|  |  |
| --- | --- |
|  | LogoParer |
|  | |
| PG19   |  |  | | --- | --- | | *Codice documento* | PG19\_GestUtenze | | *Versione* | 6.0 |  |  |  |  |  | | --- | --- | --- | --- | |  | *Data* | *Nominativo* | *Funzione* | | *Redazione* | 21-09-2017 | HSPI | Consulenti | | *Verifica* | 11-10-2017 | Gabriele Bezzi  Marco Calzolari | Responsabile Area funzione archivistica di conservazione  Responsabile della Sicurezza dei sistemi di conservazione | | *Approvazione* | 12-10-2017 | Marco Calzolari | Responsabile del Servizio |   Gestione utenze | |
|  | |

|  |
| --- |
| Il presente documento è rilasciato sotto la licenza  **Attribuzione-Non commerciale** delle Creative Commons |

**Indice**

Storia delle modifiche apportate al documento 4

Lista di distribuzione 5

Introduzione 6

Scopo e ambito del documento 6

Campo di applicazione 6

Ruoli e responsabilità 7

Informazioni Generali 8

Sez.1. Processo: Gestione utenze 10

1.1 Sotto-processo PR09.01: Definire, creare e profilare le utenze 10

1.2 Sotto-processo PR09.02: Modificare i profili delle utenze 12

1.3 Sotto-processo PR09.03: Riassegnare le password 13

1.4 Sotto-processo PR09.04: Cessare le utenze 14

1.5 Sotto-processo PR09.05: Effettuare monitoraggio su utenze e su ruoli 16

Appendice – Procedura di Autenticazione 18

Appendice – Regole di Autenticazione e Linee guida per una password “sicura” 19

# Storia delle modifiche apportate al documento

|  |  |  |
| --- | --- | --- |
| *VERSIONE* | *Variazioni* | *Data* |
| 0.2 | Prima emissione | 28-07-2014 |
| 2.0 | Revisione per adeguamento ai requisiti della ISO27001 | 30-06-2015 |
| 3.0 | Inserimento indicazioni utili ad una gestione sicura delle password | 9-11-2015 |
| 4.0 | Inserimento modalità disattivazione utenze del personale ParER  Inserimento responsabilità associate al documento Profili di accesso ai sistemi (Elenco Ruoli) | 27-11-2015 |
| 5.0 | Revisione generale | 1-07-2016 |
| 6.0 | Revisione completa per Adeguamento alle richieste della check list di Accreditamento del 2017 | 21-09-2017 |

Livello di riservatezza e rilevanza: ***critico***

Classificazione e ordinamento***:* PaRERDoc *2.4 Procedure/Esercizio***

# Lista di distribuzione

|  |
| --- |
| *Soggetti da Notificare* |
| Tutto il personale ParER |
| Outsourcer |
| Gestore dell’infrastruttura |
|  |
|  |
|  |
|  |

# Introduzione

## Scopo e ambito del documento

Il processo “Gestione utenze” descrive le modalità con cui viene garantita la corretta gestione dei soggetti che hanno accesso al sistema di conservazione, con particolare riguardo alla sicurezza dei dati e delle informazioni conservate, nel rispetto della politica generale di controllo degli accessi di ParER (vedi il documento “*Politica sulla sicurezza delle informazioni del servizio di Conservazione Digitale”* paragrafo 2.7)

È il documento indicato nella Sezione 10 del *Piano* *della sicurezza del sistema di conservazione*, a cui si fa riferimento nel paragrafo 4.3 del *Manuale della conservazione* per definire le procedure di abilitazione e autenticazione degli operatori indicati dal *Produttore*, cioè i soggetti abilitati come *Utenti* che interagiscono con i servizi del sistema di conservazione al fine di fruire delle informazioni di interesse.

Per completezza in Appendice vengono descritte la procedura di autenticazione seguita da un utente al momento dell’accesso ad un applicativo e le regole di validazione cui sono sottoposte le password.

## Campo di applicazione

Il presente processo riguarda tutti i soggetti che, tramite opportuna autenticazione, hanno accesso agli applicativi che costituiscono il sistema di conservazione di ParER (SacER, PreIngest, ecc.).

L’autenticazione alle applicazioni del sistema di conservazione viene eseguita utilizzando il componente di Identity and Access Management (SIAM) sia per quanto riguarda le funzioni on-line che per i servizi esposti.

SIAM si basa sulle seguenti entità:

* utente (operatore autorizzato ad accedere al sistema in base al suo ruolo);
* ruolo (insieme di attività che l’utente è autorizzato a svolgere nel sistema in ragione della sua collocazione nell’organizzazione di appartenenza e dei suoi ambiti di competenza);
* attività (voci di menu e pagine autorizzate, azioni esercitabili e servizi richiamabili da un utente);
* ambiti (Enti, strutture, registri e tipologie di unità documentarie su cui l’utente può operare).

SIAM fornisce agli altri componenti applicativi le informazioni relative a:

* autenticazione di un utente a una delle applicazioni, garantendo il single sign on tra i diversi applicativi mediante il proprio Identity Provider (IdP), oppure mediante qualsiasi altro IdP che lavora con standard SAML, e che sia federato con l’IdP di ParER;
* abilitazione di un utente che ha effettuato login ad una applicazione, restituendo l’insieme delle organizzazioni (strutture che effettuano versamenti in SacER o versatori in PreIngest) nell’ambito delle quali l’utente è abilitato ad operare mediante l’applicazione;
* profilazione di un utente che ha effettuato login ad una applicazione, restituendo l’insieme delle autorizzazioni (attività e ambiti) che lo caratterizzano in ragione del ruolo assegnatogli.

I ruoli previsti dal sistema e le abilitazioni che li compongono sono descritti sinteticamente nel documento “*Ruoli Utente*”. Il dettaglio delle abilitazioni è consultabile direttamente sul sistema.

La gestione dei ruoli, ovvero la modifica delle attività che sono incluse in un ruolo fa parte del processo di sviluppo (vedi documento “*PR06\_Progettazione e realizzazione di software applicativo*”); le autorizzazioni di un ruolo vengono testate durante il System test. Se il rilascio in produzione prevede anche una modifica di un ruolo, tale modifica si applica automaticamente a tutte le utenze che posseggono quel ruolo. La modifica dei ruoli e la creazione di nuovi ruoli discendono dall’approvazione dei requisiti di sicurezza inclusi nei documenti di Analisi dei Requisiti.

Il presente processo si applica sia al sistema di Produzione che al sistema di Pre-produzione utilizzato per il test degli Enti produttori o dei fornitori da loro delegati. I ruoli previsti nei due ambienti per i componenti applicativi attivi sono gli stessi.

## Ruoli e responsabilità

| **Ruolo / Funzione** | **Attività** |
| --- | --- |
| Responsabile del Servizio | * Segnala al Responsabile Area funzione archivistica di conservazione i nominativi delle utenze interne da creare o da cessare |
| Responsabile della Sicurezza | * Segnala al Responsabile Area funzione archivistica di conservazione o agli operatori di help desk i nominativi delle utenze da cessare per sospetta violazione delle norme di sicurezza |
| Responsabile Area Funzione archivistica di conservazione | * Crea e cessa le utenze sul sistema per un operatore interno a ParER e vi assegna un ruolo appropriato * Crea utenze “speciali” a seguito di accordi particolari * Cessa utenze di ParER e esterne per sospetta violazione delle norme di sicurezza |
| Responsabile Area Esercizio del Sistema di Conservazione | * Autorizza la creazione di una richiesta di reset nel caso di errato invio della password a un utente * Verifica il corretto funzionamento dei processi automatici di disattivazione e cessazione |
| Operatore di Help Desk | * Archivista che effettua le attività di gestione delle utenze e interagisce con gli Utenti esterni |
| Responsabile dell’Ente convenzionato o di un suo Ambito (Referente) | * Richiede la creazione dell’utente Gestore degli Utenti (eventualmente sé stesso), fornendone le generalità * Se necessario, ne richiede la cessazione |
| Gestore degli Utenti dell’Ente (o dell’Ambito) | * Fornisce le generalità degli operatori da abilitare al sistema di conservazione e i relativi ruoli, di cui si assume la responsabilità della creazione * Verifica le utenze abilitate per il proprio Ente o ambito di responsabilità * Segnala i nominativi delle utenze da cessare |
| Gestore esterno (dell’Ente capofila) | * Effettua le attività di gestione delle utenze e interagisce con gli Utenti degli Enti di sua competenza |

Il gestore esterno è un ruolo / funzione che deriva da specifici accordi con l’Ente convenzionato e con un Ente capofila (Ente che stipula un accordo quadro con ParER e coordina l’adesione dei singoli Enti produttori sul territorio), che si assume la responsabilità di svolgere alcune attività di supporto del processo di conservazione e di gestione del sistema di conservazione, tra cui la creazione e la cessazione di utenti esterni.

La funzione di Ente capofila può essere svolta in certi casi anche da una specifica struttura di coordinamento di un singolo Ente suddiviso in molteplici strutture (p.e. Ministero).

I gestori esterni seguono un percorso formativo specifico in ragione delle attività che debbono svolgere. Tale percorso formativo è erogato da personale di ParER.

## Informazioni Generali

La *Politica sulla sicurezza delle informazioni del servizio di Conservazione* prevede che l’accesso alle informazioni da parte di ogni singolo utente 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. L’autorizzazione da parte di ParER si realizza tramite la creazione dell’utente da parte di un operatore di Parer o da parte di un utente esterno espressamente autorizzato da ParER.

Tutte le attività di gestione delle utenze sono tracciate nei log del sistema di conservazione, mantenendo il riferimento all’utente che le ha effettuate; le attività di gestione in generale sono innescate da richieste inserite a sistema da utenti degli Enti dotati di opportune autorizzazioni, oppure, se concordato con ParER, da richieste inserite a sistema da operatori di ParER a seguito del ricevimento di una comunicazione formale dell’Ente richiedente. In generale la comunicazione formale avviene via PEC, oppure tramite documento firmato digitalmente, oppure, limitatamente agli enti interni al dominio di rete della regione Emilia-Romagna (“regione.emilia-romagna.it)”, tramite e-mail ordinaria, che ParER protocolla in ingresso.

Gli utenti del sistema di conservazione si possono classificare nelle seguenti categorie:

* Operatori interni a ParER, con diversi ruoli;
* Gestori esterni (dell’Ente capofila), che, limitatamente agli Enti convenzionati che gestiscono, svolgono alcune delle attività normalmente riservate agli operatori di ParER;
* Utenti degli Enti, ovvero persone fisiche che operano all’interno di un Ente convenzionato o di un suo fornitore delegato alle attività di test e di supporto (utenti nominativi);
* Automi degli Enti, che interagiscono con il sistema di conservazione tramite web service (utenti versatori e/o recuperatori);
* Funzionari delle Soprintendenze Archivistiche.

Gli utenti degli Enti si dividono a loro volta in due sottocategorie:

* Gestore degli Utenti dell’Ente convenzionato o di un singolo ambito (p.e. uno specifico sistema di produzione che versa in conservazione);
* Altri utenti con diverse possibili profilazioni.

Nella maggior parte degli Enti esiste un unico gestore degli utenti, che opera per l’intero Ente; enti particolarmente complessi possono avere gestori degli utenti suddivisi per ambito. Sotto propria responsabilità gli Enti possono nominare come gestore degli utenti di un ambito o dell’intero Ente un soggetto terzo, p.e. appartenente ad un proprio fornitore o al proprio Ente capofila.

Limitatamente ai sistemi di accesso gli Enti, sotto propria responsabilità, possono autorizzare la creazione di utenti di sola interrogazione anche esterni all’Ente stesso, ma sottoposti alle stesse regole di sicurezza degli utenti dell’Ente.

Gli Enti possono richiedere la creazione di utenti che non hanno necessità di accedere al sistema, ma solo di ricevere comunicazioni e notifiche. Tali utenti non hanno alcuna abilitazione al sistema, ma possono successivamente essere trasformati in utenti effettivi, tramite una modifica di profilazione.

La gestione delle password segue le politiche di sicurezza della regione Emilia-Romagna, come descritto nella *Politica sulla sicurezza delle informazioni del servizio di Conservazione*, integrate dalle specifiche necessità della conservazione digitale.

Al momento della creazione dell’utenza la password viene generata automaticamente da un randomizzatore per tutti gli utenti nominativi, mentre viene assegnata manualmente da un operatore di ParER (o di un Ente capofila) per gli automi di versamento. La password è mantenuta nel sistema come hash calcolato secondo l’algoritmo PBKDF2 (Password-Based Key Derivation Function 2).

All’indirizzo nominativo dell’utente viene inviata una prima e-mail contenente lo user-id e una seconda contenente la password per accedere al sistema; l’e-mail, seguendo un modello standard, espone le regole che l’utente dovrà seguire al momento della connessione al sistema. Inoltre l’e-mail contiene il seguente testo standard: “Al fine di rispettare le politiche di ParER relative alla sicurezza delle informazioni, Vi preghiamo di:

* *Non rispondere alla presente e-mail e non inoltrarla ad altri indirizzi*
* *Provvedere all’eliminazione della presente e-mail una volta adottata la password”.*

Tutte le password, a parte quelle degli automi di versamento, devono essere modificate al primo accesso.

Al momento dell’inserimento della nuova password, il sistema suggerisce all’operatore le “Regole” per una password “sicura”, che sono riportate in appendice, assieme alle regole di autenticazione applicate dal sistema al momento dell’accesso.

Nel caso in cui un utente provi ad accedere tre volte consecutive con una password errata, l’utenza viene bloccata; per sbloccarla bisogna attivare la procedura di riassegnazione della password descritta in questo documento.

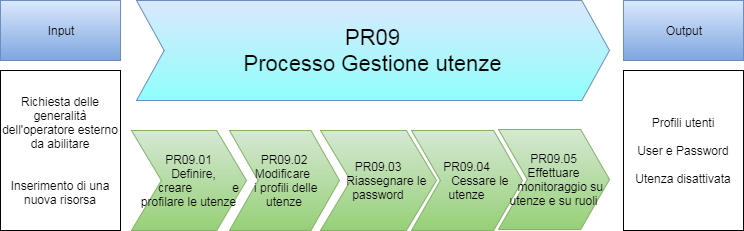
Le utenze, quando non sono più utilizzate, vengono disabilitate; dopo un certo periodo dalla disabilitazione, se non vi è nel sistema alcun evento che faccia riferimento a tale utenza, l’utenza disabilitata viene cancellata, altrimenti viene cessata; l’utenza cessata non può essere riattivata.

# Sez.1. Processo: Gestione utenze

Il processo di Gestione utenze si suddivide nei seguenti sotto-processi:

* Definire, creare e profilare le utenze;
* Modificare i profili delle utenze;
* Riassegnare le password;
* Cessare le utenze;
* Effettuare monitoraggio su utenze e su ruoli.

Di seguito viene rappresentato un quadro di sintesi del processo in esame, con indicazione degli input, degli output e la scomposizione nei relativi sotto-processi.



## Sotto-processo PR09.01: Definire, creare e profilare le utenze

***Macro-attività-*** UTENZE ESTERNE: GESTORE DEGLI UTENTI

Quando ha concluso l’accordo di conservazione con ParER, l’Ente convenzionato richiede a ParER la creazione nel sistema dell’utente Gestore degli Utenti dell’Ente (o degli utenti gestori dei diversi Ambiti, qualora ve ne fossero più d’uno), inviando una richiesta formale tramite PEC. L’invio della richiesta è di competenza del Responsabile dell’Ente convenzionato (Referente), il quale solitamente, come indicato nel Manuale della Conservazione al punto 4.2 è “il *Responsabile della gestione documentale* o il responsabile di specifici sistemi di produzione documentale versanti in conservazione […]. Se nominato può essere anche il *Coordinatore della gestione documentale.”* Il Gestore degli utenti dell’Ente o dell’Ambito (d’ora in avanti “Gestore”) può coincidere con il Referente dell’Ente stesso, oppure può essere persona da lui delegata. Sotto propria responsabilità, l’Ente può nominare come utente Gestore un appartenente a un proprio fornitore oppure al proprio ente capofila.

Per l’utente Gestore debbono essere necessariamente forniti almeno:

* Nome e cognome;
* Indirizzo di e-mail interno al dominio dell’Ente o dell’azienda fornitrice o del capofila.

Ricevuta la richiesta, un operatore di help desk di ParER (o del capofila) provvede a caricare nel sistema la richiesta di creazione del Gestore, registrando nel sistema anche il riferimento alla comunicazione, e caricando un eventuale file allegato alla comunicazione, se le informazioni sono state inviate sotto forma di allegato.

Al Gestore viene attribuito l’opportuno ruolo relativamente agli ambiti che lo riguardano.

L’operatore di help desk di ParER (o del capofila) provvede successivamente a evadere la richiesta, creando l’utente nel sistema e inviando tramite due e-mail separate all’indirizzo di mail indicato nella richiesta lo user-id e la password, che l’utente deve necessariamente cambiare al primo accesso.

***Macro-attività-*** UTENZE ESTERNE: ALTRI UTENTI

Per la creazione di ulteriori utenze normalmente il Gestore, avendo accesso al sistema, carica la richiesta di creazione direttamente nel sistema tramite l’opportuna transazione; qualora però l’Ente abbia concordato con l’help desk di inviare la richiesta tramite una comunicazione formale, l’operatore di help desk di ParER (o del capofila) provvede a caricare la richiesta in riferimento alla comunicazione, come per il caso dell’utente Gestore, desumendo le informazioni dal testo della comunicazione o dal file allegato, compilato dall’Ente in base all’apposito modulo pubblicato sul sito di ParER o del capofila.

Per queste utenze, oltre alle generalità, è necessario indicare anche il profilo che l’utente deve avere e le relative abilitazioni, ovvero il ruolo richiesto e gli ambiti di pertinenza. Anche gli automi sono trattati come utenti con un ruolo specifico.

L’Ente può indicare tra i suoi utenti anche propri fornitori di servizi; le indicazioni fornite sono sotto la piena responsabilità dell’Ente convenzionato, in quanto ParER non può effettuare alcuna verifica sulla veridicità e sulla correttezza delle informazioni fornite dagli Enti rispetto ai propri utenti.

L’operatore di help desk di ParER (o il capofila) provvede successivamente a evadere la richiesta, seguendo lo stesso iter che ha seguito per l’utente Gestore.

Destinatario delle e-mail è esclusivamente l’indirizzo individuale di posta dell’utente fornito dall’Ente.

Nel caso di utenti versatori (automi), le credenziali di accesso al sistema vengono inviate tramite e-mail all’indirizzo del Gestore degli utenti dell’Ente o ad altro indirizzo, anche del fornitore, esplicitamente indicato nella richiesta o nella comunicazione formale.

***Macro-attività-*** UTENZE PARER

Nel caso di operatori interni a ParER, il processo si innesca con l’inserimento nell’organizzazione di una nuova risorsa o con la modifica delle mansioni di una risorsa interna a ParER.

Il Responsabile del Servizio carica una richiesta di creazione nel sistema, oppure segnala vie e-mail al Responsabile Funzione archivistica di conservazione i nominativi delle utenze interne da creare. Tale segnalazione si configura come autorizzazione ad accedere alle informazioni contenute nel sistema di conservazione, nei limiti previsti dalla *Politica sulla sicurezza delle informazioni del servizio di Conservazione.*

Il responsabile dell’Area funzione archivistica di conservazione si occupa delle successive fasi di creazione e profilazione, che sono analoghe a quelle seguite per gli utenti esterni

Agli utenti interni viene assegnato il ruolo opportuno, in funzione all’area di appartenenza e delle attività svolte.

***Macro-attività-*** UTENZE “SPECIALI”

Gli utenti con ruoli particolari (Gestori Esterni appartenenti a Enti capofila, Utenti delle Soprintendenze Archivistiche, ecc.) vengono creati dagli operatori di help desk di ParER a seguito di specifici accordi formali intercorsi tra ParER e il rispettivo Ente di appartenenza.

Gli utenti automa necessari al funzionamento del Sistema di conservazione, nonché gli utenti da utilizzare per effettuare i test sul Sistema stesso sono creati dal personale dell’Area Sviluppo su richiesta del Responsabile dell’Area stessa.

***Attribuzione delle responsabilità***

| **RUOLI ORGANIZZATIVI**  **MACRO-ATTIVITÀ** | **Responsabile del Servizio** | **Responsabile dell’Ente** | **Operatore Help Desk** | **Gestore Esterno (Capofila)** | **Responsabile funzione archivistica di conservazione** | **Gestore degli Utenti** |
| --- | --- | --- | --- | --- | --- | --- |
| Utenze esterne: Gestore degli Utenti |  | R | A | A |  |  |
| Utenze esterne: Altri |  |  | A | A |  | R |
| Utenze ParER | R |  |  |  | A |  |
| Utenze “Speciali” | C |  | A |  | R |  |

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

## Sotto-processo PR09.02: Modificare i profili delle utenze

***Macro-attività-*** UTENZE ESTERNE: ALTRI UTENTI

Le successive modifiche e integrazioni rispetto alla profilazione iniziale (ruolo e ambiti) vengono effettuate dal Gestore degli utenti caricando la richiesta di modifica del profilo direttamente nel sistema tramite l’opportuna transazione; qualora però l’Ente abbia concordato con il proprio archivista di riferimento di inviare la richiesta tramite una comunicazione formale, l’operatore di help desk di ParER (o del capofila) provvede a caricare la richiesta in riferimento alla comunicazione, desumendo le informazioni dal testo della comunicazione o dal file allegato, compilato dall’Ente in base all’apposito modulo pubblicato sul sito di ParER o del capofila.

L’operatore di help desk di ParER (o del capofila) provvede successivamente a evadere la richiesta, eseguendo le opportune transazioni di sistema.

***Attribuzione delle responsabilità***

| **RUOLI ORGANIZZATIVI**  **MACRO-ATTIVITÀ** | **Gestore degli Utenti** | **Operatore Help Desk** | **Gestore Esterno (Capofila)** |
| --- | --- | --- | --- |
| Utenze esterne: Altri | R | A | A |

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

## Sotto-processo PR09.03: Riassegnare le password

***Macro-attività-*** RESET DELLA PASSWORD

Nel caso in cui l’utente abbia dimenticato la password, il suo Gestore può chiederne la riassegnazione (reset) caricando la richiesta di reset direttamente nel sistema tramite l’opportuna transazione; qualora però l’Ente abbia concordato con il proprio archivista di riferimento di inviare la richiesta tramite una comunicazione formale, l’operatore di help desk di ParER (o del capofila) provvede a caricare la richiesta in riferimento alla comunicazione, desumendo le informazioni dal testo della comunicazione o dal file allegato, compilato dall’Ente in base all’apposito modulo pubblicato sul sito di ParER o del capofila.

L’operatore di help desk di ParER (o dell’Ente capofila) procede successivamente con il reset della password, creando una nuova password e inviandola all’indirizzo di mail personale dell’utente.

Nel caso in cui si rilevi che la password di un utente sia accessibile a soggetti diversi da quelli autorizzati, l’operatore di ParER (o dell’Ente capofila) procede immediatamente con il reset della password e con le verifiche del caso, prima dell’invio.

***Macro-attività-*** REINVIO DELLA PASSWORD

In caso di Creazione nuovo utente, Riattivazione e Reset password, il Sistema genera casualmente le password, le memorizza in forma criptata e le presenta a video in chiaro in modo che l’operatore possa comunicarle all’utente; la password, quindi, per poter essere comunicata all’utente viene gestita in chiaro sul sistema.

Per ridurre al minimo i rischi derivanti dalla gestione di password in chiaro, la password generata viene visualizzata a video in modo temporaneo, per il tempo strettamente necessario a poter essere comunicata all’utente.

Nel caso in cui la comunicazione della password all’utente non vada a buon fine, non è possibile procedere immediatamente alla generazione di una nuova password, in quanto al sistema la password generata non risulta ancora utilizzata, perché non è stata modificata dall’utente al primo accesso (che non è stato effettuato).

In questo caso sono possibili due soluzioni:

* Il Gestore degli Utenti dell’Ente presenta una nuova richiesta;
* Il Responsabile dell’Esercizio del Sistema di Conservazione di ParER (o il capofila), fatte le opportune verifiche, autorizza gli operatori di help desk a caricare e evadere una richiesta di reset, evidenziando che la nuova password è necessaria perché la precedente era stata generata ma non comunicata.

***Attribuzione delle responsabilità***

| **RUOLI ORGANIZZATIVI**  **MACRO-ATTIVITÀ** | **Gestore degli Utenti** | **Operatore Help Desk** | **Gestore Esterno (Capofila)** | **Responsabile Esercizio del Sistema** |
| --- | --- | --- | --- | --- |
| Reset della password | R | A | A |  |
| Reinvio della password | R | A | A | C |

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

## Sotto-processo PR09.04: Cessare le utenze

***Macro-attività-*** DISATTIVAZIONE AUTOMATICA

L’utente che non ha mai fatto accesso al sistema negli ultimi 90 giorni viene disattivato da un processo automatico; ciò significa che non può più accedere al sistema con la password corrente.

L‘utente disattivo può essere successivamente cessato oppure riattivato, nel caso in cui non sia ancora scattato il limite temporale per la cessazione.

***Macro-attività-*** CESSAZIONE AUTOMATICA

L’utente che è disattivo da almeno 180 giorni viene eliminato automaticamente dal sistema.

L’eliminazione può dare atto a:

* cancellazione fisica dell’utenza dal sistema, ovvero eliminazione dalle tabelle del data base, nel caso in cui non esista nel sistema alcuna traccia di attività (dirette) svolte dall’utente, ovvero nel caso in cui l’utente non abbia mai agito nel sistema, e non vi siano nemmeno attività (indirette) che lo riguardano, quali p.e. richieste di riattivazione da parte di un altro utente;
* cancellazione logica dell’utenza del sistema, ovvero marcatura dell’utenza nelle tabelle del sistema, in maniera tale da non essere più accettata del sistema di autenticazione, nel caso in cui il sistema contenga dei riferimenti all’utenza; l’utente resta presente nel ruolo di “cessato” nel data base, come attributo delle azioni dirette o indirette che lo riguardano.

***Macro-attività-*** RIATTIVAZIONE

L’utenza disattiva può essere riattivata dal Gestore degli utenti dell’Ente caricando la richiesta di riattivazione direttamente nel sistema tramite l’opportuna transazione; qualora però l’Ente abbia concordato con il proprio archivista di riferimento di inviare la richiesta tramite una comunicazione formale, l’operatore di help desk di ParER (o del capofila) provvede a caricare la richiesta in riferimento alla comunicazione, desumendo le informazioni dal testo della comunicazione o dal file allegato, compilato dall’Ente in base all’apposito modulo pubblicato sul sito di ParER o del capofila.

Successivamente l’operatore di help desk di ParER (o il capofila) provvede alla riattivazione, con conseguente generazione di una nuova password, che invia all’indirizzo di mail personale dell’utente.

***Macro-attività-*** CESSAZIONE MANUALE DI UTENZE ESTERNE

Il Gestore degli utenti dell’Ente può chiedere la cessazione di utenti di sua pertinenza, p.e. a seguito di interruzione del rapporto di lavoro o di modifiche agli incarichi, caricando la richiesta di cessazione direttamente nel sistema tramite l’opportuna transazione; qualora però l’Ente abbia concordato con il proprio archivista di riferimento di inviare la richiesta tramite una comunicazione formale, l’operatore di help desk di ParER (o del capofila) provvede a caricare la richiesta in riferimento alla comunicazione, desumendo le informazioni dal testo della comunicazione o dal file allegato, compilato dall’Ente in base all’apposito modulo pubblicato sul sito di ParER o del capofila.

***Macro-attività-*** CESSAZIONE DIUTENZE PARER

Il Responsabile del Servizio, p.e. a seguito di interruzione del rapporto di lavoro o modifiche agli incarichi, segnala via e-mail il nominativo dell’utenza interna da cessare al Responsabile Funzione archivistica di conservazione, che provvede a cessare l’utenza e a informare il Responsabile del Servizio dell’avvenuta cessazione.

***Macro-attività-*** CESSAZIONE PER RAGIONI DI SICUREZZA

Il Responsabile della Sicurezza può segnalare via e-mail al Responsabile Funzione archivistica di conservazione o, se non disponibile al momento, all’help desk di ParER un’utenza da cessare in quanto dai log di sicurezza del sistema o da altre informazioni in suo possesso, quali segnalazioni da parte degli operatori di ParER del Gestore degli Utenti di un Ente risultino tentativi di violazioni di sicurezza tramite tale utenza. Il destinatario della segnalazione provvede a cessare l’utenza e a informare il Responsabile della Sicurezza dell’avvenuta cessazione.

***Attribuzione delle responsabilità***

| **RUOLI ORGANIZZATIVI**  **MACRO-ATTIVITÀ** | **Responsabile del Servizio** | **Responsabile della Sicurezza** | **Operatore Help Desk** | **Gestore degli Utenti** | **Responsabile Esercizio del Sistema** | **Responsabile funzione archivistica di conservazione** | **Gestore Esterno (Capofila)** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Disattivazione Automatica |  | R | I |  |  |  | I |
| Cessazione Automatica |  | R | I |  |  |  | I |
| Riattivazione |  |  | A | R |  |  | A |
| Cessazione Manuale Utenze Esterne |  |  | A | R |  |  | A |
| Cessazione Utenze ParER | R |  |  |  |  | A |  |
| Cessazione per ragioni di sicurezza |  | R | A |  |  | A |  |

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

## Sotto-processo PR09.05: Effettuare monitoraggio su utenze e su ruoli

***Macro-attività-*** MONITORAGGIO PERIODICO DELLE UTENZE

Annualmente gli operatori di help desk dell’Area esercizio servizi di conservazione verificano se le utenze attive sul Sistema di conservazione debbano essere ancora autorizzate ad accedere tramite uno scambio di comunicazioni formali con il Gestore degli utenti dell’Ente.

L’help desk provvede alla cessazione degli utenti che l’ente dichiara non più attuali.

***Macro-attività-*** MONITORAGGIO PERIODICO DEI RUOLI

Annualmente il Responsabile della sicurezza, con il supporto del Responsabile esercizio servizi di conservazione e del Responsabile funzione archivistica di conservazione, verifica la coerenza tra il ruolo e i profili di accesso associati ed eventualmente aggiorna il documento “*Profili di accesso ai sistemi -Elenco ruoli*”.

***Attribuzione delle responsabilità***

| **RUOLI ORGANIZZATIVI**  **MACRO-ATTIVITÀ** | **Responsabile del Servizio** | **Responsabile della Sicurezza** | **Operatore Help Desk** | **Gestore degli Utenti** | **Responsabile Esercizio del Sistema** | **Responsabile funzione archivistica di conservazione** | **Gestore Esterno (Capofila)** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Monitoraggio periodico delle utenze |  |  | A | C | R | C |  |
| Monitoraggio periodico dei ruoli |  | R,A |  |  | C | C | I |

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

# Appendice – Procedura di Autenticazione

L’ accesso ad una applicazione da parte di un utente si svolge secondo la procedura seguente:

* l’utente specifica lo URL dell’applicazione, che effettua una chiamata al modulo SIAM
* poiché l’utente non ha ancora una sessione aperta nell’applicazione, SIAM richiede l’autenticazione dell’utente all’IdP
* poiché per l’utente non è ancora definita una sessione nell’IdP, l’IdP presenta la pagina di login con cui richiede all’utente di fornire userid e password
* l’utente fornisce userid e password all’IdP
* l’IdP valida l’utente e la password nel Data Base che gli è associato (SIAM nel caso dell’IdP di ParER, LDAP o altri sistemi nel caso di IdP federati), verificando che lo user-id sia definito e che la password sia corretta e ancora valida; se le verifiche falliscono, l’IdP segnala l’errore ed il processo è terminato (nel caso in cui la password sia scaduta, l’IdP richiede all’utente nominativo di modificarla e, dopo la modifica, il processo riprende dal punto precedente; la richiesta non viene effettuata per gli automi versatori)
* la richiesta di cambio password dell’utente nominativo è effettuata automaticamente dall’IdP al momento del primo accesso al sistema da parte di un nuovo user-id; la richiesta non viene effettuata per l’utente versatore; l’eventuale cambio di password per l’utente versatore dev’essere effettuato da un utente Amministratore del modulo SIAM
* l’IdP restituisce all’applicazione l’autenticazione dell’utente (nel token SAML restituito si espongono gli attributi che definiscono il cognome, il nome, lo userid e l’identificatore dell’utente)
* Qualora l’utente sia configurato come limitato a specifici indirizzi IP, SIAM verifica che l’indirizzo di chiamata sia compreso tra quelli previsti.
* SIAM provvede a verificare che l’utente sia abilitato all’applicazione corrente; se l’utente non è abilitato, l’applicazione segnala errore ed il processo termina
* se l’applicazione richiede la scelta dell’organizzazione su cui operare, l’applicazione acquisisce dal Data Base di SIAM le abilitazioni dell’utente alle organizzazioni, tra le quali l’utente deve scegliere quella su cui operare; se l’utente non ha abilitazioni ad alcuna organizzazione, l’applicazione segnala errore ed il processo termina
* l’applicazione richiede a SIAM (mediante servizio) la lista dei ruoli che profilano l’utente e delle autorizzazioni associate a quei ruoli
* SIAM restituisce all’applicazione la lista dei ruoli / autorizzazioni che profilano l’utente
* SIAM restituisce inoltre all’applicazione le news da comunicare sulla home page
* l’applicazione restituisce all’utente la home page dell’applicazione con le informazioni relative all’utente che ha fatto l’accesso, l’organizzazione scelta e le eventuali news ed il menù dell’applicazione profilato in funzione delle autorizzazioni dell’utente.

# Appendice – Regole di Autenticazione e Linee guida per una password “sicura”

La password deve essere modificata al primo accesso dopo l’invio da parte dell’operatore di ParER o dell’ente capofila.

Inoltre deve essere modificata almeno ogni 90 giorni.

Dal punto di vista del testo, la password deve:

* essere lunga almeno 8 caratteri;
* contenere almeno un numero;
* contenere almeno un carattere speciale (per es. !, \*, /, ?, #);
* essere diversa dalle ultime cinque password utilizzate.

Qualora l’utente sia configurato come limitato a specifici indirizzi IP, viene verificato che l’indirizzo di chiamata sia compreso tra quelli previsti.

Regole “di buon senso” da applicare nella creazione di una password, suggerite all’utente, ma non validabili dal sistema:

* scegliere la password in modo che non sia collegata alla propria vita privata (per es. il nome o il cognome di familiari, la targa dell'auto, la data di nascita, la città di residenza, ecc.)
* non scegliere come password parole comuni riportate in un vocabolario (facilmente attaccabili da software di password cracking).
* modificare la password anche prima della scadenza automatica di 90 giorni nel caso in cui si sospetti che qualcun altro ne sia venuto a conoscenza