Politica sulla sicurezza delle informazioni del servizio di Conservazione Digitale

Codice documento	PoliticaSicurezza
Versione	1.0

	Data	*Nominativo*	*Funzione*
Redazione	17/05/2021	Giovanni Galazzini	Consulente esterno
Verifica	18/05/2021	Marco Calzolari	Responsabile della Sicurezza del ParER
Approvazione	18/05/2021	Marco Calzolari	Responsabile del Servizio

Indice

Storia delle modifiche del documento

Versione	Variazioni	Data
1.0	Prima emissione	18/05/2021

Classificazione del documento

Livello di Riservatezza	**TLP: WHITE**
Classificazione	PaRERDoc *Policy … / Policy*

Introduzione

Data la natura delle proprie attività, ParER pone particolare attenzione alla sicurezza delle informazioni come fattore irrinunciabile per la protezione del patrimonio informativo proprio e degli enti produttori.

Per assicurare che i requisiti di sicurezza siano correttamente presidiati e garantiti, ParER, recependo la *Politica per la sicurezza delle informazioni della Regione Emilia-Romagna* e i *Disciplinari tecnici* di Regione, ha identificato, applicato e descritto la propria politica sulla sicurezza delle informazioni, contenuta nel presente documento.

Di conseguenza, la Politica di ParER:

- recepisce le regole definite dalla Regione Emilia-Romagna, descritte nelle Politiche e nei Disciplinati tecnici, e le declina considerando le specificità del Servizio di Conservazione;
- costituisce il quadro generale di riferimento del Polo archivistico dell'Emilia-Romagna (ParER) rispetto alle politiche di sicurezza delle informazioni;
- assicura, attraverso la sua implementazione, una corretta gestione della sicurezza del sistema di conservazione dei documenti digitali.

Standard e documenti di riferimento

L’elenco aggiornato degli standard e dei documenti di riferimento è contenuto nell’Allegato 1 del Manuale di conservazione “Normativa e Standard di riferimento”.

Sez.1. Profilo di minaccia

Un aspetto particolarmente critico per la qualità del servizio, data la sua natura, è la sicurezza dei documenti. Il servizio di Conservazione Digitale comporta l'archiviazione di informazioni di varia natura e importanza, alcune di particolare criticità per il carattere di riservatezza o unicità che le caratterizza (ad esempio documenti che provengono dalla Sanità).

Tra i documenti, infatti, ve ne sono di contenenti dati personali, ricadenti nella sfera della normativa sulla protezione dei dati (i.e. normativa privacy), elemento che impone l'osservanza di particolari accorgimenti, oltre che la valutazione di un quadro di minacce potenziali al servizio più ampio.

In generale, le minacce a cui deve far fronte ParER, sono riassumibili nelle seguenti (*elenco non esaustivo*):

- accesso e/o diffusione non autorizzata di documenti, anche contenenti informazioni personali/sensibili (requisito minacciato: riservatezza);
- archiviazione di un dato/documento non corretto (requisito minacciato: integrità);
- perdita di documenti (requisito minacciato: integrità);
- alterazione delle informazioni contenute nei documenti (requisito minacciato: autenticità);
- indisponibilità del servizio di conservazione dei documenti (requisito minacciato: disponibilità).

Sez.2. Politiche

Le politiche per la sicurezza delle informazioni si applicano a tutto il ciclo di vita del servizio di conservazione dalla fase di attivazione, attraverso la fase di esercizio (immissione, gestione e messa a disposizione dei documenti), fino alla fase di terminazione del servizio, nonché alle connesse attività di natura tecnologica di analisi, progettazione, sviluppo e manutenzione delle infrastrutture, dei sistemi e delle applicazioni.

Le politiche sono adottate da ParER per la sicurezza delle informazioni del sistema di conservazione dei documenti digitali in funzione della loro criticità, valore e sensibilità rispetto al servizio complessivo di conservazione.

Esse interessano, in generale, la totalità del personale ParER, con l'intento di assicurare la protezione delle informazioni in ogni passaggio dei trattamenti operati e per l'intero ciclo di vita delle informazioni stesse.

2.1 Uso accettabile degli asset

Obiettivo:

L'obiettivo della seguente politica è:

- indirizzare i comportamenti degli utenti relativamente agli asset utilizzati, allo scopo di prevenire l'accesso non autorizzato ai documenti;
- definire le politiche per la dismissione sicura degli asset.

Riferimenti esterni:

Relativamente all'uso accettabile degli asset, ParER fa riferimento alle norme adottate in materia dalla Regione Emilia-Romagna e pubblicate sulla Intranet Regionale:

- *"Disciplinare tecnico per utenti dei sistemi informativi della regione Emilia-Romagna" (Determina n. 8901 del 6 giugno 2017)*, con particolare attenzione ai Capitoli 3 e 7;
- *Linee Guida per la governance del sistema informatico regionale (Delibera n. 281 del 29/02/2016)* e successivi aggiornamenti, in particolare al Capitolo 14.

Regole/requisiti:

Tutto il personale deve:

- **essere a conoscenza del proprio ruolo e delle responsabilità nel contribuire ad un corretto e sicuro utilizzo delle risorse informative**. In particolare, ognuno è responsabile della protezione e della conservazione dei beni regionali, materiali e immateriali, avuti in affidamento per l'espletamento dei propri compiti, nonché del loro utilizzo in modo proprio e conforme ai fini regionali;
- **proteggere i computer e le altre strumentazioni informatiche, in caso di assenza, anche temporanea, dalla postazione di lavoro**, tramite la sospensione o il blocco della sessione di lavoro;
- **utilizzare sulle postazioni di lavoro esclusivamente il software autorizzato e fornito dall'Ente**;

- segnalare sempre, in ogni caso e preventivamente al proprio referente informatico o all'assistenza utenti dei Servizi regionali competenti in materia di informatica, la necessità di installare eventuale software aggiuntivo rispetto all'installazione standard, anche se gratuito e necessario per lo svolgimento dell'attività lavorativa;
- **utilizzare stampanti in cui è attiva la funzionalità di stampa riservata** e il rilascio della stampa è subordinata alla presenza dell'utente presso la stampante; ciò allo scopo di mantenere la riservatezza dei documenti stampati;
- **evitare di archiviare nel proprio computer i documenti informatici conservati nel Sistema di Conservazione**, se non per il tempo strettamente necessario per lo svolgimento di specifiche attività di testing;
- evitare di lasciare informazioni ritenute strategiche e/o sensibili (su supporto cartaceo e/o elettronico) dove possono essere lette, copiate e sottratte da personale non autorizzato e procedere allo smaltimento sicuro (es. distruzione) dei supporti cartacei contenenti tali informazioni quando essi non siano più necessari;
- astenersi dall'utilizzo **di dispositivi mobili e supporti rimovibili** (CD, hard disk, ecc.) relativamente alle **attività di versamento e distribuzione di documenti in conservazione.**

Responsabilità:

Soggetti coinvolti: / **Attività:**	**Resp.le del Servizio**	**Resp.le Servizi di Conservazione**	**Resp.le della sicurezza del sistema di conservazione**	**Resp.le Sistemi di Conservazione**	**Analista/Sviluppatore - Area Sistemi di Conservazione**	**Resp.le Funzione Archivistica di Conservazione**	**Archivista - Area Servizi di Conservazione**	**Resp.le dell'Infrast. Tecnologica**	**Resp.le Amministrativo**
Definizione/revisione della regola	A,R		C					C	
Attuazione della regola	A	R	C	R	R	R	R	R	R
Monitoraggio/verifica di attuazione della regola			A,R						

2.2 Risorse umane

Obiettivo:

L'obiettivo della seguente politica è garantire che il personale di ParER (dipendenti e collaboratori) abbia piena consapevolezza delle problematiche relative alla sicurezza delle informazioni. Perciò ParER applica nei confronti di tutte le persone coinvolte nel processo di conservazione (personale interno, fornitori e altre terze parti) gli indirizzi generali sulla sicurezza, affinché:

- comprendano l'importanza degli indirizzi generali, delle politiche e delle procedure adottate da ParER per assicurare la sicurezza delle informazioni;
- comprendano il loro ruolo all'interno del sistema di conservazione, con particolare riferimento alle problematiche della sicurezza;
- siano informati sui comportamenti da tenere per assicurare gli opportuni livelli di sicurezza.

Riferimenti esterni:

ParER fa riferimento alle norme adottate in materia dalla Regione Emilia-Romagna e pubblicate sulla Intranet Regionale; tali norme coprono l'intero percorso che un dipendente regionale compie all'interno di ParER, dal momento dell'assunzione fino alla risoluzione del rapporto di lavoro:

- *"Disciplinare tecnico per utenti dei sistemi informativi della regione Emilia-Romagna" (Determina n. 8901 del 6 giugno 2017);*
- *Linee Guida per la governance del sistema informatico regionale (Delibera n. 281 del 29/02/2016)* e successivi aggiornamenti;
- *LEGGE REGIONALE 26 novembre 2001, n. 43 TESTO UNICO IN MATERIA DI ORGANIZZAZIONE E DI RAPPORTI DI LAVORO NELLA REGIONE EMILIA-ROMAGNA* e successivi aggiornamenti.

Regole/requisiti:

- **nella fase di selezione e per tutta la durata del rapporto di lavoro:**
  - devono essere valutati i livelli di affidabilità, competenza e conoscenza degli obiettivi e delle problematiche di sicurezza dell'organizzazione in funzione delle attività che dovranno essere svolte;
  - devono essere chiaramente comunicati (e sottoscritti dal soggetto) gli eventuali obblighi di riservatezza per i quali viene richiesto l'impegno; va altresì specificato se tali obblighi permangono anche a valle della cessazione del rapporto di lavoro;
  - il personale deve ricevere un'adeguata e **continuativa formazione** inerente le tematiche di sicurezza e privacy dei dati, con particolare riferimento a:
    - politiche e procedure in materia di sicurezza delle informazioni;
    - principali rischi che si insistono su dati e informazioni;
    - misure disponibili per prevenire eventi dannosi;

- obblighi legislativi, regolamentari e contrattuali in materia di informazione e trattamento e protezione dei dati (con particolare riferimento ai dati dei clienti);

- le **modalità di chiusura del rapporto di lavoro con ParER** devono assicurare la corretta rimozione dei dritti di accesso alle risorse informative nonché la restituzione di tutti i beni forniti in uso al personale.

Responsabilità:

Soggetti coinvolti: / Attività:	Resp.le del Servizio	Resp.le Servizi di Conservazione	Resp.le della sicurezza del sistema di conservazione	Resp.le Sistemi di Conservazione	Analista/ Sviluppatore - Area Sistemi di Conservazione	Resp.le Funzione Archivistica di Conservazione	Archivista - Area Servizi di Conservazione	Resp.le dell'Infrast. Tecnologica	Resp.le Amministrativo
Definizione/revisione della regola	A,R	C	C	C				C	
Attuazione della regola	A,R	R	C	R				R	
Monitoraggio/verifica di attuazione della regola	A,R								

2.3 Gestione terze parti

Obiettivo:

L'obiettivo della presente politica è assicurare la conformità ai requisiti legali e ai principi legati alla sicurezza delle informazioni nei contratti con le terze parti, in accordo con le caratteristiche specifiche della relazione che ParER deve instaurare con le terze parti stesse.

Riferimenti esterni:

ParER fa riferimento alle norme adottate in materia dalla Regione Emilia-Romagna e pubblicate sulla Intranet Regionale:

- *Linee Guida per la governance del sistema informatico regionale (Delibera n. 281 del 29/02/2016)* e successivi aggiornamenti, in particolare all'Allegato 5 e 8.

Regole/requisiti:

Gli accordi con le terze parti e con il gestore dell'infrastruttura che accedono alle informazioni e/o agli strumenti che le elaborano:

- **devono essere basati su contratti formali** contenenti opportuni requisiti di sicurezza. I requisiti di sicurezza devono risultare adeguati rispetto ai rischi, accidentali e/o intenzionali, di distruzione, perdita, divulgazione, alterazione e accesso non autorizzato delle risorse informative dell'organizzazione;
- **devono garantire il rispetto dei requisiti di legge in materia di protezione dei dati personali e copyright** delle risorse informative accedute e utilizzate.
- **devono prevedere accordi per garantire la riservatezza e la non-divulgazione delle informazioni critiche** dell'organizzazione. Tali accordi devono necessariamente contemplare tutti i requisiti dell'organizzazione definiti per assicurare la protezione delle risorse informative;
- **devono includere**, ove possibile, **la possibilità di effettuare attività di audit di II parte sui fornitori** per verificare il rispetto dei requisiti di sicurezza concordati.

Responsabilità:

Soggetti coinvolti: / Attività:	Resp.le del Servizio	Resp.le Servizi di Conservazione	Resp.le della sicurezza del sistema di conservazione	Resp.le Sistemi di Conservazione	Analista/ Sviluppatore - Area Sistemi di Conservazione	Resp.le Funzione Archivistica di Conservazione	Archivista - Area Servizi di Conservazione	Resp.le dell'Infrast. Tecnologica	Resp.le Amministrativo
Definizione/revisione della regola	A,R	C	C	C					
Attuazione della regola	A,R	R	C	R					
Monitoraggio/verifica di attuazione della regola	A	R	R	R					

2.4 Gestione degli asset

Obiettivo:

L'obiettivo della presente politica è assicurare che tutti gli asset associati al servizio di conservazione siano stati opportunamente identificati e inventariati e che sia stato individuato un responsabile al fine di gestire le minacce associate alla sicurezza delle informazioni.

Riferimenti esterni:

ParER fa riferimento alle norme adottate in materia dalla Regione Emilia-Romagna e pubblicate sulla Intranet Regionale:

- **"***Disciplinare tecnico per gli amministratori di sistema della Giunta e dell'Assemblea Legislativa*" (Determinazione n. 83 del 07/01/2021), in particolare al Capitolo 8.

Regole/requisiti:

- ai fini della selezione e attuazione di adeguati meccanismi di controllo, **le informazioni gestite devono essere identificate e classificate:**
  - **in ordine al grado di sensibilità e criticità**;
  - al fine di distinguere precisamente le informazioni di proprietà dei fruitori del servizio (clienti), da quelle da esse derivate e/o comunque ricadenti nella sfera di "titolarità" / appartenenza di ParER;
- tutti i **componenti tecnologici e organizzativi** necessari alla gestione del servizio di conservazione delle informazioni digitali **devono essere identificati e classificati in ordine alla classificazione delle informazioni gestite**;
- ogni qualvolta si **dismette un dispositivo elettronico o informatico** che contiene dati personali/sensibili, è necessario adottare idonei accorgimenti e misure, anche attraverso soggetti terzi, tecnicamente qualificati, che attestino l'esecuzione delle operazioni effettuate o che si impegnino ad effettuarle;
- tutti i cambiamenti, che hanno un impatto sugli utenti del Servizio di conservazione, devono essere comunicati tramite opportuni canali.

In considerazione delle caratteristiche e della missione del servizio, e in relazione al fatto che non è ParER a stabilire la criticità relativa delle informazioni conservate (bensì i titolari delle informazioni stesse), **si stabilisce che tutte le informazioni affidate a ParER dai clienti abbiano tutte lo stesso livello di criticità e, pertanto, siano soggette allo stesso grado di protezione.**

Responsabilità:

Soggetti coinvolti: / Attività:	Resp.le del Servizio	Resp.le Servizi di Conservazione	Resp.le della sicurezza del sistema di conservazione	Resp.le Sistemi di Conservazione	Analista/ Sviluppatore - Area Sistemi di Conservazione	Resp.le Funzione Archivistica di Conservazione	Archivista - Area Servizi di Conservazione	Resp.le dell'Infrast. Tecnologica	Resp.le Amministrativo
Definizione/revisione della regola	A,R		C					C	
Attuazione della regola	A	R	C	R	R	R	R	R	R
Monitoraggio /verifica di attuazione della regola			A,R						

2.5 Analisi dei rischi

Obiettivo:

L'obiettivo della presente politica è assicurare che i rischi associati al servizio di conservazione siano identificati, valutati e trattati.

Riferimenti esterni: NA

Regole/requisiti:

- **il sistema di controllo relativo al servizio di conservazione deve essere risk based**: l'Analisi dei Rischio è l'elemento principale da cui discendono tutte le attività di controllo, le Politiche in merito alla sicurezza e le procedure operative legate alla sicurezza delle informazioni.
- i necessari **controlli** per la mitigazione di potenziali rischi devono essere **definiti a seguito di un'attività di risk assessment;**
- **l'attività di risk assessment va ripetuta con cadenza periodica e regolare**, a garanzia del permanere dell'efficacia delle misure di mitigazione identificate e attuate.

Responsabilità:

Soggetti coinvolti: / Attività:	Resp.le del Servizio	Resp.le Servizi di Conservazione	Resp.le della sicurezza del sistema di conservazione	Resp.le Sistemi di Conservazione	Analista/ Sviluppatore - Area Sistemi di Conservazione	Resp.le Funzione Archivistica di Conservazione	Archivista - Area Servizi di Conservazione	Resp.le dell'Infrast. Tecnologica	Resp.le Amministrativo
Definizione dei modelli di analisi dei rischi		C	A,R	C		C		C	C
Esecuzione delle attività di risk assessment	A	R	R	R		R		R	R
Accettazione dei rischi	A,R	C	C	C		C		C	C
Monitoraggio /verifica di attuazione della regola			A,R						

2.6 Separazione dei ruoli e degli ambienti

Obiettivo:

L'obiettivo della presente politica è garantire i necessari livelli di sicurezza nell'esercizio del servizio di conservazione, attraverso l'attuazione dei principi di separazione dei ruoli.

Riferimenti esterni: NA

Regole/requisiti:

- **i principi di separazione dei ruoli e privilegio minimo** devono prevedere, almeno, la seguente separazione dei ruoli per incompatibilità:
  - Programmatori/Archivisti;
  - Programmatori/DBA;
  - Programmatori/Amministratori di sistema;
  - Programmatori/Collaudatori;
  - Programmatori/Responsabile della sicurezza;
  - Archivisti/DBA;
  - Archivisti/Amministratori di sistema;
  - Amministratori di sistema/Responsabile della sicurezza;
  - Chi svolge un'operazione / Chi verifica l'operazione.
- devono essere attuate opportune misure di sicurezza a garanzia di un'adeguata **separazione degli ambienti di sviluppo, test e produzione**.
- **i sistemi**, che costituiscono l'infrastruttura ICT utilizzata da ParER per erogare il servizio di conservazione, **devono essere opportunamente protetti e segregati (tra loro e dagli ambienti/sistemi/funzionalità destinati alla gestione del servizio)**, in modo da minimizzare la possibilità di accessi non autorizzati.

Responsabilità:

Soggetti coinvolti: / Attività:	Resp.le del Servizio	Resp.le Servizi di Conservazione	Resp.le della sicurezza del sistema di conservazione	Resp.le Sistemi di Conservazione	Analista/Sviluppatore - Area Sistemi di Conservazione	Resp.le Funzione Archivistica di Conservazione	Archivista - Area Servizi di Conservazione	Resp.le dell'Infrast. Tecnologica	Resp.le Amministrativo
Definizione/revisione della regola	A,R		C						
Attuazione della regola	A	R	C	R	R	R	R	R	R
Monitoraggio/verifica di attuazione della regola			A,R						

2.7 Controllo degli accessi

Obiettivo:

L'obiettivo della seguente politica è garantire l'accesso sicuro alle informazioni conservate, in modo da prevenire trattamenti non autorizzati delle stesse o la loro visione da parte di utenti (interni o esterni) che non possiedono i necessari diritti.

Riferimenti esterni:

Per ciò che attiene agli **accessi logici ai sistemi informatici gestiti dalla Regione Emilia-Romagna (SICTR) e all'accesso a tutti gli ulteriori apparati informatici utilizzati da ParER per l'erogazione del servizio di conservazione (compreso il Sito di DR)**, si fa riferimento alle norme adottate in materia dalla Regione Emilia-Romagna e pubblicate sulla Intranet Regionale:

- Determinazione n° 4137 del 28/03/2014 "*Disciplinare tecnico in materia di sicurezza delle applicazioni informatiche nella Giunta e nell'Assemblea legislativa della Regione Emilia-Romagna*";
- Determina n. 8901 del 06/06/2017 "*Disciplinare tecnico per utenti dei servizi informativi della Regione Emilia-Romagna: si applica a tutti, dipendenti, fornitori, politici, consulenti, stagisti e tutti coloro che si collegano alla rete regionale e utilizzano i suoi servizi (Giunta, AL, Agenzie regionali)*";
- Determinazione n° 19529 del 23/11/2018 "*Disciplinare tecnico per le verifiche di sicurezza sul sistema informativo regionale, da applicare nella Giunta e nell'Assemblea Legislativa della Regione Emilia-Romagna*";
- **"***Linee Guida per la governance del sistema informatico regionale*" (*Delibera n. 281 del 29/02/2016*) e successivi aggiornamenti;
- **"***Disciplinare tecnico per gli amministratori di sistema della Giunta e dell'Assemblea Legislativa*" (Determinazione n. n. 83 del 07/01/2021), in particolare al Capitolo 5;
- Determina n. 14128 del 30/07/2019 *"Disciplinare per l'esercizio diritti dell'interessato sui propri dati personali (Giunta e Assemblea)";*
- Determina n. 12807 del 03/08/2018 *"Disciplinare tecnico per la gestione degli incidenti di sicurezza e data breach".*

Regole/requisiti:

Il ciclo di vita delle utenze deve essere regolamentato da un'opportuna procedura, dal momento dell'assegnazione, fino alla sua dismissione;

Personale interno e consulenti – l'accesso alle informazioni da parte di ogni singolo utente (personale ParER, nonché dipendenti di imprese esterne e/o consulenti cui l'accesso è consentito per l'esecuzione degli specifici obblighi contrattuali) deve essere subordinato ad una **procedura di autorizzazione da parte di ParER** e **limitato alle sole informazioni di cui necessita** in funzione del ruolo e delle mansioni assegnate (principio del minimo privilegio);

- *Personale esterno (clienti)* - l'accesso alle informazioni da parte degli Utenti degli Enti Produttori deve avvenire secondo precise regole (di accesso e visibilità delle informazioni) condivise da ParER con gli *Enti Produttori*
- **le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo e agli incarichi ricoperti, nel rispetto dei principi di separazione**

dei ruoli e devono essere **sottoposte a revisione periodica**, con cadenza almeno annuale. Deve essere in ogni caso prevista la tempestiva modifica/disattivazione dei diritti d'accesso in caso di revisione/sospensione/revoca dei profili autorizzativi assegnati;

- è necessario definire un **processo di gestione delle credenziali di autorizzazione e dei relativi profili di accesso**. Specifiche procedure devono essere definite per l'assegnazione, la gestione e il controllo dei profili associati ad elevati privilegi (es. amministratori di sistema, "*superutenti*" in genere);
- devono essere definiti standard, procedure e istruzioni per la **gestione delle password** in conformità alle normative vigenti, con particolare riferimento a quelle in materia di protezione dei dati personali;
- **devono essere monitorati e regolarmente verificati**, nel rispetto dei limiti imposti dalla vigente normativa sulla protezione dei dati personali, **gli accessi da parte degli utenti alla rete, ai servizi di rete, al sistema operativo alle applicazioni e alle informazioni dell'organizzazione;**
- deve essere adottata particolare attenzione al **tracciamento degli accessi legati alle utenze amministrative**, al fine di garantire l'inalterabilità dei log e la loro conservazione secondo le tempistiche previste e per l'espletamento degli obblighi di verifica imposti dalla vigente normativa sulla protezione dei dati personali;
- l'accesso alle informazioni in formato digitale da parte di utenti e sistemi autorizzati deve essere subordinato al superamento di una **procedura di identificazione e autenticazione**. La comunicazione e la trasmissione di informazioni all'interno, così come verso l'esterno, deve fondarsi sullo stesso principio;
-

Responsabilità:

Soggetti coinvolti: / Attività:	Resp.le del Servizio	Resp.le Servizi di Conservazione	Resp.le della sicurezza del sistema di conservazione	Resp.le Sistemi di Conservazione	Analista/ Sviluppatore - Area Sistemi di Conservazione	Resp.le Funzione Archivistica di Conservazione	Archivista - Area Servizi di Conservazione	Resp.le dell'Infrast. Tecnologica	Resp.le Amministrativo
Definizione/revisione della regola	A,R		C						
Attuazione della regola	A	R	C	R	R	R	R	R	R
Monitoraggio/verifica di attuazione della regola			A,R						

2.8 Sicurezza dello sviluppo applicativo

Obiettivo:

L'obiettivo della seguente politica è quello di assicurare che gli aspetti di sicurezza siano inclusi nelle fasi di progettazione e sviluppo del software di conservazione, anche in relazione all'architettura di erogazione del servizio.

ParER considera lo sviluppo del software di conservazione elemento fondamentale per garantire l'erogazione del proprio Servizio; per questo ha deciso di mantenere lo sviluppo interno.

Riferimenti esterni:

ParER fa riferimento:

- alle linee guida regionali per lo sviluppo sicuro, presenti nel *Disciplinare Tecnico in materia di sicurezza delle applicazioni informatiche nella Giunta e nell'Assemblea Legislativa della Regione Emilia-Romagna (Determinazione n. 4137 del 28/03/2014)*;
- alle linee guida per lo sviluppo sicuro specifiche per il servizio di conservazione, contenute nel documento *Sicurezza sviluppo applicativo;*
- alle *Linee guida per la governance del sistema informatico regionale (Delibera n. 281 del 29/02/2016)*, per quanto riguarda le verifiche relative ai requisiti di sicurezza dei sistemi e delle informazioni.

Regole/requisiti:

- **nelle fasi di progettazione e sviluppo del software di conservazione devono essere opportunamente considerati gli aspetti di sicurezza**. In particolare devono essere indirizzate le seguenti tematiche:
    - inclusione dei requisiti di sicurezza nelle specifiche funzionali dei servizi e dei sistemi, anche in relazione alla modalità di erogazione dei servizi prevista (es. servizi cloud-based);
    - adozione di best practice nel rispetto dei principi fondamentali di sviluppo sicuro quali:
        - Riduzione della superficie d'attacco;
        - Security by default;
        - Privilegio minimo (Least Privilege);
        - Defence In Depth;
        - Separazione dei ruoli (SoD);
        - Semplicità dei meccanismi di sicurezza.
    - separazione degli ambienti di sviluppo e di test, con impiego di procedure formali di controllo e accettazione nel passaggio fra ambienti
    - gestione controllata della documentazione.
- **ogni sviluppo a sistema deve essere adeguatamente autorizzato, testato e approvato prima del suo passaggio in Produzione**. Durante le fasi di test è necessario verificare che siano rispettati anche i requisiti di sicurezza delle informazioni e dei principi suddetti;

- non si effettuano attività di cancellazione dei **dati personali in ambiente di test** in quanto le misure di sicurezza applicate al test sono analoghe all'ambiente di produzione;
- **è necessario archiviare giornalmente nei sistemi preposti tutto il codice sviluppato relativo Sistema di Conservazione**.

Responsabilità:

Soggetti coinvolti: / Attività:	Resp.le del Servizio	Resp.le Servizi di Conservazione	Resp.le della sicurezza del sistema di conservazione	Resp.le Sistemi di Conservazione	Analista/ Sviluppatore - Area Sistemi di Conservazione	Resp.le Funzione Archivistica di Conservazione	Archivista - Area Servizi di Conservazione	Resp.le dell'Infrast. Tecnologica	Resp.le Amministrativo
Definizione/revisione della regola	A,R		C	C				I	
Attuazione della regola			C	A	R			R	
Monitoraggio/verifica di attuazione della regola			A,R						

2.9 Crittografia

Obiettivo:

L'obiettivo della seguente politica è quello di assicurare adeguato livello di protezione ai dati e alle informazioni gestite.

Riferimenti esterni: NA

Regole/requisiti:

- **Le password gestite devono essere adeguatamente protette** attraverso meccanismi di crittografia; **particolari accorgimenti debbono essere adottati a protezione delle password degli amministratori di sistema;**
- **i flussi informativi in entrata e in uscita relativi ai servizi di conservazione** devono essere **protetti mediante idonei protocolli di crittografia** (es. HTTPS e FTPS).

Il processo di conservazione non prevede l'utilizzo della crittografia degli oggetti conservati, in quanto:

- deve assicurare la conservazione a lungo termine del documento digitale e di conseguenza la piena disponibilità nei confronti non solo dell'ente produttore, ma di tutta la comunità di riferimento (previa verifica dell'autorizzazione all'accesso ai documenti);
- non deve in alcun modo alterare il documento inviato in conservazione utilizzando tecniche crittografiche proprie.

Responsabilità:

Soggetti coinvolti: / Attività:	Resp.le del Servizio	Resp.le Servizi di Conservazione	Resp.le della sicurezza del sistema di conservazione	Resp.le Sistemi di Conservazione	Analista/ Sviluppatore - Area Sistemi di Conservazione	Resp.le Funzione Archivistica di Conservazione	Archivista - Area Servizi di Conservazione	Resp.le dell'Infrast. Tecnologica	Resp.le Amministrativo
Definizione/revisione della regola	A,R		C			C		C	
Attuazione della regola	A	R	C	R	R	R	R	R	R
Monitoraggio/verifica di attuazione della regola			A,R						

2.10 Sicurezza fisica

Obiettivo:

L'obiettivo della seguente politica è quello di prevenire l'accesso non autorizzato alle sedi e ai locali dell'organizzazione e garantire adeguati livelli di sicurezza alle aree e agli asset mediante i quali vengono gestite le informazioni.

Riferimenti esterni:

ParER fa riferimento al *Disciplinare Tecnico relativo al controllo degli accessi ai locali della Giunta della Regione Emilia-Romagna (Determinazione n. 1894/2018)*.

Regole/requisiti:

- devono essere garantiti:
  - delimitazione e opportuna protezione del **perimetro fisico relativo ai sistemi di conservazione**;
  - isolamento/separazione delle **aree di carico e scarico**;
  - adeguati **sistemi di controllo e tracciamento degli accessi fisici**;
  - definizione di una **adeguata collocazione delle apparecchiature per l'elaborazione delle informazioni**;
  - predisposizione di idonei **impianti di sicurezza fisica e ambientale**;
  - predisposizione di un adeguato **piano di manutenzione** degli impianti di sicurezza fisica e ambientale.

Responsabilità:

Soggetti coinvolti: / **Attività:**	**Resp.le del Servizio**	**Resp.le Servizi di Conservazione**	**Resp.le della sicurezza del sistema di conservazione**	**Resp.le Tecnologie e sviluppo sistema di conservazione**	**Analista/ Sviluppatore - Area Sistemi di Conservazione**	**Resp.le Funzione Archivistica di Conservazione**	**Archivista - Area Servizi di Conservazione**	**Resp.le dell'Infrast. Tecnologica**	**Resp.le Amministrativo**
Definizione/revisione della regola	A,R		C					C	
Attuazione della regola								A	
Monitoraggio/verifica di attuazione della regola			A,R						

2.11 Capacity management

Obiettivo:

L'obiettivo della seguente politica è quello di garantire una gestione efficace che tenga conto dei necessari livelli di disponibilità e delle performance.

Riferimenti esterni: NA

Regole/requisiti:

Devono essere attuati i necessari controlli a garanzia del monitoraggio del consumo delle risorse e delle previsioni di saturazione (es. elaborazione e analisi di statistiche periodiche)**,** al fine di intervenire con tempismo e assicurare la necessaria disponibilità degli ambienti, in coerenza con le esigenze (anche prestazionali) del servizio condivise con gli *Enti Produttori*.

Responsabilità:

Soggetti coinvolti: / Attività:	Resp.le del Servizio	Resp.le Servizi di Conservazione	Resp.le della sicurezza del sistema di conservazione	Resp.le Tecnologie e sviluppo sistema di conservazione	Analista/ Sviluppatore - Area Sistemi di Conservazione	Resp.le Funzione Archivistica di Conservazione	Archivista - Area Servizi di Conservazione	Resp.le dell'Infrast. Tecnologica	Resp.le Amministrativo
Definizione/revisione della regola	A,R		C					C	
Attuazione della regola								A	
Monitoraggio/verifica di attuazione della regola			A,R						

2.12 Gestione malware

Obiettivo:

L'obiettivo della seguente politica è quello di garantire un adeguato livello di sicurezza della piattaforma tecnologica a supporto del servizio (lato client e lato server), considerando opportunamente tali aspetti nelle tematiche relative alla gestione del malware.

Riferimenti esterni:

Il personale ParER segue le norme adottate in materia dalla Regione Emilia-Romagna e pubblicate sulla Intranet Regionale:

- *"Linee Guida per la governance del sistema informatico regionale" (Delibera n. 281 del 29/02/2016) e successivi aggiornamenti*;
- *"Disciplinare tecnico per utenti dei sistemi informativi della regione Emilia-Romagna" (Determina n. 8901 del 6 giugno 2017)*.

Regole/requisiti:

- devono essere **definite opportune politiche di protezione delle postazioni di lavoro e dei server dalla contaminazione di malware**, che prevedano:
  - identificazione delle postazioni e dei sistemi operativi target, in base alle esigenze operative e alla diffusione degli attacchi;
  - selezione di opportune tecnologie anti-malware;
  - definizione di modalità di installazione delle tecnologie anti-malware;
  - definizione delle modalità di aggiornamento e verifica della corretta; configurazione;
  - definizione di meccanismi di notifica early-warning.

Responsabilità:

Soggetti coinvolti: / Attività:	Resp.le del Servizio	Resp.le Servizi di Conservazione	Resp.le della sicurezza del sistema di conservazione	Resp.le Tecnologie e sviluppo sistema di conservazione	Analista/ Sviluppatore - Area Sistemi di Conservazione	Resp.le Funzione Archivistica di Conservazione	Archivista - Area Servizi di Conservazione	Resp.le dell'Infrast. Tecnologica	Resp.le Amministrativo
Definizione/revisione della regola	A,R		C						
Attuazione della regola	A	R	C	R	R	R	R	R	R
Monitoraggio/verifica di attuazione della regola			A,R						

2.13 Backup

Obiettivo:

L'obiettivo della seguente politica è quello di considerare opportunamente, nella fase di realizzazione e esercizio, gli aspetti di sicurezza relativamente all'adozione di procedure di backup e ripristino dei dati.

Riferimenti esterni:

ParER fa riferimento alle norme adottate in materia dalla Regione Emilia-Romagna e pubblicate sulla Intranet Regionale:

- *"Linee Guida per la governance del sistema informatico regionale" (Delibera n. 281 del 29/02/2016) e successivi aggiornamenti*, in particolare al Paragrafo 6.5.

Regole/requisiti:

- **devono essere garantiti adeguate misure e strumenti di backup in funzione dell'importanza dei sistemi e dei dati** in essi contenuti in modo da assicurare che i dati, le configurazioni e i software possano essere ripristinati successivamente ad un malfunzionamento o un crash di sistema;
- le procedure di backup/rispristino dei dati devono tener conto delle peculiarità del servizio di conservazione **(i dati in conservazione non devono essere più modificati),** pertanto è da preferire la modalità incrementale di backup. Per gli altri dati, invece, è possibile fare riferimento alle politiche regionali;
- **i supporti di backup devono essere conservati in una location differente rispetto a quella in cui sono conservati i dati originari**, ad una sufficiente distanza dalla location originaria e deve essere garantito un adeguato livello di protezione fisica.
- il processo di back up e restore dei dati deve essere periodicamente testato, e gli esisti delle verifiche opportunamente documentati;
- l'eventuale affidamento della conservazione di copie di backup dei dati a terze parti va regolato attraverso opportuni accordi contrattuali, nei quali siano indicate le misure di protezione (cfr. Cap. 2.3) e i criteri di trasferimento delle informazioni e/o tracciamento dei relativi supporti.

Per il dettaglio delle politiche di backup del Sistema di Conservazione adottate da ParER, si rimanda alla Sez.6 del presente documento.

Responsabilità:

Soggetti coinvolti: / Attività:	Resp.le del Servizio	Resp.le Servizi di Conservazione	Resp.le della sicurezza del sistema di conservazione	Resp.le Tecnologie e sviluppo sistema di conservazione	Analista/ Sviluppatore - Area Sistemi di Conservazione	Resp.le Funzione Archivistica di Conservazione	Archivista - Area Servizi di Conservazione	Resp.le dell'Infrast. Tecnologica	Resp.le Amministrativo
Definizione/revisione della regola	A,R		C					C	
Attuazione della regola								A	

Monitoraggio/verifica di attuazione della regola			A,R						

2.14 Monitoraggio e Gestione dei Log

Obiettivo:

L'obiettivo della seguente politica è quello di garantire i livelli di sicurezza necessari nella gestione e monitoraggio degli eventi e delle attività relative alla Sicurezza Informatica sul sistema di conservazione.

Riferimenti esterni:

ParER fa riferimento alle norme adottate in materia dalla Regione Emilia-Romagna e pubblicate sulla Intranet Regionale:

- *Disciplinare tecnico per gli amministratori di sistema della Giunta e dell'Assemblea Legislativa" (Determinazione n. 83 del 07/01/2021),* in particolare al Capitolo 6;
- *"Disciplinare tecnico per utenti dei sistemi informativi della regione Emilia-Romagna" (Determina n. 8901 del 6 giugno 2017),* in particolare al Capitolo 13.
- *"Linee Guida per la governance del sistema informatico regionale" (Delibera n. 281 del 29/02/2016) e successivi aggiornamenti*.

Regole/requisiti:

- **devono essere loggati gli eventi e le attività ogniqualvolta questi coinvolgano il sistema di conservazione**; inoltre deve essere possibile associare i log all'utente che ha effettuato le attività;
- **il contenuto dei log può variare a seconda dei sistemi considerati e in funzione delle limitazioni tecniche presenti**;
- **devono essere soggette a log le seguenti attività** che vanno monitorate con regolarità:
  - tentativi di accesso (falliti e riusciti) ai sistemi più critici;
  - utenti creati o disabilitati dai sistemi;
  - assegnazione e utilizzo di particolari privilegi a sistema;
  - utilizzo di utenze di amministratore;
- **devono essere ben identificate le fonti dei log** (componenti infrastrutturali, applicative e le attività da monitorare);
- **i dati di log raccolti devono essere adeguatamente protetti da accessi non autorizzati e preservati nella loro integrità;**
- i dati di **log** vanno **conservati per il tempo minimo necessario** a rispondere alla finalità per la quale sono stati raccolti e comunque nel rispetto di quanto previsto dalle politiche regionali (ad esempio il tempo di conservazione previsto da Regione è almeno un anno, mentre i dati sul database di Parer restano conservati per un massimo di 10 anni);
- **i dati di log vanno revisionati con cadenza periodica**, allo scopo di identificare eventuali anomalie e porvi rimedio;
- i dati di log devono essere resi disponibili agli Enti Produttori che ne facciano richiesta.

Responsabilità:

Soggetti coinvolti:	Resp.le del Servizio	Resp.le Servizi di Conservazione	Resp.le della sicurezza del sistema di conservaz	Resp.le Tecnologie e sviluppo sistema di conservaz	Analista/ Sviluppatore - Area Sistemi di Conservazione	Resp.le Funzione Archivistica di Conservazione	Archivista - Area Servizi di Conservazione	Resp.le dell'Infrast. Tecnologica	Resp.le Amministrativo

Attività:			ione	ione					
Definizione/revisione della regola	A,R		C	C				C	
Attuazione della regola			A	R	R			R	
Monitoraggio/verifica di attuazione della regola			A,R						

2.15 Compliance

Obiettivo:

L'obiettivo della seguente politica è quello di garantire il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni reputazionali.

Riferimenti esterni:

Relativamente al monitoraggio della normativa, ParER, fa riferimento al *Manuale della conservazione*, in particolare al Capitolo 2.3.

Regole/requisiti:

Deve essere garantito il rispetto dei requisiti in merito a:

- disposizione di legge applicabili in merito alla protezione dei dati personali e relativi Provvedimenti del garante, in riferimento ai dati trattati sia in qualità di titolare del trattamento, sia in qualità di responsabile del trattamento nell'ambito del servizio di conservazione;
- disposizioni di legge in merito alla tutela dei beni culturali;
- normativa sulla conservazione, come descritto nell'Allegato 1 "Normativa e standard di riferimento" del Manuale di Conservazione;
- norma ISO/IEC 27001:2013, ISO27017: 2015, ISO27018: 2019 e ISO9001:2015;
- i requisiti richiesti da AgID per l'accreditamento dei soggetti che svolgono attività di conservazione dei documenti secondo la circolare n. 65/2014 (G.U. n. 89 del 16/04/2014);
- obblighi contrattuali legati al servizio, con particolare riferimento agli obblighi in materia di protezione dei dati.

Responsabilità:

Soggetti coinvolti: / Attività:	Resp.le del Servizio	Resp.le Servizi di Conservazione	Resp.le della sicurezza del sistema di conservazione	Resp.le Tecnologie e sviluppo sistema di conservazione	Analista/ Sviluppatore - Area Sistemi di Conservazione	Resp.le Funzione Archivistica di Conservazione	Archivista - Area Servizi di Conservazione	Resp.le dell'Infrast. Tecnologica	Resp.le Amministrativo
Definizione/revisione della regola	A,R		C						C
Attuazione della regola	A	R	C	R	R	R	R	R	R
Monitoraggio/verifica di attuazione della regola			A,R						

2.16 Gestione degli incidenti

Obiettivo:

L'obiettivo della seguente politica è quello di garantire che gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza delle informazioni dell'organizzazione siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business.
Per incidente di sicurezza delle informazioni (di seguito "incidente") si intende un evento accidentale o un'azione deliberata potenzialmente in grado di compromettere almeno uno dei requisiti di sicurezza del sistema di conservazione.

Riferimenti esterni:

ParER, per quanto riguarda gli incidenti relativi all'infrastruttura ICT, fa riferimento:

- al *Disciplinare tecnico per la gestione degli incidenti di sicurezza e data breach (*Determina n. 12807 del 03/08/2018);
- al *Disciplinare tecnico per utenti sull'utilizzo dei sistemi informativi nella Giunta e nell'Assemblea legislativa della Regione Emilia-Romagna,* in particolare al Capitolo 14 (Determina n. 8901 del 06/06/2017).

Regole/requisiti:

- **tutti i dipendenti e i collaboratori sono tenuti a rilevare e notificare**, a chi di competenza e secondo adeguate procedure, eventuali **eventi rilevanti per la sicurezza delle informazioni**;
- **gli incidenti rilevati devono essere comunicati a tutti i soggetti coinvolti e**, ove prescritto dalla legge o dalla normativa regolamentare, **alle autorità e agli enti competenti**, in coordinamento con la Regione e nel risetto delle procedure da essa previste (es. notifiche di Data Breach)**;**
- **gli eventi/incidenti che possano avere un impatto sui livelli di sicurezza devono essere rilevati e gli eventuali danni**, potenziali e non, **devono essere gestiti**, ove possibile, **in tempi brevi** secondo specifiche procedure condivise con tutti i soggetti interessati (a partire dagli Enti Produttori);
- **deve esistere un sistema di registrazione e classificazione degli incidenti** per effettuare analisi volte al miglioramento dei livelli di sicurezza delle informazioni coerentemente con le reali problematiche riscontrate;
- **gli audit log inerenti le attività degli utenti, degli amministratori di sistema e degli operatori di sistema e gli eventi che possono compromettere la sicurezza delle risorse informative devono essere tracciati, registrati e conservati per un periodo di tempo ritenuto idoneo** (anche in conformità alle normative vigenti) ai fini della ricostruzione degli incidenti, e a supporto di future attività di accertamento di comportamenti illeciti.

Responsabilità:

Soggetti coinvolti: / Attività:	Resp.le del Servizio	Resp.le Servizi di Conservazione	Resp.le della sicurezza del sistema di conservazione	Resp.le Tecnologie e sviluppo sistema di conservazione	Analista/ Sviluppatore - Area Sistemi di Conservazione	Resp.le Funzione Archivistica di Conservazione	Archivista - Area Servizi di Conservazione	Resp.le dell'Infrast. Tecnologica	Resp.le Amministrativo
Definizione/revisione della regola	A,R		C					C	
Attuazione della regola	A	R	C	R	R	R	R	R	R
Monitoraggio/verifica di attuazione della regola			A,R						

2.17 Continuità operativa

Obiettivo:

L'obiettivo della seguente politica è quello di garantire la continuità operativa del servizio di conservazione e l'eventuale ripristino tempestivo dei servizi erogati nel momento in cui siano stati colpiti da eventi anomali di una certa gravità, riducendo le conseguenze di tali eventi sia all'interno che all'esterno del contesto dell'organizzazione.

Riferimenti esterni: NA

Regole/requisiti:

- **deve essere sviluppato un piano di continuità operativa** che si basi su un'analisi dei rischi e un'analisi degli impatti che tenga conto delle reali necessità del servizio e delle aspettative degli Enti Produttori;
- **il piano deve essere opportunamente comunicato e aggiornato**;
- **il piano deve essere periodicamente sottoposto a test di verifica**;
- **devono essere correttamente mantenuti i rapporti con tutti i soggetti interessati** in caso di disastro;
- **anche in situazione di crisi e disastro, devono essere mantenuti requisiti di sicurezza delle informazioni trattate**.

Responsabilità:

Soggetti coinvolti: / Attività:	Resp.le del Servizio	Resp.le Servizi di Conservazione	Resp.le della sicurezza del sistema di conservazione	Resp.le Tecnologie e sviluppo sistema di conservazione	Analista/ Sviluppatore - Area Sistemi di Conservazione	Resp.le Funzione Archivistica di Conservazione	Archivista - Area Servizi di Conservazione	Resp.le dell'Infrast. Tecnologica	Resp.le Amministrativo
Definizione/revisione della regola	A,R		C					C	
Attuazione della regola	R	R	A,R	R	R	R	R	R	R
Monitoraggio/verifica di attuazione della regola			A,R						

2.18 Verifiche di sicurezza

Obiettivo:

L'obiettivo della seguente politica è quello di garantire la rilevazione di vulnerabilità potenziali dei sistemi informativi al fine di assicurare la sicurezza e la disponibilità dei servizi e delle relative informazioni.

Riferimenti esterni:

Per quanto riguarda:

- le verifiche relative ai requisiti di sicurezza dei sistemi e delle informazioni, ParER fa riferimento alle *Linee guida per la governance del sistema informatico regionale (Delibera n. 281 del 29/02/2016)*;
- le verifiche annuali delle attività degli amministratori di sistema effettuate dalla Regione, si fa riferimento al **"***Disciplinare tecnico per gli amministratori di sistema della Giunta e dell'Assemblea Legislativa*" (Determinazione n. 83 del 07/01/2021), in particolare al Capitolo 7;
- le verifiche di sicurezza effettuate dalla Regione, si fa riferimento al *Disciplinare Tecnico per le Verifiche Di Sicurezza Sul Sistema Informativo Regionale* (Determinazione n. 19529 del 23/11/2018).

Regole/requisiti:

- **Devono essere pianificate attività periodiche orientate alla verifica di conformità ed efficacia del sistema di gestione della sicurezza delle informazioni**, in particolare rivolte a:
  - processi di pianificazione, attuazione, controllo e miglioramento del sistema;
  - attuazione e efficacia del sistema dei controlli organizzativi;
  - attuazione e efficacia del sistema dei controlli tecnologici, anche attraverso attività di vulnerability assessment e/o penetration test, che sono svolte in conformità ai requisiti ISO/IEC 27008.

Responsabilità:

Soggetti coinvolti: / **Attività:**	**Resp.le del Servizio**	**Resp.le Servizi di Conservazione**	**Resp.le della sicurezza del sistema di conservazione**	**Resp.le Tecnologie e sviluppo sistema di conservazione**	**Analista/ Sviluppatore - Area Sistemi di Conservazione**	**Resp.le Funzione Archivistica di Conservazione**	**Archivista - Area Servizi di Conservazione**	**Resp.le dell'Infrast. Tecnologica**	**Resp.le Amministrativo**
Definizione/revisione della regola	A,R		C					C	
Attuazione della regola	A		R	R				R	
Monitoraggio/verifica di attuazione della regola			A,R						

2.19 Sicurezza delle Comunicazioni

Obiettivo:

L'obiettivo della seguente politica è quello di garantire che siano opportunamente considerati gli aspetti di sicurezza nelle tematiche relative alla sicurezza delle comunicazioni (Network security: segregazione delle reti, monitoraggio dei gateway (firewall)).

Riferimenti esterni:

Relativamente alla gestione delle reti, ParER fa riferimento alle *Linee guida per la governance del sistema informatico regionale (Delibera n. 281 del 29/02/2016)*.

Regole/requisiti:

Tutti **i flussi contenenti pacchetti informativi in entrata e in uscita nell'esercizio dei servizi di conservazione devono essere protetti** mediante opportuni protocolli di crittografia (HTTPS e FTPS) o veicolati attraverso canali di posta certificata (PEC).

Ove possibile, i flussi di traffico originati dall'utenza del servizio (interna ed esterna) sono separati da quelli legati alle attività di amministrazione e gestione (i.e. reti differenziate).

Non è consentito utilizzare **dispositivi mobili e supporti rimovibili** (CD, hard disk, ecc.) per il trasferimento relativamente alle **attività di versamento e distribuzione di documenti in conservazione.**

Responsabilità:

Soggetti coinvolti: / **Attività:**	**Resp.le del Servizio**	**Resp.le Servizi di Conservazione**	**Resp.le della sicurezza del sistema di conservazione**	**Resp.le Tecnologie e sviluppo sistema di conservazione**	**Analista/Sviluppatore - Area Sistemi di Conservazione**	**Resp.le Funzione Archivistica di Conservazione**	**Archivista - Area Servizi di Conservazione**	**Resp.le dell'Infrast. Tecnologica**	**Resp.le Amministrativo**
Definizione/revisione della regola	A,R	C	C			C		C	C
Attuazione della regola			A	R				R	
Monitoraggio/verifica di attuazione della regola			A,R						

2.20 Relazioni con autorità esterne e gruppi specialistici

Obiettivo:

L'obiettivo della seguente politica è quello di garantire che siano stati identificati i referenti per mantenere le necessarie relazioni con le autorità esterne.

Riferimenti esterni: NA

Regole/requisiti:

- **Devono essere identificate e assegnate le responsabilità per i contatti e le comunicazioni** relative a questioni inerenti la sicurezza delle informazioni del servizio di conservazione nei confronti delle diverse autorità.
  In particolare:
  - il Responsabile Servizio di conservazione e archivio di deposito e storico dell'Emilia-Romagna è responsabile per le comunicazioni con AgID e con la Soprintendenza archivistica;
  - il Responsabile del Servizio è responsabile per le comunicazioni con la Magistratura;
  - il Responsabile della sicurezza del sistema di conservazione ha la responsabilità di mantenere i contatti con l'Ente di certificazione;
  - il Servizio ICT regionale è responsabile della comunicazione alle autorità/organismi esterni (Garante della Privacy, Polizia Postale, CSIRT, ecc), in caso di incidenti di Sicurezza e Data breach.
- **Devono essere opportunamente individuati i flussi di comunicazione verso l'interno e verso l'esterno**, rilevanti per la sicurezza delle informazioni.
  In particolare:
  - comunicazioni legate alle funzioni di vigilanza (AgID, Soprintendenza archivistica);
  - comunicazioni legate ad eventi che hanno impatto sui requisiti di disponibilità, integrità e riservatezza.

Responsabilità:

Soggetti coinvolti: / Attività:	Resp.le del Servizio	Resp.le Servizi di Conservazione	Resp.le della sicurezza del sistema di conservazione	Resp.le Tecnologie e sviluppo sistema di conservazione	Analista/Sviluppatore - Area Sistemi di Conservazione	Resp.le Funzione Archivistica di Conservazione	Archivista - Area Servizi di Conservazione	Resp.le dell'Infrast. Tecnologica	Resp.le Amministrativo
Definizione/revisione della regola			A,R			C		C	C
Attuazione della regola	A,R	R				R			
Monitoraggio/verifica di attuazione della regola	C		A,R			C			

2.21 Telelavoro e attività svolte al di fuori della sede ParER

Obiettivo:

L'obiettivo della seguente politica è quello di garantire che, sia nel caso di telelavoro sia di attività svolte al di fuori della sede ParER, siano rispettati gli stessi requisiti di sicurezza garantiti dall'utilizzo delle postazioni di lavoro interne alla sede di ParER.

Riferimenti esterni:

"*Disciplinare tecnico per utenti dei sistemi informativi della regione Emilia-Romagna" (Determina n. 8901 del 6 giugno 2017)* applicato al telelavoro e alle attività svolte al di fuori della sede ParER sia dal personale regionale sia da quello esterno che svolge attività connesse al servizio di conservazione.

Regole/requisiti:

- Nel caso di personale regionale **che svolge delle attività lavorative relative al Servizio di conservazione al di fuori della sede ParER, nell'ambito di un contratto attivo per il Telelavoro**, è necessario attenersi al Capitolo 8 del "Disciplinare tecnico per utenti dei sistemi informativi della regione Emilia-Romagna" e rispettare quanto indicato nella presente "Politica sulla sicurezza delle informazioni del sistema di conservazione".
- Nelle seguenti casistiche:
  - personale esterno **che svolge delle attività lavorative relative al Servizio di conservazione al di fuori della sede ParER**;
  - personale regionale **che svolge delle attività lavorative relative al Servizio di conservazione al di fuori della sede ParER al di fuori di un contratto attivo per il Telelavoro**;

  è necessario attenersi al Capitolo 8 del "Disciplinare tecnico per utenti dei sistemi informativi della regione Emilia-Romagna" (se applicabile) e rispettare quanto indicato nella presente "Politica sulla sicurezza delle informazioni del sistema di conservazione". In particolare, è necessario seguire le seguenti regole:
  - Nel caso di postazione di lavoro personale, l'utente è tenuto:
    - ad impostare una password a protezione del dispositivo;
    - ad impostare un blocca schermo automatico che si attiva dopo 5 minuti dall'abbandono della postazione;
    - a provvedere all'installazione di un antivirus e delle ultime patch di sicurezza del Sistema Operativo all'interno della postazione di lavoro.
  - Nel caso di postazione di lavoro regionale mobile, l'utente è tenuto ad effettuare un collegamento al dominio all'interno della rete regionale prima dell'utilizzo all'esterno della rete.

Responsabilità:

Soggetti coinvolti:	Resp.le del Servizio	Resp.le Servizi di Conservazione	Resp.le della sicurezza del sistema di conservazi	Resp.le Tecnologie e sviluppo sistema di conservazi	Analista/Sviluppatore - Area Sistemi di Conservazione	Resp.le Funzione Archivistica di Conservazione	Archivista - Area Servizi di Conservazione	Resp.le dell'Infrast. Tecnologica	Resp.le Amministrativo

Attività:			one	one					
Definizione/revisione della regola	A,R	C	C	C	C	C	C	C	C
Attuazione della regola	R	R	A	R	R	R	R	R	R
Monitoraggio/verifica di attuazione della regola			A,R						

Sez.3. Ruoli e responsabilità

Per attuare una politica di Sicurezza delle Informazioni efficiente e efficace è necessario stabilire una struttura organizzativa che sia in grado di definire, implementare e controllare l'applicazione della Politica stessa attraverso:

- la definizione degli obiettivi e delle finalità delle politiche di sicurezza identificate;
- la realizzazione del sistema di gestione della sicurezza delle informazioni, assicurandosi che tutti gli aspetti rilevanti per la Sicurezza delle informazioni si realizzino in conformità alle necessità del servizio di conservazione;
- la definizione di misure coerenti e adeguate al valore del patrimonio da proteggere e all'obiettivo del monitoraggio dell'efficacia del sistema per la sicurezza delle informazioni.

Per questo motivo, a supporto della gestione della sicurezza delle informazioni, ParER si è dotato di un'adeguata struttura organizzativa descritta nel Piano della sicurezza del sistema di conservazione in grado di definire le procedure di gestione della Sicurezza delle informazioni, di implementare tali procedure e di mantenere le misure di protezione delle informazioni, nonché di adempiere a tutti i vincoli imposti dalle normative vigenti.

Sez.4. Violazioni

Qualunque violazione a queste norme deve essere individuata e gestita. Il personale che contravviene alle politiche definite in questo documento potrà essere sanzionato secondo quando definito nel contratto di lavoro con il dipendente.

Sez.5. Ciclo di revisione

Il presente documento è di proprietà di ParER, che ha il compito di provvedere all'aggiornamento del medesimo ogni qualvolta vengano riviste le strategie dell'organizzazione e gli standard/normative di riferimento.

Il ciclo di aggiornamento viene incluso in un ciclo di Management review del SGSI al quale il servizio di conservazione si riferisce. ParER gestisce e assicura il Riesame periodico da parte della Direzione del SGSI stesso, effettuandone una valutazione globale sullo stato e sull'efficacia.

L'obiettivo del Management review è quello di:

- assicurare l'idoneità, l'adeguatezza e l'efficacia nel tempo del SGSI in termini di processi, organizzazione e risorse;
- verificare il livello di sicurezza raggiunto;
- rivedere le politiche di sicurezza.

Il Riesame deve tenere conto di variazioni del quadro legislativo nazionale e del quadro normativo interno all'organizzazione di ParER, di variazioni organizzative interne, di variazioni delle informazioni trattate in termini di numerosità e/o tipologia, delle infrastrutture tecnologiche e dei processi operativi compresi nel perimetro, dell'individuazione di nuove minacce e di variazioni degli obiettivi di sicurezza. Viene effettuato con frequenza almeno annuale, che può diventare maggiore in base alle necessità o a seguito di particolari condizioni rilevate nell'ambito di verifiche ispettive / monitoraggi / analisi di incidenti di sicurezza.

Elementi di input al riesame del SGSI sono infatti, tra gli altri, i risultati dei precedenti riesami, i risultati raccolti in sede di verifiche tecniche, ispettive e audit, sia interni che esterni, lo stato delle azioni correttive individuate nel piano di trattamento del rischio.

A valle del Riesame periodico almeno annuale, il responsabile del Servizio identifica i possibili miglioramenti applicabili al sistema e i nuovi obiettivi per la sicurezza delle informazioni, comunicati successivamente a tutte i soggetti interessati; vengono dunque pianificate le modalità con cui procedere, le azioni necessarie al raggiungimento degli obiettivi e le risorse da impiegare a tale scopo.

Sez.6. Sez.6. Allegato – Politiche di Backup del Sistema di Conservazione

ParER adotta politiche di Backup sui sistemi coerenti con le Regole regionali (Politiche e Disciplinari) e con quanto riportato al Paragrafo 2.13 del presente documento.

Nello specifico, si riportano di seguito in estrema sintesi le politiche adottate per i componenti principali del Sistema di conservazione: Database, Oggetti Memorizzati su Nastro e Sistemi Operativi.

A ParER è stata dedicata nel sistema di RER un'infrastruttura specifica per il backup, che prevede le seguenti policy:

- Sistema operativo: il backup e ripristino del sistema operativo viene gestito tramite la schedulazione di IMAGE Backup del disco di sistema operativo. Tale backup è schedulato almeno ogni 2 settimane.
- Database: il backup del database avviene con l'agente per Oracle del TSM e la retention è di 30 gg:
  - il backup FULL è schedulato una volta alla settimana
  - gli archive log sono schedulati ogni 4 ore.
- Immagini DICOM: il backup è a livello file system gestito interamente come archiviazione dal modulo applicativo TPI sviluppato da Parer che si interfaccia direttamente con il TSM server. La retention è illimitata e la schedulazione avviene giornalmente.

Inoltre, è attiva una replica della copia primaria dei documenti archiviati in locale e su diversi Siti dell'Infrastruttura ParER

La cancellazione delle copie di backup è tracciata a mezzo di un sistema di Trouble ticketing.