|  |  |
| --- | --- |
| P:\RER\sitoParER\Grafica\Loghi\logo-rer-+-ibc.jpg | P:\RER\sitoParER\Grafica\LogoParer-2013\LogoParer.jpg |
|  | |
| PG10 Audit   |  |  | | --- | --- | | *Codice documento* | PG10\_Audit | | *Versione* | V1.0 |  |  |  |  |  | | --- | --- | --- | --- | |  | *Data* | *Nominativo* | *Funzione* | | *Redazione* | 24/05/2018 | HSPI | Consulenti esterni | | *Verifica* | 12/10/2018 | Marco Calzolari | *Responsabile della sicurezza dei sistemi per la conservazione* | | *Approvazione* | 12/10/2018 | Marco Calzolari | *Responsabile del Servizio* | | |
|  | |
| Il presente documento è rilasciato sotto la licenza **Attribuzione-Non commerciale** delle Creative Commons. | |

# Indice

Indice 3

Storia delle modifiche del documento 4

Classificazione del documento 4

Lista di distribuzione 4

Introduzione 5

Scopo del documento 5

Campo di applicazione 6

Sez.1. Ruoli e attività Errore. Il segnalibro non è definito.

Sez.2. Pianificare e gestire gli Audit 7

2.1. Pianificare annualmente Audit 7

Sez.3. Analizzare i risultati e definire le azioni necessarie 9

3.1. Presentare e analizzare i risultati dell’audit 9

3.2. Definire azioni correttive e preventive 9

Sez.4. Matrice RACI 10

# Storia delle modifiche del documento

| **Versione** | **Variazioni** | **Data** |
| --- | --- | --- |
| 1.0 | Prima emissione | 12/10/2018 |

# Classificazione del documento

|  |  |
| --- | --- |
| **Livello di Riservatezza** | *Ad uso interno* |
| **Classificazione** | ***PaRERDoc 2.7 Procedure/Sicurezza*** |

# Lista di distribuzione

| **Soggetti da Notificare** | |
| --- | --- |
| ***Nominativi*** | ***Ruoli Organizzativi*** |
| Tutto il personale ParER |  |

# Introduzione

## Scopo del documento

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 di ParER, 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.

Gli ambiti principali di verifica sono:

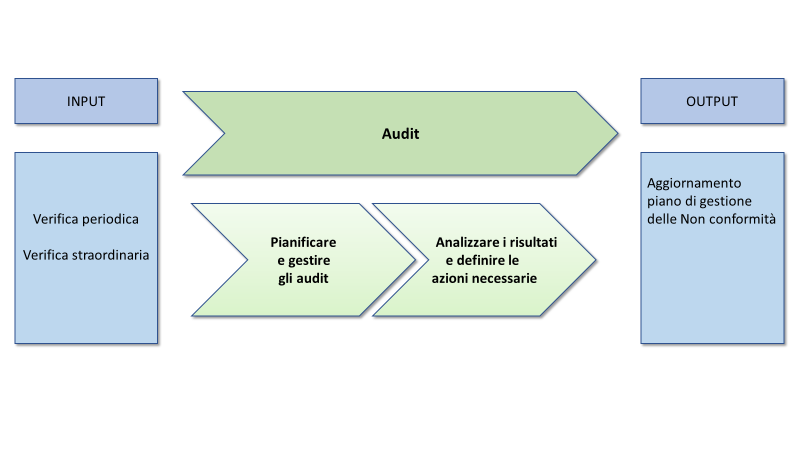
* processi interni;
* processi esterni (outsourcing).

I principali obiettivi della procedura sono:

* verificare periodicamente (annualmente o in occasione di cambiamenti significativi) il livello di conformità del servizio e del sistema di conservazione alle policy/procedure/standard in materia di sicurezza;
* verificare l’efficacia dei controlli e delle misure di sicurezza implementate dal ParER.

Gli obiettivi sono raggiunti attraverso l’utilizzo di due tipologie di audit:

* audit di sistema: audit condotti sul sistema di gestione della sicurezza di ParER e sui requisiti imposti dall’accreditamento. Tali audit comprendono verifiche sul livello di conformità a policy/procedure e standard e verifiche sull’efficacia dei controlli implementati, delle misure di sicurezza adottate e delle attività necessarie per l’accreditamento;
* audit tecnici: audit che hanno per oggetto aspetti tecnici/tecnologici, anche attraverso attività di vulnerability assessment e/o penetration test (es. le metodologie di sviluppo software), svolte in conformità ai requisiti ISO/IEC 27008.



## Campo di applicazione

La presente procedura si applica alla pianificazione e gestione degli audit di sistema/tecnici che hanno per oggetto il servizio ed il sistema di conservazione.

# 

# 1. Pianificare e gestire gli Audit

## 1.1. Pianificare annualmente Audit

Il Responsabile della Sicurezza pianifica, compilando l’apposito template “Pianificazione annuale Audit”, le attività di audit interno di sistema e tecnico indentificando gli obiettivi dell’audit, gli ambiti oggetto di verifica e i periodi di riferimento, in modo da coprire tutte le aree e i requisiti indicati nella “Politica di sicurezza del sistema di conservazione”. Lo scopo delle attività in oggetto sono:

* verificare periodicamente il livello di conformità del servizio e del sistema di conservazione alle policy/procedure/standard in materia di sicurezza;
* verificare periodicamente gli outsourcer coinvolti nell’erogazione del servizio di conservazione;
* verificare l’efficacia dei controlli e delle misure di sicurezza implementate da ParER.

La pianificazione deve essere effettuata tenendo conto dei risultati dei precedenti audit e della maturità e importanza dei processi e degli ambiti oggetto di verifica.

Eventuali audit straordinari possono essere indetti:

* al verificarsi di Non conformità rilevanti e ripetitive;
* per la verifica dell’efficacia di Azioni Correttive/Azioni Preventive attuate;
* per la verifica dell’efficacia degli interventi formativi sul personale;
* in tutti i casi in cui Responsabile della sicurezza del sistema di conservazione lo ritenga necessario per il conseguimento degli obiettivi prefissati.

1.2. Comunicare pianificazione e dettagli dell’Audit

Definita la pianificazione, il Responsabile della sicurezza del sistema di conservazione o suo delegato deve informare le aree interessate all’audit e predisporre quanto necessario per l’esecuzione della verifica stessa tra cui il gruppo di specialisti che effettuerà la verifica (gruppo di verifica). Per l’effettuazione dell’audit il Responsabile della sicurezza del sistema di conservazione può ricorrere al supporto di risorse professionali specialistiche interne o esterne a ParER scelte sulla base della conoscenza delle norme e degli standard di riferimento e in base a requisiti di obiettività ed imparzialità.

Il Responsabile della sicurezza del sistema di conservazione concorda con il Responsabile di area / Responsabile outsourcing la data effettiva di inizio della verifica, sulla base di quanto già indicativamente previsto nel Piano annuale definito.

Vengono definiti:

* data ed orario previsti di esecuzione dell’audit;
* processo/i, ambito/i in esame e relativo/i responsabile/i;
* documenti di riferimento applicabili;
* personale coinvolto;
* requisiti da verificare.

1.3. Condurre Audit

Il gruppo di verifica, identificato dal Responsabile della sicurezza del sistema di conservazione, conduce nelle date e orari concordati le verifiche pianificate.

Le attività di verifica sono fondate sul riscontro oggettivo della conformità degli ambiti esaminati alle prescrizioni e requisiti di riferimento e, se previsto, sulla verifica dell’applicazione e dell’efficacia delle azioni correttive e/o preventive eventualmente definite negli audit precedenti.

L’audit è condotto attraverso l’esame dei documenti e sulla base di domande specifiche relative alle prescrizioni e requisiti indicati nella “Politica di sicurezza del sistema di conservazione”, intervistando i responsabili delle aree di competenza e accertando la presenza delle evidenze/registrazioni necessarie.

Durante le attività di verifica, il Responsabile del gruppo di verifica discute e valuta i risultati che emergono coinvolgendo direttamente i Responsabili dei processi/ambiti verificati.

# 2. Analizzare i risultati e definire le azioni necessarie

## 2.1. Presentare e analizzare i risultati dell’audit

Il Responsabile del gruppo di verifica presenta i risultati dell’audit in un apposito Verbale di Audit (“Rapporto\_X\_audit\_interno\_XXXX”), affinché essi siano chiaramente compresi dai destinatari. Il Verbale tiene traccia di quanto verificato e di eventuali anomalie/difformità rilevate ed è strutturato nei seguenti campi:

* area / processo / ambito sottoposto a verifica;
* persona intervistata;
* data della verifica;
* non conformità riscontrate e loro descrizione;
* eventuali Osservazioni;
* requisiti/prescrizioni di riferimento;
* documentazione di riferimento e consultata.

## 2.2. Definire azioni correttive e preventive

Nel verbale si evidenzia se l’audit in oggetto è stato pianificato o se è straordinario (nel qual caso si indicano le motivazioni che hanno portato alla sua attivazione).

L’audit porta all’identificazione delle anomalie che, sulla base della gravità e degli impatti stimati, vengono classificate come Osservazioni o come Non conformità.

Il Verbale di audit rimane a disposizione del Responsabile dell’area sottoposta a verifica, il quale ha la responsabilità di comunicare i risultati al personale della sua area ed avviare la gestione delle eventuali Non conformità emerse.

Per la gestione dei rilievi emersi, si rimanda alla procedura “*PG11\_Gestione delle Non Conformità”*.

# Matrice RACI

| **RUOLI**  **ATTIVITÀ** | **Responsabile della sicurezza del sistema di conservazione** | **Responsabile area** | **Responsabile del gruppo di verifica** |
| --- | --- | --- | --- |
| Audit di conformità ai requisiti di sicurezza |  |  |  |
| Pianificare annualmente Audit | A,R |  |  |
| Comunicare pianificazione e dettagli dell’audit | A,R | C,I |  |
| Condurre audit | C,I | C,I | A,R |
| Analizzare i risultati e definire le azioni necessarie |  |  |  |
| Presentare e analizzare i risultati dell’audit |  | I | R,A |
| Definire azioni correttive e preventive |  | R | A,I |

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