|  |  |
| --- | --- |
|  | LogoParer |
|  | |
| |  |  |  |  | | --- | --- | --- | --- | |  | *Data* | *Nominativo* | *Funzione* | | *Redazione* | 14/11/2018 |  |  | | *Verifica* |  |  |  | | *Approvazione* |  |  |  |   Impiego Esempi ParER   |  |  | | --- | --- | | *Codice documento* | Impiego Esempi ParER\_v0.1.docx | | *Versione* | 0.1 | | |
|  | |
| Il presente documento è rilasciato sotto la licenza  **Attribuzione-Non commerciale** delle Creative Commons | |

**INDICE**

STORIA DELLE MODIFICHE DEL DOCUMENTO 4

CLASSIFICAZIONE DEL DOCUMENTO 4

LISTA DI DISTRIBUZIONE 4

Introduzione 5

Scopo e ambito del documento 5

Campo di applicazione 5

1 Politica sulla sicurezza delle informazioni del sistema di Conservazione 6

2 Piano di continuità operativa 6

3 Procedure 6

PG00 Gestione documentazione 6

PG10 Audit 7

PG11 Gestione non conformità 7

PG14 Gestione incidenti di sicurezza 7

PG19 Gestione Utenze 8

# STORIA DELLE MODIFICHE DEL DOCUMENTO

| **Versione** | **Variazioni** | **Data** |
| --- | --- | --- |
| 1.0 | Prima emissione | 14/11/2018 |
|  |  |  |

# CLASSIFICAZIONE DEL DOCUMENTO

|  |  |
| --- | --- |
| **Livello di Riservatezza** | Pubblico |
| **Rilevanza** | Non Critico |
| **Classificazione** | Non Classificato |

# LISTA DI DISTRIBUZIONE

| **Soggetti da Notificare** | |
| --- | --- |
| ***Nominativi*** | ***Ruoli Organizzativi*** |
|  | Personale PAT coinvolto nel progetto Ricordi |

# Introduzione

## Scopo e ambito del documento

Il presente documento fornisce alcuni suggerimenti in merito agli adattamenti che si possono fare al fine di riutilizzare come esempi alcuni documenti di ParER rilevanti per la Certificazione 27001, che non sono stati caricati nell’area documentale dell’Azione A2, in quanto la certificazione 27001 non è oggetto del progetto Ricordi.

## Campo di applicazione

I documenti di esempio forniti da ParER di rilevanza per la Certificazione 27001 sono i seguenti:

| *Documento* | *Tipo* | *Riutilizzabilità* |
| --- | --- | --- |
| Politica sulla sicurezza delle informazioni del sistema di Conservazione\_v5.0 | Policy | Alta |
| Piano\_continuità\_operativa\_v3.0 | Piano Operativo | Alta (da semplificare) |
| PG00\_GestDocumentazione\_v.5.0 | Procedura | Media |
| PG10\_Audit\_v1.0 | Procedura | Alta |
| PG11\_Gestione\_NC\_v1.0 | Procedura | Alta |
| PG14\_GestIncSicurezza\_v1.0 | Procedura | Bassa |
| PG19\_Gestione Utenze\_v7.0 | Procedura | Media |

Altri documenti ugualmente rilevanti per la Certificazione e l’Accreditamento sono stati caricati nella documentazione dell’Azione A2.

# Politica sulla sicurezza delle informazioni del sistema di Conservazione

Questo documento costituisce il quadro generale di riferimento del Polo archivistico dell'Emilia-Romagna (ParER) rispetto alle politiche di sicurezza delle informazioni, implementate dal Polo per assicurare una corretta gestione della sicurezza delle informazioni del sistema di conservazione dei documenti digitali; contiene quindi le direttive strategiche volte a indirizzare la corretta gestione della sicurezza delle informazioni.

Poiché la regione Emilia-Romagna ha affrontato la questione della sicurezza tramite Disciplinari, Linee guida, ecc. il documento fa riferimento a tali documenti; ciò non ostante i vari capitoli sono completi nei contenuti, e quindi possono essere riutilizzati.

Le matrici di Responsabilità fanno riferimento alla struttura organizzativa di ParER, che vede la presenza di una figura non prevista da AgiD (responsabile dell’esercizio del servizio di conservazione); in generale però tale figura non ha responsabilità rilevanti ai fini della sicurezza.

Alcuni capitoli (p.e. 2.7) fanno esplicito riferimento all’infrastruttura e quindi andranno adattati.

Il capitolo sullo sviluppo non è rilevante, ma potrebbe essere sostituito da una politica sui test del software utilizzato.

Il capacity management potrebbe essere sostituito dal monitoraggio dell’archivio.

Più in generale le politiche di PAT potrebbero essere molto simili a quelle di ParER, ma il dettaglio della loro attuazione può in buona parte essere rimandato all’accordo di servizio tra PAT e ParER.

# Piano di continuità operativa

Lo scopo del Piano è descrivere i possibili scenari di disastro, le strategie di risposta, le risorse coinvolte e le procedure operative di ripristino dei servizi tecnologici e del servizio di conservazione.

Fino alla sezione 8 il Piano di ParER dovrebbe essere adattabile con poco sforzo;

Della sezione 9 in avanti dovrebbe essere specifico di PAT il solo scenario “D1\_BU - Impedimento accesso uffici per disordini sociali, disastro ambientale o disastro accidentale”; per il resto bisognerebbe fare riferimento all’accordo con ParER / Piano di Continuità di ParER (che potremmo allegare all’accordo).

# Procedure

## PG00 Gestione documentazione

La Procedura descrive il modo in cui ParER definisce e gestisce la documentazione interna necessaria per sostenere un’efficace ed efficiente operatività dei processi relativa alle modalità di progettazione, gestione e modifica del sistema di conservazione e delle sue componenti, in conformità con gli standard ISO27001 e ISO 15489-1 e con uno sguardo in avanti alla ISO9001 (che ParER ancora non possiede, ma ha in piano di conseguire).

Per la certificazione 9001 è probabile che la procedura cambi in modo significativo.

Se PAT ha già una procedura di Gestione della documentazione probabilmente conviene adattarla per stressare gli aspetti legati alla sicurezza (Riservatezza e Criticità dei documenti, Processo di Autorizzazione e Pubblicazione); se no si può semplificare quella di ParER, eliminando i riferimenti alla documentazione di sviluppo software

Va tenuto presente che la procedura dev’essere realistica, in quanto sicuramente viene verificata in fase di certificazione, visto che la certificazione si basa molto sui documenti dell’Ente.

## PG10 Audit

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 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. La procedura si applica sia ai processi interni che ai processi esterni (outsourcing).

La procedura di ParER dovrebbe essere ampliamente riapplicabile, una volta eliminati i riferimenti agli Audit tecnici.

## PG11 Gestione non conformità

La procedura fornisce 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.

La procedura di ParER dovrebbe essere ampliamente riapplicabile.

## PG14 Gestione incidenti di sicurezza

La procedura 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.

La procedura è molto specifica di ParER sia nelle classificazioni che nei passi operativi; può essere utilizzata come traccia, ma probabilmente va riscritta per PAT.

## PG19 Gestione Utenze

La procedura descrive le modalità con cui viene garantita la corretta gestione dei soggetti che hanno accesso al sistema di conservazione, con particolare riguardo alla sicurezza dei dati e delle informazioni conservate, nel rispetto della politica generale di controllo degli accessi dell’ente conservatore, riportato nelle Politiche e nel Piano della Sicurezza.

Per completezza riporta anche le regole di autenticazione seguita da un utente al momento dell’accesso ad un applicativo e le regole di validazione cui sono sottoposte le password.

La procedura caricata in A.3 è l’aggiornamento di quella originariamente caricata in A.2.

Visto i ruoli differenti svolti da ParER e PAT probabilmente la procedura va rivista abbastanza pesantemente; però va mantenuta congruenza, perché è indispensabile per la 27001 di ParER che tutti operino con gli stessi criteri.

Forse conviene alleggerirla molto, facendo esplicito riferimento a quella di ParER.