonché dei documenti conservati di cui al *Capitolo 8 - Archiviazione dei documenti paragrafo 8.2 Archiviazione dei documenti e dei fascicoli informatici del Manuale di gestione del Comune di Vigevano*. Le modalità di conservazione e accesso ai documenti, analogici o digitali, sono specificate con riferimento al Manuale di conservazione di PARER (Allegato n. 9 – PARER – ManualeConservazione_ver2021fin e suoi allegati)

Al Servizio ICT sono delegate tutte le funzionalità informatiche per definire i vari diritti UTENTE all'interno del sistema.

L'utente che può accedere ad una delle componenti del sistema deve essere dotato di un sistema di autenticazione complesso che richiede credenziali personali da inserire durante l'operazione di login. Ad ogni utente possono essere associati determinati diritti e permessi.

Architettura, sicurezza e gestione

Il sistema di Gestione documentale e Protocollo Informatico del Comune di Vigevano è costituito da un software applicativo erogato in modalità SaaS/Pass su datacenter certificato AGID conforme allo standard ISO 27001 e fruibile attraverso l'infrastruttura di rete LAN dell'Ente.

La soluzione software, erogata in modalità SaaS, attraverso opportuna VPN dedicata a maggior garanzia della sicurezza di trasmissione dati, prevede il collegamento con il sistema di conservazione a norma (ParER) e tramite opportuni web service il collegamento con altri applicativi verticali in uso all'Ente.

Il Comune di Vigevano assicura la connessione alla LAN dell'Ente attraverso l'autenticazione a due fattori in modo da consentire a coloro che svolgono l'attività lavorativa da remoto (telelavoro, smart working) di accedere al sistema di gestione documentale in sicurezza.

Disaster recovery e backup effettuati dal CSP (Cloud Service Provider) assicurando la disponibilità dei servizi al 99,95% su base annua e vengono effettuati su data center situati sul territorio nazionale dotati di tutti i sistemi di sicurezza fisica necessari.

La manutenzione ordinaria e straordinaria viene effettuata in accordo con il Responsabile ICT dell'Ente.

La società che eroga il servizio di gestione documentale e protocollo del Comune di Vigevano è stata nominata Responsabile esterno al trattamento dei dati secondo quanto previsto dalla normativa vigente in materia di Privacy a seguito del benessere del DPO dell'Ente.