Istituto Comprensivo Statale "Falcomatà-Archi"
PLESSI SEC. I GRADO: Ibico/Pirandello - Klearchos – PRIMARIA: S. Caterina - S. Brunello - Archi Cep - INFANZIA: S. Caterina - Archi Centro
Via Montello n.7 – S. Caterina, **Tel 0965 48679**
e-mail: rcic80500x@istruzione.it - pec: rcic80500x@pec. istruzione.it - Sito web: **http://www.icfalcomatarchi.edu.it/**
C.F: 92081760800 - C.M.: RCIC80500X

ISTRUZIONI PER LA SELEZIONE E LA GESTIONE SICURA DI PAROLE CHIAVE

Sommario

1 Premessa

La normativa vigente riguardante la protezione dei dati personali impone al titolare ed al responsabile di adottare tutte le misure necessarie a tale scopo. Tra queste risulta indispensabile impartire precise istruzioni agli incaricati, che utilizzano una parola chiave (*password*) come strumento complementare di autenticazione, in aggiunta al codice identificativo personale (*nome utente*).

Poiché la gestione della parola chiave rappresenta oggi uno degli aspetti più delicati dell'intera politica di sicurezza di accesso logico ai sistemi informativi, è indispensabile che gli incaricati prendano nota di quanto qui indicato e che si attengano strettamente a queste raccomandazioni.

L'incaricato deve rendersi conto che la parola chiave rappresenta la prima barriera in una strategia di accesso selettivo a dati personali, e pertanto una parola chiave selezionata con criteri non soddisfacenti può portare alla compromissione dell'intera rete informativa Istituzionale.

Per questa ragione tutti gli incaricati, ai quali viene attribuito un profilo di autorizzazione e devono operare nell'ambito di un sistema di autenticazione, sono responsabili di prendere tutte le iniziative appropriate per garantire la sicurezza delle parole chiave.

Nel caso l'incaricato abbia qualsiasi dubbio circa le modalità sicure di generazione, utilizzo e conservazione delle parole chiave, deve rivolgersi al proprio titolare o responsabile, per ottenere opportuni chiarimenti ed istruzioni.

2 Obiettivo delle presenti istruzioni

L'obiettivo di queste istruzioni è di stabilire uno standard soddisfacente di sicurezza per creare parole chiave sicure, per proteggere queste parole chiave e per indicare la frequenza della modifica.

2.1 Destinatari

Destinatari di questo documento sono tutti gli incaricati, interni ed esterni all'Istituto, ai quali è stato attribuito una Profilo di autorizzazione, che può essere attivato solo grazie un sistema di autenticazione, basato su una parola chiave. Questo documento si applica in fase di utilizzo di qualsiasi sistema informativo, che si trovi all'interno della rete Istituzionale, collegato o meno a tale rete, o che custodisce qualsiasi dato personale di competenza dell'Istituto e non destinato alla diffusione.

3 Linee guida

3.1 Generalità

Tutte le parole chiave a livello di sistema, come ad esempio quelle dell'amministratore di un sistema operativo Windows e simili, devono essere cambiate con una frequenza più elevata, rispetto a quella attribuita a parole chiave conferite ad utenti con profilo di accesso di minore rischio 3/6 MESI
Tutte le parole chiave utilizzate a livello di sistema devono essere inserite nel database globale di gestione delle parole chiave.
Tutte le parole chiave attribuite ai singoli incaricati per accedere alla posta elettronica, al proprio computer, ad Internet, eccetera, devono essere cambiate almeno ogni sei mesi. Quest'intervallo di tempo deve essere ridotto a tre mesi, se queste parole chiave vengono utilizzate per accedere a dati personali sensibili.
Si raccomanda comunque vivamente di ridurre al massimo questo intervallo di tempo, perché più esso è breve, minori sono le probabilità che la parola chiave venga in qualche modo scoperta e compromessa.
È fatto assoluto divieto di inserire parole chiave in messaggi di posta elettronica oppure in finestre di dialogo in sessioni Internet od altre forme di comunicazione elettronica.

3.2 Linee guida per la costruzione delle parole chiave

Le parole chiave possono essere utilizzate per accedere a differenti profili di autorizzazione, nell'ambito del sistema informativo Istituzionale.
Gli utilizzi più frequenti sono ad esempio: contabilità di utente, accesso ad Internet, accesso a sistemi di posta elettronica, accesso a screen saver, accesso a sistemi locali.
Poiché sono molto rari i sistemi informativi che possono utilizzare parole chiave dinamiche, che vengono usate una volta sola, è indispensabile che ogni incaricato prenda nota delle modalità con cui è possibile adottare parole chiave di difficile individuazione.

3.2.1 Parole chiave deboli

Le parole chiave di facile individuazione (*parole chiave deboli*) hanno le seguenti caratteristiche:

- La parola chiave contiene meno di 8 caratteri, anche se il sistema può accettare parole chiave di 8 caratteri ed oltre
- La parola chiave si può trovare in una comune dizionario italiano, in inglese od altra lingua comune
- La parola chiave è una parola di uso comune, come ad esempio il nome di qualche membro della famiglia, di animali da salotto, di amici, di collaboratori o di caratteri di fantasia
- Sono da ritenere insoddisfacenti anche parole chiave legate a espressioni informatiche, hardware e software, come pure quelle legate a date di nascita od altre informazioni personali, come l'indirizzo, il numero telefonico e simili
- Sono inoltre da scartare parole o sequenze numeriche del tipo aaaaaaaa, bbbb, 121212, 123456, eccetera. Sono da scartare parole come sopra, digitate alla rovescia
- E' da scartare una qualsiasi delle parole chiave precedentemente indicata come debole, preceduta o seguita da una cifra come ad esempio giovanni1, oppure 1giovanni.

3.2.2 Parole chiave sicure

Per contro, sono da ritenere parole chiave di soddisfacente sicurezza quelle che hanno le seguenti caratteristiche:

- Sono composte da caratteri maiuscoli e minuscoli
- Utilizzano anche caratteri di interpunzione, come; [,] , * " , ed una combinazione di numeri e lettere
- Devono avere una lunghezza minima di 8 caratteri alfanumerici, se il sistema consente di raggiungere questa lunghezza
- Non devono rappresentare una parola in una qualsiasi lingua o dialetto sufficientemente diffuso
- Non devono essere basate su informazioni personali, come nomi di membri della famiglia e simili
- Un altro importante accorgimento riguarda la selezione di parole chiave, che possano essere facilmente digitate sulla tastiera, senza doverla guardare, per ridurre al minimo il tempo di digitazione ed evitare che la digitazione possa essere osservata da terzi nelle vicinanze.

Le parole sicure non devono mai essere scritte o archiviate in linea.

Ecco qualche indicazione per creare delle parole chiave sicure ma facili da ricordare:
- Un primo suggerimento è quello di creare una parola chiave basata sul titolo di una canzone o su un'altra frase, debitamente sintetizzata - ad esempio "tea for two" diventa "teax2"
- La parola chiave può essere formata abbreviando una intera frase come ad esempio "che gelida manina" diventa "chegemani"

Attenzione: non usare mai alcuna degli esempi sopra illustrati come parola chiave.

3.3 Raccomandazione per la protezione della parola chiave

Non utilizzare la stessa parola chiave per sistemi di autenticazione interni all'Istituto e per sistemi di autenticazione esterni, come ad esempio l'accesso al proprio conto corrente bancario ed altre attività, non legate all'attività Istituzionale.
Ove ad un incaricato vengano attribuiti diversi profili di autorizzazione, non deve essere usata la stessa parola chiave in relazione a differenti profili (ad esempio, deve essere scelta una parola chiave per l'accesso all'area tecnica del sistema, una per l'accesso all'area sanitaria ed una parola chiave separata per l'accesso alla contabilità).
La parola chiave prescelta non deve essere condivisa con alcun soggetto, interno o esterno all'Istituto, ivi inclusi i superiori, a qualsiasi livello.
Tutte le parole chiave che sono state generate da un incaricato devono essere trattate come informazione strettamente riservata.
In particolare, ecco un elenco delle cose che non bisogna fare:

- Non rivelate una parola chiave attraverso il telefono a chicchessia
- Non scrivete una parola chiave in un messaggio di posta elettronica
- Non rivelate la parola chiave al vostro superiore
- Non parlate di parole chiave di fronte a terzi
- Non date alcune indicazioni in merito al formato ed alla lunghezza della parola chiave che utilizzate
- Non svelate la parola chiave su questionari o su formulari di sicurezza
- Non rivelate la parola chiave a membri della famiglia
- Non rivelate la parola chiave ad un vostro collega di lavoro.

Se qualcuno insiste per conoscere la vostra parola chiave, dapprima fate riferimento a questo documento e successivamente informate immediatamente il responsabile della sicurezza logica (*responsabile dei sistemi informativi*) oppure il titolare del trattamento dei dati oppure un responsabile del trattamento dei dati.

Non utilizzare mai la caratteristica, offerta da parecchie applicazioni, di ricordare la parola chiave.
Non scrivete la parola chiave su un qualsiasi documento e non nascondetelo in alcuna parte del vostro ufficio.
Non archiviate la parola chiave in un qualsiasi tipo di sistema di elaborazione, incluso un telefono cellulare, un computer palmare e simile, senza utilizzare un algoritmo di cifratura (*la protezione crittografica o cifratura consiste nella trasformazione di un file informatico, grazie ad una chiave, in modo tale che il testo sia incomprensibile*).
Ricordatevi di cambiare la parola chiave almeno una volta ogni sei mesi; quest'intervallo viene ridotto a tre mesi nei casi in cui la parola chiave consenta l'accesso al trattamento di dati sensibili.
Se avete anche solo il minimo sospetto che la vostra parola chiave sia stata in qualche modo compromessa o venuta a conoscenza di terzi, provvedete immediatamente alla sostituzione della parola chiave e riferite l'accaduto al responsabile della sicurezza logica, oppure al titolare od al responsabile del trattamento di dati personali.

Si faccia attenzione che, nell'ambito delle misure di controllo del livello di sicurezza del sistema informativo, è possibile che il responsabile della sicurezza logica effettui tentativi di violazione della vostra parola chiave. Nel caso il tentativo abbia esito positivo, vi verrà chiesto di sostituire immediatamente la parola chiave.

3.4 Frasi chiave

Le frasi chiave possono essere utilizzate per l'autenticazione remota di un utente, utilizzando algoritmi con chiave pubblica e privata.
Un sistema con chiave pubblica e privata definisce una relazione matematica tra la chiave pubblica, nota a tutti, e la chiave privata, che conosciuta soltanto all'utente.
Senza la parola frase che permette di decifrare la chiave privata, l'utente non può ottenere l'accesso al sistema.
Questa architettura di sicurezza è spesso usata in Italia nella gestione di applicativi di firma digitale (es. *registrazioni di utenti di posta elettronica presso provider*).
Le frasi chiave non sono la stessa cosa delle parole chiave.
Una frase chiave è una versione più lunga di una parola chiave e quindi più sicura.
Una frase chiave è tipicamente composta da molte parole ed è questa la ragione per cui essa più sicura contro i cosiddetti "attacchi del dizionario".
Una frase chiave sicura è relativamente lunga e contiene una combinazione di lettere maiuscole e minuscole, nonché numeri e segni di interpunzione. Ecco un esempio di una soddisfacente frase chiave:
"la mattinA e' BELLA"
Tutte le regole prima illustrate, che si applicano alla selezione delle parole chiave, si applicano anche alle frasi chiave.

3.5 Disattivazione del profilo di autenticazione

Nel caso l'incaricato non utilizzi il proprio codice identificativo personale e parola chiave per un periodo superiore a sei mesi il suo profilo di autenticazione viene disattivato. Per riprendere la operatività, l'incaricato deve prendere contatto con il titolare o responsabile del trattamento di dati personali. **In nessun caso un codice identificativo personale (*username* / *userid*) non più utilizzato può essere assegnato ad un altro incaricato.**

3.6 Disattivazione del profilo di autorizzazione

Per esplicita prescrizione di legge, il profilo di autorizzazione concesso ad un incaricato deve essere verificato almeno una volta l'anno.
È possibile che l'incaricato, pure debitamente autenticato, si trovi impossibilitato ad utilizzare il proprio profilo di autorizzazione per scadenza dello stesso e mancato rinnovo.
Per riprendere la operatività, l'incaricato deve prendere contatto con il titolare od il responsabile del trattamento di dati personali che attiva i necessari provvedimenti di ripristino dell'operatività.

4 Interventi di emergenza

Per misure di sicurezza si prevede esplicitamente che sia possibile, per il titolare od il responsabile del trattamento di dati personali, di accedere alla parola chiave di un incaricato, ove per una qualunque ragione egli non sia presente sul posto di lavoro e sorga una urgente esigenza di accedere a dati personali, che sono accessibili soltanto con il suo profilo di autorizzazione.
Giova sottolineare che, ove il profilo di autorizzazione sia condiviso con altri soggetti, la procedura di emergenza non ha ragione di essere utilizzata, in quanto agli stessi dati si può accedere grazie ad un altro incaricato, che utilizza la propria parola chiave.
Nel caso il profilo di autorizzazione rientri nella categoria sopraripportata (*profilo di autorizzazione non condiviso con altri incaricati*), è fatto obbligo all'incaricato di trascrivere la propria parola chiave su un foglio di carta, che deve essere inserito in una busta debitamente sigillata e controfirmata, meglio se chiusa con sigilli inviolabili a numerazione univoca.
Tale busta deve essere consegnata al custode delle password se nominato od al Titolare del trattamento e il suo contenuto deve essere costantemente aggiornato, ogniqualvolta l'incaricato decide di sostituire la propria parola chiave.
È facoltà del titolare, in presenza dell'incaricato, aprire la busta sigillata e verificare che la parola chiave presente sul foglio di carta corrisponde a quella effettivamente in uso.

È fatto obbligo al titolare del trattamento di verbalizzare in apposito registro, con controfirma di garanzia da parte di terzi, la avvenuta apertura della busta e la presa di conoscenza della parola chiave.
Resta inteso che dal momento in cui il titolare od il responsabile hanno preso conoscenza della parola chiave, all'incaricato che l'ha selezionata non compete più alcuna ulteriore responsabilità in merito a trattamenti non autorizzati od accessi non consentiti ai dati personali, di cui al suo profilo di autorizzazione.

La sua responsabilità verrà pienamente rimessa in essere, non appena l'incaricato avrà avuto la possibilità di selezionare una nuova parola chiave ed assumersene quindi la piena responsabilità del suo corretto utilizzo. In tale occasione ci si rammenti di inserire la nuova parola chiave della busta sigillata, come precedentemente illustrato.

5 Sanzioni

Un incaricato che abbia violato queste linee guida di sicurezza potrebbe essere sottoposto ad azioni disciplinari di vario livello per i possibili riflessi che la sua negligenza potrebbe avere avuto sulla sicurezza del sistema informativo Istituzionale e su provvedimenti sanzionatori amministrativi – penali intrapresi a carico dell'organizzazione.