|  |
| --- |
|  |
|  |
| Bozza di Piano della sicurezza  del sistema di conservazione  della Provincia Autonoma di TRENTO   |  |  |  |  | | --- | --- | --- | --- | |  | *Data* | *Nominativo* | *Funzione* | | *Redazione* |  |  |  | | *Verifica* |  |  |  | | *Approvazione* |  |  |  |  |  |  | | --- | --- | | *Codice documento* | PianoSicurezza | | *Versione* | 1.0 | |
|  |
|  |
| Questo documento rappresenta una bozza pubblicabile sul sito del progetto RICORDI, in quanto non contiene alcun elemento riservato, la cui pubblicazione possa metetre a rischio il esrvizio di Conservazione della Provincia Autonoma di Trento  Eventuali informazioni riservate sarenno inserite nella copia criptografata che verrà inviata ad AgID al momento della richiesta di accreditamento |

# Indice

Indice 3

Storia delle modifiche apportate al Piano 5

Lista di distribuzione 6

Sez.1. PREMESSA - RIFERIMENTI E ALLEGATI 7

Sez.2. TERMINOLOGIA (GLOSSARIO, ACRONIMI) 8

Sez.3. NORMATIVA E STANDARD DI RIFERIMENTO 10

Sez.4. ORGANIZZAZIONE DEL SISTEMA DI CONSERVAZIONE 11

4.1 Ruoli e responsabilità del sistema di conservazione 11

4.2 Ruoli e responsabilità della sicurezza informatica del sistema di conservazione 11

4.3 Procedure di produzione, diffusione e gestione della documentazione di sicurezza 13

4.4 Procedure per l’acquisto di prodotti e servizi 13

4.5 Procedure per l’alienazione degli asset dell’organizzazione 14

4.6 Piano di formazione del personale 14

4.7 Continuità operativa 14

4.8 Piano degli audit interni del sistema e delle verifiche tecniche 15

Sez.5. PERIMETRO DEL SISTEMA DI CONSERVAZIONE 16

5.1 Schema topologico 16

5.2 Componenti fisiche 16

5.3 Piani di manutenzione delle infrastrutture 16

5.4 Servizi tecnici e impianti 16

5.5 Sistemi di sicurezza logica 17

5.6 Disaster Recovery e Continuità Operativa 17

5.6.1 Continuità operativa 17

5.6.2 Ridondanza geografica 18

5.6.3 Infrastruttura di rete (geografica e locale) 18

5.6.4 Procedura per il disaster recovery 18

Sez.6. VERIFICA DELLA CONFORMITÀ E MIGLIORAMENTO DELLA SICUREZZA DEI DATI 19

Sez.7. MONITORAGGIO E CONTROLLI 20

7.1 Procedure di monitoraggio 20

7.2 Gestione dei log 20

7.3 Politiche di conservazione dei log 20

Sez.8. POLITICHE DI SICUREZZA 21

Sez.9. GESTIONE DEGLI INCIDENTI 22

Sez.10. ELENCO DELLE PROCEDURE DI SICUREZZA PER LA CONSERVAZIONE 23

Sez.11. Documenti integrativi 26

# Storia delle modifiche apportate al Piano

|  |  |  |
| --- | --- | --- |
| *VERS.* | *Variazioni* | *Data* |
| 1.0 | Prima emissione |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Livello di riservatezza: ***riservato***

# Lista di distribuzione

|  |  |
| --- | --- |
| *Soggetti da Notificare* | |
| *Nominativi* | *Ruoli organizzativi* |
|  | Responsabile della funzione archivistica di conservazione |
| AgID |  |
|  |  |
|  |  |

# PREMESSA - RIFERIMENTI E ALLEGATI

Il presente Piano della Sicurezza (PdS) descrive l’implementazione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) della Provincia autonoma di Trento (PaT) per quanto attiene le attività di conservazione dei documenti informatici.

Il PdS fa riferimento ad una serie di documenti e procedure che devono essere utilizzate all’interno dell’organizzazione stessa.

Il presente piano descrive i principi, le regole e le politiche di sicurezza adottate a garanzia della sicurezza dei documenti conservati, sia rispetto a quanto posto in essere internamente alla PaT sia da parte dei fornitori di servizi di connettività e di data center. Le politiche di sicurezza adottate, descritte all’interno del documento “*Politiche per la sicurezza del Sistema di conservazione”,* sono disponibili agli Enti e Fornitori di PaT tramite pubblicazione sul sito web.

I piani e le procedure di dettaglio sono descritti in appositi documenti che per motivi di riservatezza sono conservati presso PaT e resi disponibili su richiesta agli interessati.

# TERMINOLOGIA (GLOSSARIO, ACRONIMI)

In aggiunta ai termini indicati nell’allegato 1 del DPCM del 3 dicembre 2013 recante Regole tecniche in materia di sistema conservazione, all’interno del documento si fa riferimento alle definizioni riportate nella tabella che segue.

|  |  |
| --- | --- |
| ***Glossario dei termini - definizioni*** | |
| Sistema | Applicazione/Servizio che deve essere disponibile agli aventi diritto in termini di esercizio e disponibilità dell’informazione. |
| Disponibilità richiesta | Tempo in cui il sistema deve essere utilizzabile in conformità alle funzionalità previste, esclusi i tempi programmati per la manutenzione, rispetto alle ore concordate per l’esercizio. |
| Periodo criticità servizio | Data/periodo in cui il dato o il servizio deve essere tassativamente erogato per esigenze specifiche del business, quali scadenze o presentazione dei dati. |
| RBAC | Role Based Access Control - Sistema di controllo accessi basato sui ruoli in cui le entità del sistema che sono identificate e controllate rappresentano posizioni funzionali in una organizzazione o processi. |
| Tempo di ripristino richiesto (Recovery Time Objective - RTO) | Tempo entro il quale un processo informatico ovvero il Sistema Informativo primario deve essere ripristinato dopo un disastro o una condizione di emergenza (o interruzione), al fine di evitare conseguenze inaccettabili. |
| Obiettivo temporale di recupero (Recovery Point Objective - RPO) | Indica la perdita dati tollerata: rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di un evento imprevisto. |

| ***Acronimi*** | |
| --- | --- |
| CA | Certification Authority |
| CAD | Codice dell’Amministrazione Digitale; il testo vigente è costituito dal DLgs 82/2005, e successive modifiche. |
| DLgs | Decreto Legislativo |
| DM | Decreto Ministeriale |
| DPCM | Decreto del Presidente del Consiglio dei Ministri |
| DPR | Decreto del Presidente della Repubblica |
| ParER | Polo archivistico della regione Emilia-Romagna |
| PaT | Provincia autonoma di Trento |
| SICTR | Servizio ICT regionale |
| SGSI | Sistema di Gestione della sicurezza delle informazioni |
| ICT | Information and communication technology |

# NORMATIVA E STANDARD DI RIFERIMENTO

La Normativa e gli standard rilevanti per la conservazione ed in particolare per la sicurezza del sistema di conservazione sono contenuti nell’Allegato 1 del *Manuale di conservazione* “*Normativa e standard di riferimento*”.

# ORGANIZZAZIONE DEL SISTEMA DI CONSERVAZIONE

## Ruoli e responsabilità del sistema di conservazione

Il modello organizzativo definito dalla Provincia autonoma di Trento prevede che la PaT possa svolgere le funzioni di archiviazione e conservazione digitale per tutte le Pubbliche Amministrazioni del territorio trentino, che ne richiedono i servizi, per favorire lo sviluppo integrato della conservazione digitale dei documenti informatici nel rispetto dei principi di efficacia, efficienza ed economicità.

Lo svolgimento delle attività di conservatore richiede la presenza di più attori coinvolti nel Servizio, ognuno dei quali ha la responsabilità di specifiche attività da svolgere. Questi ruoli si inseriscono nell’organigramma della PaT, così come previsto nel documento “*Manuale di conservazione”* del servizio in oggetto (vedi *Sez.5.* STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE).

In particolare le attività relative al servizio di conservazione coinvolgono tutti i settori della PaT che interagiscono tra loro al fine di garantire la gestione delle esigenze del produttore dei documenti.

Al fine di dotarsi di un sistema di conservazione, la PaT ha scelto di fruire dei servizi del Cloud PA offerti dal Polo Archivistico della Regione Emilia-Romagna (ParER), con cui è in atto un proficuo processo di collaborazione a partire dal xx/xx/xxxx.

## Ruoli e responsabilità della sicurezza informatica del sistema di conservazione

Nell’ambito della PaT sono stati definiti i ruoli e le responsabilità specifiche per all’attuazione degli indirizzi e delle attività necessarie per assicurare la sicurezza delle informazioni conservate. In particolare:

***Responsabile del Servizio****:*

* Definisce e raccomanda le misure di sicurezza organizzative, procedurali e tecnologiche a tutela della sicurezza delle informazioni conservate.
* Verifica il rispetto e la corretta applicazione delle misure organizzative, procedurali e tecnologiche attraverso verifiche periodiche avvalendosi del supporto delle altre figure previste nell’ambito della sicurezza delle informazioni.
* Pianifica un percorso formativo, specifico e periodico in materia di sicurezza per il personale.
* Promuove la cultura relativa alla sicurezza delle informazioni.
* Predispone, con il supporto del Responsabile della sicurezza e il Responsabile della funzione archivistica di conservazione, il *Piano della sicurezza del sistema di conservazione* e la *Politica sulla sicurezza delle informazioni del servizio di Conservazione Digitale*, nel rispetto della normativa vigente e degli standard riconosciuti in materia di conservazione digitale.
* Verifica che il SGSI sia conforme agli Standard relativi alla sicurezza delle informazioni.

***Responsabile della Sicurezza dei sistemi per la conservazione:***

* Attua le misure organizzative, procedurali e tecnologiche a tutela della sicurezza delle informazioni conservate stabilite dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza.
* Individua eventuali difformità e pianifica le necessarie azioni correttive.
* Monitora le performance dell’organizzazione attraverso la verifica dell’andamento degli indicatori associati agli obiettivi e si occupa del reporting verso la Direzione.

***Responsabile della Funzione Archivistica di conservazione***

* Supporta il Responsabile del Servizio e il Responsabile della Sicurezza dei sistemi per la conservazione, nella redazione del piano della sicurezza del sistema di conservazione, per gli aspetti di natura archivistica e di gestione documentale, nel rispetto della normativa vigente e degli standard riconosciuti in materia di conservazione digitale.
* Recepisce eventuali segnalazioni del personale che opera nel servizio di conservazione e degli Enti produttori in merito a problematiche sulla sicurezza dei documenti versati o conservati.
* Trasmette al Responsabile della Sicurezza dei sistemi per la conservazione le segnalazioni ricevute, affinché questi possa individuare e pianificare le necessarie azioni correttive.

***Responsabile dei Sistemi Informativi per la conservazione:***

* Attua le misure organizzative, procedurali e tecnologiche definite dal Responsabile del servizio di conservazione in merito all’infrastruttura tecnologica e alle procedure operative di erogazione del servizio.
* Monitora le eventuali problematiche impattanti sulla sicurezza delle informazioni, di concerto con il Gestore dell’Infrastruttura di rete della PaT (Trentino Digitale SpA) e con l’Outsourcer del sistema (ParER), segnalandole al Responsabile della sicurezza dei sistemi per la conservazione.
* Pianifica e monitora l’attuazione delle necessarie azioni correttive con i soggetti responsabili.

***Responsabile dello Sviluppo e della Manutenzione del sistema di conservazione:***

* Attua le misure organizzative, procedurali e tecnologiche definite dal Responsabile del servizio di conservazione rispetto allo sviluppo e manutenzione delle componenti software del sistema di conservazione.
* Monitora le eventuali problematiche impattanti sulla sicurezza delle informazioni nelle fasi di progettazione e realizzazione delle componenti software, in raccordo con il Responsabile dei sistemi informativi per la conservazione e, ove necessario, segnalandole al Responsabile della sicurezza dei sistemi per la conservazione.
* Pianifica e monitora l’attuazione delle necessarie azioni correttive con i soggetti responsabili.

***Responsabile del trattamento dei dati personali***

Garantisce il rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, sia riguardo ai dati personali contenuti nei documenti oggetto di conservazione che a quelli degli operatori del servizio di conservazione, trattati per consentire l’accesso al sistema di conservazione.

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 operatori del servizio di conservazione, trattati per consentire l’accesso al sistema di conservazione. L’impostazione adottata negli schemi di convenzione con gli enti produttori consiste pertanto nel riconoscimento della titolarità del trattamento di dati personali contenuti nei documenti oggetto di conservazione in capo allo stesso ente produttore e nella contestuale nomina della PaT quale “responsabile” del trattamento dei dati personali necessari all’esecuzione della convenzione e al compimento degli atti conseguenti.

Di conseguenza, la PaT si impegna, nel trattamento dei suddetti dati, ad attenersi alle istruzioni e a svolgere i compiti indicati dall'ente, così come meglio definiti nell’Allegato alla Convenzione con l’Ente Produttore “Accordo Trattamento dati personali”, da considerarsi parte sostanziale e integrante di ogni convenzione per lo svolgimento della funzione di conservazione dei documenti informatici sottoscritta con gli enti produttori.

Il Responsabile del trattamento dei dati personali 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.

Poiché il sistema informativo di supporto al processo di conservazione è gestito e amministrato dal ParER, la PaT trasferisce al ParER la responsabilità del trattamento dei dati personali necessari alla gestione e all’amministrazione del sistema informativo, per cui il ParER si impegna, nel trattamento dei suddetti dati, ad attenersi alle istruzioni e a svolgere i compiti indicati dalla PaT, così come meglio definiti nell’Allegato al Contratto di Servizio stipulato tra la PaT e il ParER, da considerarsi parte sostanziale e integrante del contratto stesso.

## Procedure di produzione, diffusione e gestione della documentazione di sicurezza

La documentazione prodotta dalla PaT nell’ambito del sistema di gestione della sicurezza delle informazioni del proprio servizio di conservazione, in linea con quanto richiesto dalla ISO27001: 2013 par. 7.5, seguono un processo strutturato di definizione, redazione, verifica, approvazione, emissione e distribuzione dei documenti interni alla PaT e della documentazione relativa a fornitori coinvolti nelle attività di sviluppo ed esercizio, come descritto nella procedura di *Gestione della Documentazione*.

## Procedure per l’acquisto di prodotti e servizi

Le politiche di sicurezza seguite dalla PaT si applicano a tutti gli attori coinvolti a diverso titolo nel sistema di conservazione, ivi inclusi i fornitori di prodotti / servizi; tutte le forniture sono sottoposte alla verifica del possesso di specifici requisiti a garanzia del rispetto delle politiche di sicurezza stabilite dalla PaT. In particolare nei capitolati tecnici e nei contratti vengono richiamate le politiche per la sicurezza delle informazioni e gli standard metodologici e tecnologici a cui i fornitori dovranno attenersi nell’esecuzione delle forniture.

Nel corso della fornitura, inoltre, la PaT sottopone a verifiche periodiche l’operato dell’Outsourcer, allo scopo di valutarne il livello di conformità alle politiche, procedure e standard richiesti per l’erogazione dei servizi oggetto di fornitura.

Per ciò che attiene le modalità di acquisizione di prodotti / servizi IT la PaT si attiene al Decreto legislativo 12 aprile 2006, n. 163 (Codice dei contratti pubblici relativi a lavori, servizi e forniture in attuazione delle direttive 2004/17/CE e 2004/18/CE) e alle Linee guida emanate dall’Amministrazione della PaT.

## Procedure per l’alienazione degli asset dell’organizzazione

La PaT prevede che, in base a quanto stabilito nell’Accordo di servizio, nel caso di cessazione del contratto con il ParER, dopo la restituzione degli archivi, il ParER proceda alla cancellazione degli archivi medesimi tramite procedure di cancellazione sicura, sia dal sito primario che dal sito di Disaster Recovery.

La PaT non utilizza supporti non riscrivibili e supporti cartacei come sistema di acquisizione e di memorizzazione dei dati in conservazione.

## Piano di formazione del personale

La formazione al personale della PaT prevede apposite sessioni educative di sensibilizzazione e formazione per il personale operante nel servizio di conservazione in merito alle politiche e procedure di sicurezza e con particolare riferimento alla riservatezza e confidenzialità delle informazioni trattate e delle relative modalità, sia durante il rapporto di lavoro che al termine, mantenendo evidenza della loro partecipazione e della consegna dei documenti.

Ogni cambiamento o aggiornamento del sistema di sicurezza viene comunicato tempestivamente a tutte le parti interessate.

## Continuità operativa

La continuità operativa è definita come la capacità di una organizzazione di adottare, per ciascun processo critico e per ciascun servizio istituzionale critico erogato con strumenti tecnologici, attraverso accorgimenti, procedure e soluzioni tecnico-organizzative, misure di reazione e contenimento ad eventi imprevisti che possono compromettere, anche parzialmente, all’interno o all’esterno dell’organizzazione, il normale funzionamento dei servizi e delle funzioni istituzionali.

Il documento “*Piano di continuità Operativa*” descrive l’approccio adottato dalla PaT per garantire la continuità operativa del servizio di conservazione. Esso comprende tutte le misure di carattere organizzativo, procedurale e tecnologico che assicurano la capacità della PaT di rispondere in modo efficace ed efficiente a gravi eventi di interruzione o indisponibilità del servizio di conservazione e/o infrastrutture di supporto (disastro), in modo da riprendere l’operatività in un tempo accettabile e con una qualità dei servizi adeguata.

Scopo del documento è descrivere gli scenari di crisi previsti dal piano, le strategie di risposta, le risorse coinvolte, le procedure operative di ripristino del servizio di conservazione.

Il Piano di continuità operativa si applica a tutte le attività che fanno riferimento alla missione e agli obiettivi strategici di PaT e pertanto tutta l’organizzazione si deve attenere a quanto descritto nel documento.

Il piano definisce le responsabilità e le azioni più idonee a gestire in modo efficace gli eventi di disastro attraverso:

* la tempestiva e l’accurata informazione verso i fruitori del servizio di conservazione;
* l’istituzione di presidi dedicati, con caratteristiche di intervento immediato, secondo una logica di *escalation* e soluzione;
* una identificazione chiara di ruoli e funzioni per minimizzare i tempi di reazione e le perdite di dati;
* una tempestiva ed efficace gestione della crisi sia dal punto di vista tecnologico che organizzativo.

A tal fine, il Piano di continuità operativa fornisce specifiche e modalità operative per:

* informare gli operatori coinvolti e interessati sulle singole responsabilità;
* rendere le modalità operative uniformi e standardizzate;
* migliorare continuamente il flusso operativo.

Per quanto attiene agli aspetti tecnologici del piano, si fa riferimento al *Piano di Continuità Operativa* del ParER.

## Piano degli audit interni del sistema e delle verifiche tecniche

Con l’obiettivo di verificare periodicamente il livello di conformità del servizio di conservazione erogato alle politiche, alle procedure e agli standard di riferimento applicabili, la PaT adotta la procedura descritta nel documento “*Audit del SGSI”*. Le attività in oggetto, in termini di pianificazione, gestione e reportistica delle attività, coinvolgono non solo i processi interni della PaT, ma anche quelli affidati in outsourcing (ParER), al fine di verificare l’intero ciclo di vita del servizio di conservazione.

# PERIMETRO DEL SISTEMA DI CONSERVAZIONE

Nel presente capitolo è descritto l’ambito di applicazione del Sistema di Gestione della Sicurezza delle informazioni della PaT, oggetto del presente Piano della sicurezza, nonché il perimetro fisico e logico degli asset a supporto dell’erogazione dei servizi in oggetto.

PaT ha individuato il presente ambito di applicazione del SGSI:

• Servizio di conservazione dei documenti informatici.

Le sedi dell’organizzazione che rientrano nel perimetro in oggetto sono:

* Gli Uffici operativi di PaT;
* I Centri Elaborazione Dati del ParER (sito primario e sito di Disaster Recovery).

Il SGSI del ParER di DR è descritto nella *Politica della Sicurezza* pubblicata sul sito del ParER.

## Schema topologico

Lo schema topologico del sistema è descritto nel capitolo 8.3.1 del *Manuale di Conservazione del* ParER.

L’accesso al sistema del ParER da parte della PaT avviene tramite Internet con protocolli Https e Ftps ed è esclusivamente di tipo applicativo; nessuna attività sistemistica viene svolta dalla PaT sul sistema di conservazione, la cui amministrazione è in carico esclusivamente al ParER.

## Componenti fisiche

Le componenti fisiche del sistema sono descritte nel capitolo 8.3.2 del *Manuale di Conservazione* del ParER.

Le uniche componenti del sistema in carico alla PaT sono le stazioni di lavoro degli utenti, la cui installazione e gestione è regolamentata da XXXXXXXXXXXXXXXXXXXXXXX.

## Piani di manutenzione delle infrastrutture

I piani di manutenzione delle infrastrutture del sito primario / DR sono gestiti dal ParER e comunicati tempestivamente alla PaT, nel caso in cui si prevedano possibili turbative del servizio.

## Servizi tecnici e impianti

La gestione dei servizi tecnici e degli impianti del sito primario / DR è in carico al ParER.

## Sistemi di sicurezza logica

La sicurezza logica del sito primario / DR, in termini di controllo degli accessi, firewall, antivirus, intrusion detection/intrusion prevention, è demandata al ParER.

La sicurezza logica delle stazioni di lavoro della PaT è regolamentata da XXXXXXXXXXXXXXXXXXXXXXX.

Per quanto concerne, l’accesso al sistema di conservazione, si fa riferimento al documento di procedura di *Gestione utenze*, in cui sono dettagliati anche i controlli effettuati dal sistema in merito agli accessi applicativi.

Le procedure e le politiche indicate riguardano tutti gli attori del sistema di conservazione (operatori dell’ente produttore e suoi delegati, operatori della PaT, Soprintendenza archivistica, fornitori e terze parti) e vengono periodicamente verificate ed aggiornate per garantire il corretto livello di sicurezza negli accessi al sistema.

## Disaster Recovery e Continuità Operativa

### 5.6.1 Continuità operativa

La tabella di seguito riporta il **Recovery Time Objective (RTO)**, ovvero la quantità massima di tempo accettabile necessario per il pieno recupero dell'operatività del sistema di conservazione dopo un incidente o disastro:

| **SERVIZIO** | **RTO** |
| --- | --- |
| Servizio di conservazione | 0 - 1 gg |

La tabella di seguito riporta il **Recovery Point Objective (RPO)**, ovvero il tempo massimo che deve intercorre tra la produzione di un dato e la sua messa in sicurezza, indicato da PaT per i relativi Dati in relazioni ai vari intervalli temporali:

| **DATO** | **RPO** |
| --- | --- |
| Dati in conservazione (oggetti in conservazione). Si considerano i dati a seguito del rapporto di versamento (identifica la responsabilità della PaT) | 0 - 1 gg |
| Dati di configurazione (Sacer: strutture, tipologie documentarie, utenti) | 3 -7 gg |
| Dati del SGSI | 2 - 3 mm |

I tempi sopra riportati sono garantiti alla PaT dal ParER, tranne l’RPO del SGSI, in quanto le componenti del SGSI sono gestite dalla PaT nel proprio sistema documentale.

### 5.6.2 Ridondanza geografica

I criteri di ridondanza geografica del sistema sono desritti nel capitolo 8.3.1 del *Manuale di Conservazione del* ParER.

### 5.6.3 Infrastruttura di rete (geografica e locale)

La rete locale della PaT …………

L’accesso a Internet ………….

### 5.6.4 Procedura per il disaster recovery

Le attività per la gestione del disaster recovery sono descritte nel *Disaster Recovery Plan* del ParER.

Il test di disaster recovery viene eseguito con periodicità annuale.

# VERIFICA DELLA CONFORMITÀ E MIGLIORAMENTO DELLA SICUREZZA DEI DATI

Per “Gestione dei rischi” si intende l’insieme dei processi di identificazione del contesto di riferimento in termini di fattori di rischio ai quali l’organizzazione è sottoposta nello svolgimento delle proprie attività (minacce, vulnerabilità, controlli esistenti), di analisi e valutazione in termini di impatti e probabilità di accadimento, di valutazione delle opzioni di trattamento e accettazione dei rischi residui, di monitoraggio e comunicazione in relazione ai risultati delle analisi e alle decisioni prese per il trattamento.

I principali elementi informativi alla base della metodologia di gestione dei rischi per la sicurezza delle informazioni definita dalla PaT sono:

* processi critici nell’ambito del servizio di conservazione;
* informazioni gestite nelle diverse fasi del processo;
* catena organizzativa, tecnica e logica sottesa all’erogazione del servizio, a supporto delle informazioni gestite, in termini di:
  + modello degli asset;
  + modello organizzativo;
  + modello dei componenti infrastrutturali;
* sistema dei controlli predisposti a protezione delle informazioni e della continuità dei servizi erogati;
* quadro di riferimento per l’impostazione del sistema di gestione della sicurezza delle informazioni.

Il processo di gestione del rischio è la base a partire dalla quale PaT ha definito ed indirizzato le proprie attività di controllo, rappresentate all’interno del presente documento e riportate nei successivi capitoli.

Per un ulteriore dettaglio, si fa riferimento al documento che descrive la metodologia adottata da PaT per l’Analisi del rischio (*Modello di analisi e trattamento dei rischi*).

Le attività di verifica e miglioramento (Audit) sono descritte in dettaglio nella procedura “*Audit del SGSI*” di conformità ai requisiti di sicurezza.

# MONITORAGGIO E CONTROLLI

## Procedure di monitoraggio

Il monitoraggio dell’infrastruttura hardware e software è in carico al ParER

Il monitoraggio delle utenze e dei relativi diritti di accesso al sistema di conservazione è effettuato periodicamente come descritto nella procedura di *Gestione Utenze*.

## Gestione dei log

Il ParER gestisce i log secondo quanto indicato nel capitolo 8.4.9 del suo *Manuale di Conservazione*.

La PaT ha diritto di consultazione dei log, previa richiesta al ParER, per la porzione di informazioni di suo interesse. I log operativi (p.e. gestione delle utenze) sono disponibili on line al personale autorizzato della PaT in ogni momento.

## Politiche di conservazione dei log

Vedi il *Manuale di Conservazione* del ParER

# POLITICHE DI SICUREZZA

Data la natura delle proprie attività, la PaT 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, PaT ha identificato, applicato e descritto la propria politica sulla sicurezza delle informazioni, contenuta in dettaglio nel documento “*Politica sulla sicurezza delle informazioni del servizio di Conservazione Digitale*”.

In particolare la PaT si impegna a sostenere il sistema di gestione della sicurezza:

* definendo una Politica, articolata in una parte generale e in una parte di dettaglio dove sono presenti le politiche specifiche;
* applicando la Politica a tutto il personale interno, i fornitori, le terze parti e gli enti produttori;
* applicando la Politica relativa agli asset ad ogni *asset* che compone il sistema di conservazione dei documenti digitali (organizzativo, procedurale, applicativo, infrastrutturale, ecc.);
* definendo ed attribuendo ruoli e responsabilità per il sistema di gestione della sicurezza;
* sensibilizzando le parti interessate e coinvolte sulla sicurezza delle informazioni;
* determinando obiettivi e politiche specifiche per la sicurezza delle informazioni, appropriati per i vari ambiti di attività;
* facilitando adeguate attività di valutazione dei rischi ed approvando i livelli di rischio accettabili;
* facilitando il controllo delle misure e dei controlli di sicurezza complessivamente attuati, mediante attività di monitoraggio, verifica e controllo, di gestione e di prevenzione degli incidenti e di continuità operativa, sempre in armonia con le strategie dell’organizzazione;
* impegnandosi nella revisione periodica del sistema di gestione della sicurezza;
* facilitando il miglioramento continuo del sistema di gestione della sicurezza, recependo modifiche nell’organizzazione o nel contesto e assicurando le risorse sufficienti per gestirlo e mantenerlo.

# GESTIONE DEGLI INCIDENTI

Per incidente di sicurezza si intende un evento o un’azione compiuta in maniera deliberata o meno, che è potenzialmente in grado di compromettere il corretto funzionamento dei sistemi e/o delle reti dell’organizzazione o l’integrità e/o la riservatezza delle informazioni in esse memorizzate od in transito, o che violi le politiche di sicurezza definite o la Normativa vigente.

La PaT ha definito una classificazione per gli incidenti attraverso una codifica preventiva basata sulle minacce dell’analisi dei rischi. I livelli di impatto sono stati identificati in maniera coerente con quanto descritto da AgID, in modo da segnalare gli eventi significativamente impattanti l’erogazione del servizio di conservazione.

Gli incidenti di sicurezza che sono gestiti secondo quanto descritto nella procedura *“Gestione incidenti di sicurezza”*, che include specifiche istruzioni operative su come affrontare gli incidenti di sicurezza, con indicazione delle azioni da intraprendere e delle responsabilità degli attori coinvolti nel processo.

La procedura “Gestione incidenti di sicurezza” è articolata nelle seguenti attività:

* Gestire gli eventi:
* *rilevare l’evento*: vengono rilevati eventi rilevanti per la sicurezza. Il rilevamento avviene a valle delle segnalazioni provenienti da strumenti automatici o ancora da segnalazioni del personale dell’amministrazione
* *valutare l’evento*: vengono riconosciuti uno o più eventi di sicurezza come incidente e a ogni incidente ne viene assegnato un livello di gravità.
* processare l’evento (bassa gravità): vengono attuate le prime contromisure, allo scopo di minimizzare i danni causati dall'evento/incidente a bassa gravità;
* *Gestire eventi gli incidenti sicurezza:* vengono attuate le opportune contromisure nel caso di incidenti a media/alta gravità. Questo sottoprocesso è completamente in carico al Responsabile della sicurezza del sistema di conservazione.
* *Gestire attività post-incidente:* attività di registrazione ed analisi degli incidenti verificatisi.

# ELENCO DELLE PROCEDURE DI SICUREZZA PER LA CONSERVAZIONE

|  |  |  |  |
| --- | --- | --- | --- |
| **Ambito** | **Descrizione sintetica** | **Nome della procedura** | **Collocazione** |
| Procedura di gestione documentale dell’organizzazione | La Procedura descrive il modo in cui la (PaT) definisce e gestisce la documentazione interna necessaria per sostenere un’efficace ed efficiente operatività del processo di conservazione | Gestione della documentazione |  |
| Procedura di gestione delle comunicazioni | La Procedura descrive il modo in cui la PaT definisce le comunicazioni rilevanti nell’ambito del processo di erogazione del servizio di conservazione e le relative modalità di formalizzazione delle stesse alla luce dei vincoli imposti alle Pubbliche Amministrazioni dalla normativa vigente. | Gestione delle Comunicazioni |  |
| Procedura di formazione | La Procedura descrive il modo in cui la PaT gestisce le attività di formazione rilevanti per la sicurezza del processo di conservazione | Formazione | *Se esiste, fare riferimento a auna procedura generale della PaT* |
| Procedura di gestione delle utenze | La procedura descrive le modalità con cui viene garantita la corretta gestione degli accessi applicativi al sistema di conservazione e include in Appendice la procedura di autenticazione seguita da un utente al momento dell’accesso all’applicativo | Gestione utenze | *Vedi procedura di ParER* |
| Procedura di Verifica Utenze | La Procedura descrive in dettaglio la maniera in cui la PaT effettua il monitoraggio periodico delle utenze che possono accedere al Sistema di Conservazione, come descritto nella procedura di Gestione Utenze, allo scopo di verificare il numero e lo stato di attività. | Verifica utenze | *Vedi procedura di ParER* |
| Procedura di gestione degli incidenti di sicurezza | La procedura Gestione incidenti di sicurezza descrive le modalità con cui vengono gestiti gli eventi che hanno un impatto sui requisiti di integrità, disponibilità e riservatezza dei dati conservati o del Servizio di conservazione | Gestione incidenti sicurezza |  |
| Procedura di gestione degli Audit SGSI | La procedura di Audit di conformità ai requisiti di sicurezza descrive l’insieme di attività e responsabilità legate alla pianificazione, conduzione e documentazione degli Audit della PaT, eseguiti per valutare il grado di applicazione e di efficacia di quanto indicato nella “Politica di sicurezza del sistema di conservazione” e nei documenti ad esso collegati e per orientare la successiva gestione delle Non Conformità riscontrate | Audit del SGSI |  |
| Procedura di Gestione delle Non Conformità | Lo scopo della procedura è di fornire indicazioni operative per la gestione delle non conformità effettive o potenziali che, verificandosi inficiano il buon andamento operativo del Servizio di conservazione e le azioni attuate per eliminare le cause delle NC stesse ovvero la descrizione delle attività svolte per la gestione delle Azioni Correttive e Preventive. | Gestione delle Non conformità |  |
| Procedura di Riesame della Direzione | La procedura ha lo scopo di descrivere come la PaT gestisce i processi interni di valutazione delle performance del servizio di conservazione erogato; nello specifico vengono qui dettagliate le attività di Riesame della Direzione.  La presente procedura è correlata con la procedura di gestione degli Audit, che descrive il processo di pianificazione, esecuzione e valutazione dei risultati degli Audit condotti internamente a PaT da personale di PaT e/o da specialisti esterni. | Riesame della Direzione |  |

# Documenti integrativi

|  |  |
| --- | --- |
| **Documento** | **Collocazione** |
| Politica sulla sicurezza delle informazioni del servizio di Conservazione Digitale |  |
| Modello di analisi e trattamento dei rischi |  |
| Piano di Continuità Operativa della PaT |  |
| Piano della sicurezza del ParER |  |
| Disaster Recovery Plan del ParER |  |