GESTIONE UTENZE

1. Introduzione

1.1 Obiettivi

Il presente documento ha l'obiettivo di definire le regole di sicurezza per il controllo degli accessi logici, disciplinando i ruoli e le responsabilità che intervengono nel processo.

Il presente documento si applica all'interno Della struttura del Titolare, nel rispetto delle disposizioni impartite dalle normative vigenti in materia di Privacy.

1.2 Descrizione

Una corretta gestione delle utenze, in particolare di quelle privilegiate, e delle password ad esse associate è alla base della sicurezza nell'amministrazione dei sistemi e del controllo sulle attività svolte.

La mancanza di criteri per la corretta gestione delle utenze, l'utilizzo di password deboli o la totale mancanza di password per le Utenze di tipo amministratore comporta i seguenti rischi:

- possibile installazione nella postazione amministratore di programmi che agevolano azioni intrusive non autorizzate;
- utilizzo improprio dei privilegi dell'amministratore;
- distruzione dei dati;
- blocco completo di parti del Sistema Informatico;
- esportazioni non autorizzate e utilizzo di informazioni riservate (come ad esempio, dati aziendali, dati personali e sensibili oggetto di trattamento ex legge 196/03, dati personali trattati da persone fisiche per scopi esclusivamente personali).

1.3 Definizioni e Acronimi

Credenziali Insieme di informazioni di sicurezza assegnate all'utente, che consentono di identificarlo ed autenticarlo.

Utenza Insieme di attributi di sicurezza associati all'utente, costituiti da credenziali e da autorizzazioni per l'accesso e l'utilizzo delle risorse IT.

Profilo Insieme delle operazioni che l'utente può compiere sui dati e programmi.

Owner È colui che per primo introduce dati in azienda o che istituzionalmente li origina.

SSO Sistema centralizzato di accesso ai sistemi informativi.

Amministratore E' colui che ha la gestione delle macchine o applicazioni specifiche a lui assegnate.

2. Ruoli e responsabilità

Di seguito si evidenziano i ruoli e le responsabilità delle funzioni che intervengono.2.2

2.1 Security Management

Chi si occupa di Security Management ha la responsabilità di:

- definire le regole generali per il controllo degli accessi logici (di cui al presente documento);
- essere di riferimento per chiarimenti e fornire soluzioni in caso le regole non possano trovare facile e immediata applicazione nell'infrastruttura tecnologica esistente;
- controllare l'effettiva e corrente applicazione delle regole di sicurezza definite;
- creare ed amministrare i profili office di accesso di utenti interni ed esterni (consulenti e fornitori), ed amministrarne le credenziali;
- creare e gestire le utenze dell'infrastruttura tecnologica (comprese utenze esterne ed utenze applicative);
- garantire la completezza delle informazioni di sicurezza relative agli utenti;
- garantire la consistenza dei dati presenti nel sistema di sicurezza centrale per l'amministrazione delle utenze;
- gestire la storicizzazione degli account e delle loro attività per garantire la corretta ricostruzione dei dati degli utenti;
- governare il processo di alimentazione dallo strumento di amministrazione verso altri eventuali sottosistemi di sicurezza
- garantire l'applicazione dei profili indicati in termini di correttezza, completezza e disponibilità
- monitorare gli eventi, mantenendo la responsabilità di definire e/o cancellare gli utenti;
- redigere tutta la documentazione necessaria (istruzioni operative).

2.2 Sviluppo

Chi si occupa di sviluppo ha la responsabilità di:

- analizzare e valutare aspetti di sicurezza nel controllo degli accessi logici e provvedere allo sviluppo di soluzioni adeguate o alla definizione di specifiche ad hoc, sulla base dell'approccio definito da chi si occupa di Security Management;

2.3 Direzione Risorse Umane

Ha la responsabilità di:

- comunicare tempestivamente a chi si occupa di security tutte le variazioni relative ai dipendenti (nuovi assunti, dimessi, licenziati, cambio di ruolo, etc.).

3. Aspetti legali

In conformità con le attuali disposizioni impartite in materia di Privacy, vige l'obbligo, nei casi previsti, di proteggere l'accesso ai dati mediante l'utilizzo di una parola chiave; ciò vale indipendentemente dal fatto che i dati risiedano su computer collegati stabilmente in rete o configurati in modalità *stand alone.*

Il presente documento recepisce anche i contenuti per l'attuazione delle prescrizioni previste dalla legge e consente di focalizzare l'importanza di una corretta e disciplinata gestione aziendale delle utenze e password.

4. Regole di sicurezza per il controllo degli accessi logici

4.1 Requisiti di sicurezza

Di seguito, si definiscono gli indirizzi e le regole per la corretta gestione delle credenziali, sia utente che amministrative.

Per credenziali si intende la coppia user-ID e password (parola chiave).

La user-id deve definire in modo univoco un utente per i sistemi informatici, mentre la password costituisce l'elemento segreto che consente all'utente – e solo ad esso - l'accesso alle risorse a cui è stato autorizzato.

Le credenziali sono gestite dal gruppo degli amministratori (ossia dei soggetti che hanno il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione).

Le credenziali utente seguono un caratteristico ciclo di vita, che in linea di massima è distinto dai seguenti momenti:

- creazione: gli amministratori di sistema creano una nuova user-id ed assegnano una password per il primo logon del nuovo utente al sistema;
- modifica: variazione apportata all'utenza o alla password;
- sospensione: è realizzata dagli amministratori e comporta l'impossibilità dell'utente ad operare con le proprie credenziali;
- cancellazione: rimozione dell'user-id (e del profilo corrispondente) dalla lista degli utenti autorizzati ad accedere a un certo insieme di risorse.

Ciascuna di queste fasi deve essere opportunamente definita nell'istruzione operativa relativa alla amministrazione delle utenze.

Ai fini della sicurezza riveste particolare importanza la gestione della parola chiave ed il controllo sulla corretta valorizzazione ed uso della parola chiave stessa da parte di utenti finali e degli amministratori. In particolare gli amministratori, in quanto dotati di privilegi particolari, sono soggetti a regole di gestione più restrittive rispetto agli utenti.

4.2 Criteri generali

4.2.1 Creazione e gestione dell'account

Definizione dell'utenza

Ad ogni utente di dati e risorse informatiche (interno o esterno) deve essere assegnato un codice identificativo (user-id) unico. L'utenza deve essere profilata seguendo le indicazioni di questo documento.

L'Ufficio Personale è responsabile di richiedere a chi si occupa di security la creazione delle utenze e l'assegnazione di una macchina (PC, laptop) al personale. Sempre l'IT è responsabile della creazione degli account sugli applicativi di propria pertinenza o che ha in gestione.

L'account deve essere fornito a personale esterno solo in presenza di una specifica ed effettiva necessità di lavorare e con il minimo privilegio necessario per svolgere la mansione.

Revoca, cancellazione o modifica dell'utenza

Quando una persona lascia l'organico o non ha più la necessità di accedere ai sistemi informativi del titolare, il suo account deve essere immediatamente disabilitato.

In particolare, l'Ufficio Personale è responsabile di comunicare all'ufficio Security l'uscita di un dipendente/collaboratore, cosa che comporterà la revoca immediata e/o la cancellazione delle utenze dell'utente stesso; sempre l'ufficio del personale dovrà avvisare tempestivamente l'ufficio Security, nel caso in cui alcuni utenti dovessero cambiare ruolo al interno della struttura, in modo da far modificare prontamente il profilo di tali utenti ed adattarli alle nuove necessità operative.

Revisione delle utenze

Devono essere revocate le utenze non più in uso da 6 mesi. E' necessario effettuare un controllo almeno annuale di tali utenze.

4.2.2 Credenziali (UTENZA E PASSORD)

L'utenza è strettamente personale e non cedibile.

Per quanto concerne la definizione delle password, si ricorda che la Password è strettamente personale, ed al fine di proteggerne la segretezza, è necessario attenersi alle seguenti norme:

- deve essere custodita da parte del dipendente con la massima cura;
- non deve essere comunicata ad altri;
- non deve essere scritta su supporti facilmente accessibili (post-it, blocco appunti, ecc.). Nel caso si voglia mantenerne traccia scritta, per propria memoria, essa deve essere conservata in luogo sicuro;
- deve essere cambiata di frequente ed essere definita secondo le regole descritte di seguito

4.2.3 Nuova assegnazione di parole chiave (PASSWORD)

La parola chiave viene nuovamente assegnata dall'IT nei seguenti casi:

- quando l'utenza è stata sospesa per aver superato il numero massimo di tentativi di accesso falliti inserendo una parola chiave non corretta;
- quando l'utenza è stata sospesa, decorso il periodo massimo consentito di non utilizzo;
- quando il soggetto dimentica la parola chiave;
- perdita di confidenzialità, qualora l'utente non possa modificarla autonomamente.

In tutti questi casi, l'evento di riattivazione dell'utenza e la fonte della richiesta devono essere tracciati.

4.2.4 Sospensione delle credenziali

La sospensione consiste nel blocco delle funzionalità associate all'utenza, in modo che non sia possibile avvalersene per operare sulle risorse informatiche.

- Durante il periodo di sospensione, non devono avvenire attività anomale sull'utenza disabilitata (ad es. una sua temporanea riabilitazione) se non preventivamente autorizzate. La sospensione (senza revoca) deve essere tempestivamente attivata dagli amministratori in caso di investigazioni a carico del dipendente.

Al cessare dell'evento che ha causato la sospensione, gli amministratori ripristinano l'utenza, previa autorizzazione del responsabile dell'utente.
Eventuali problematiche particolari connesse all'utenza (ad es. legate alle chiavi di cifratura) devono essere valutate e gestite con il supporto dell'IT.

4.2.5 Revoca delle credenziali

La revoca delle credenziali consiste nella cancellazione dell'utenza, nei casi previsti, per impedirne successivi utilizzi non autorizzati.

La revoca delle credenziali avviene *immediatamente* nei seguenti casi:

- quando il dipendente lascia l'azienda;
- quando personale esterno a cui sia stata concessa un'utenza lascia l'Azienda (interinali, stagisti, consulenti…).

Tali eventi devono necessariamente essere tutti tracciati.

4.2.6 Revisione utenze

Gli Amministratori verificano periodicamente (ad es. con un controllo annuale) l'effettiva correttezza degli accessi consentiti agli utenti.

La finalità di tale attività è eliminare gli account appartenenti a persone che hanno lasciato l'azienda o che hanno cambiato sede/mansione, per cui non hanno più ragione di essere mantenuti, in modo da evitare che possano essere sfruttati per attività non autorizzate.

Dietro segnalazione dell'Ufficio del Personale o periodicamente (indicativamente mensilmente) gli amministratori devono altresì provvedere a:

- controllare l'intero set delle utenze e disabilitare le eventuali utenze non utilizzate da oltre 90gg;
- cancellare dopo altri 60 gg le utenze disabilitate.

4.3 Regole di sicurezza per la gestione delle credenziali amministrative

4.3.1 User-Id

Gli amministratori (di sistema o di applicativo) devono essere dotati di due utenze, una con privilegi amministrativi e una con privilegi utente.

Le utenze amministrative devono essere utilizzate *solo per svolgere le attività di amministratore del sistema* (creazione, sospensione, cancellazione di utenti, modifica di privilegi, sblocco o reset della parola chiave, modifiche alle librerie di sistema, ecc…).

Per tutte le altre attività, gli amministratori devono possedere e avvalersi di un'utenza non privilegiata.

4.3.2 Assegnazione delle credenziali amministrative

Le credenziali per l'accesso come amministratore ai Sistemi Informatici sono assegnate da Responsabile IT ai dipendenti che ricoprono tale incarico specifico.

Le assegnazioni di utenze privilegiate ad esterni hanno carattere eccezionale e devono essere giustificate ed autorizzate dalla Direzione Generale.

L'utenza amministrativa è comunicata all'interessato insieme alla parola chiave, che deve essere "robusta"- vedi par. 4.4.3).

4.3.3 Parole chiave per amministratori

Per la gestione della parola chiave degli amministratori, i sevizi interessati devono definite regole univoche e il più possibile omogenee per tutti i sistemi o applicativi di pertinenza, e modalità di governo differenziate per gli utenti e per gli amministratori.

Le regole adottate devono essere tese a realizzare il più alto livello possibile di sicurezza, e possono prevedere anche l'utilizzo di tool o procedure sviluppate *ad hoc*.

Di seguito si riportano le regole di sicurezza sulle parole chiave per gli amministratori, che rafforzano i criteri generali espressi in precedenza. Esse vanno applicate sui vari sistemi di controllo degli accessi (compatibilmente con le possibilità tecniche dei sistemi stessi) e si applicano anche agli apparati di rete:

- nella costruzione della parola chiave, questa:
  - deve essere lunga più di 8 caratteri alfanumerici, compreso l'uso di minuscole e maiuscole, e deve contenere almeno una lettera ed almeno una cifra;
  - dove possibile, deve essere previsto anche l'uso di caratteri speciali;

- il cambio della parola chiave amministrativa deve avvenire ogni 60 giorni (possibilmente con avvertimento automatizzato);
- il sistema non deve permettere il reset lockout, ovvero di azzerare il numero di tentativi di logon falliti per parola chiave errata, dopo un periodo predefinito;
- dopo 60 giorni di inattività l'utenza amministrativa viene sospesa e la parola chiave ad essa associata non è più valida; l'utenza sospesa può essere riattivata solo da un altro amministratore;
- il sistema deve dare notizia della data e ora dell'ultima connessione dell'utenza amministrativa;
- devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Devono inoltre essere previste regole particolari per la gestione delle utenze di root e per il loro utilizzo in caso di emergenza.

4.4 Controlli

Devono essere previsti strumenti e metodi formali di verifica delle credenziali.

I database delle password devono essere soggetti a verifiche *a posteriori* (audit) per accertarsi che le parole chiave siano conformi alle regole.

I tools hanno come obiettivo quello di garantire la corretta applicazione delle regole di sicurezza. Data la rilevanza di una corretta realizzazione delle regole emanate, è necessario effettuare un monitoraggio delle stesse, sia in termini di grado di conformità, sia in termini di violazioni.

Ciò consente anche di effettuare degli aggiustamenti su quelle regole che vengono violate con regolarità.