Comune di Ischia
Provincia di Napoli

alphasoft
TECNOLOGIE PER L'INFORMATICA

Manuale di Gestione Documentale
(art. 5 DPCM 3/12/2013)
Istruzioni operative
Politiche di Sicurezza

Cod. **MANGEDOC** Rev. **1.0** Data: 09-10-2015

Sommario: In questo allegato sono riportate le Politiche di sicurezza adottate dall'Ente a cui debbono attenersi responsabili ed incaricati ai trattamenti dei documenti.

REVISIONI

Rev.	Data	Redattore/i	Descrizione
1.0	09/10/2015	Maria Pia Papa	

INDICE

1 PREMESSA

La gestione documentale è un'attività trasversale a tutte le unità organizzative dell'Ente e, pertanto, tutto il personale (impiegati, funzionari e dirigenti) dell'Amministrazione è tenuto, in uno sforzo di squadra, a comportarsi in accordo con le politiche di sicurezza che vengono impartite in questo capitolo. È responsabilità di tutti gli utilizzatori del sistema informatico conoscere queste linee guida e comportarsi in accordo con le medesime.

L'incarico del Responsabile della Sicurezza (RS), o suo delegato, di pubblicare le politiche accettabili di uso, è quello di stabilire le regole per proteggere l'Amministrazione da azioni illegali o danneggiamenti effettuati da individui in modo consapevole o accidentale senza imporre restrizioni contrarie a quanto stabilito dall'Amministrazione in termini di apertura, fiducia e integrità del sistema informativo.

Sono di proprietà dell'Amministrazione i sistemi di accesso ad Internet, l'Intranet, la Extranet ed i sistemi correlati, includendo in ciò anche i sistemi di elaborazione, la rete e gli apparati di rete, il software applicativo, i sistemi operativi, i sistemi di memorizzazione/archiviazione delle informazioni, il servizio di posta elettronica, i sistemi di accesso e navigazione in Internet, etc. Questi sistemi e/o servizi devono essere usati nel corso delle normali attività di ufficio solo per scopi istituzionali e nell'interesse dell'Amministrazione e in rapporto con possibili interlocutori della medesima.

2 SCOPO

Lo scopo di queste politiche è sottolineare l'uso accettabile del sistema informatico dell'Amministrazione.

Le regole sono illustrate per proteggere gli impiegati e l'Amministrazione.

L'uso non appropriato delle risorse strumentali espone l'Amministrazione al rischio di non poter svolgere i compiti istituzionali assegnati, a seguito, ad esempio, di virus, della compromissione di componenti del sistema informatico, ovvero di eventi disastrosi.

3 AMBITO DI APPLICAZIONE

Queste politiche si applicano a tutti gli impiegati dell'Amministrazione, al personale esterno (consulenti, personale a tempo determinato, …) che collabora con l'amministrazione e al personale dipendente di ditte che sono autorizzate all'accesso al sistema informativo dell'Ente.

Esse si applicano a tutti gli apparati che sono di proprietà dell'Amministrazione o "affittate" da questa.

4 POLITICHE – USO GENERALE E PROPRIETA'

Gli utenti del sistema informativo dovrebbero essere consapevoli che i dati da loro creati sui sistemi dell'Amministrazione e comunque trattati, rimangono di proprietà della medesima.

Gli impiegati sono responsabili dell'uso corretto delle postazioni di lavoro assegnate e dei dati ivi conservati anche perché la gestione della rete (Intranet) non può garantire la confidenzialità dell'informazione memorizzata su ciascun componente "personale" della

rete dato che l'amministratore della rete ha solo il compito di fornire prestazioni elevate e un ragionevole livello di confidenzialità e integrità dei dati in transito.

Gli impiegati devono attenersi alle linee guida per l'uso personale di Internet/Intranet/Extranet.

Per garantire la manutenzione della sicurezza e della rete, soggetti autorizzati dall'Amministrazione (di norma amministratori di rete) possono monitorare gli apparati, i sistemi ed il traffico in rete in ogni momento.

Per i motivi di cui sopra l'Amministrazione si riserva il diritto di controllare la rete ed i sistemi per un determinato periodo per assicurare la conformità con queste politiche.

5 POLITICHE – SICUREZZA E PROPRIETA' DELL'INFORMAZIONE

Il personale dell'Amministrazione dovrebbe porre particolare attenzione in tutti i momenti in cui ha luogo un trattamento delle informazioni per prevenire accessi non autorizzati alle informazioni.

Mantenere le credenziali di accesso (normalmente UserID e password) in modo sicuro e non condividerle con nessuno. Gli utenti autorizzati ad utilizzare il sistema informativo sono responsabili dell'uso delle proprie credenziali, componente pubblica (UserID) e privata (password). Le password dovrebbero essere cambiate con il primo accesso al sistema informativo e successivamente, al minimo ogni quattro mesi, ad eccezione di coloro che trattano dati personali sensibili o giudiziari per i quali il periodo si riduce a tre mesi.

Tutte le postazioni di lavoro (PC da tavolo e portatili) dovrebbero essere rese inaccessibili a terzi quando non utilizzate dai titolari per un periodo massimo di dieci minuti attraverso l'attivazione automatica del salva schermo protetto da password o la messa in stand-by con un comando specifico.

Uso delle tecniche e della modalità di cifratura dei file coerentemente a quanto descritto in materia di confidenzialità dall'Amministrazione.

Poiché le informazioni archiviate nei PC portatili sono particolarmente vulnerabili su essi dovrebbero essere esercitate particolari attenzioni.

Eventuali attività di scambio di opinioni del personale dell'Amministrazione all'interno di "news group" che utilizzano il sistema di posta elettronica dell'Amministrazione dovrebbero contenere una dichiarazione che affermi che le opinioni sono strettamente personali e non dell'Amministrazione a meno che non si tratti di discussioni inerenti e di interesse dell'Amministrazione eseguite per conto della medesima.

Tutti i PC, i server ed i sistemi di elaborazione in genere, che sono connessi in rete interna dell'Amministrazione (Intranet) e/o esterna (Internet/Extranet) di proprietà dell'Amministrazione o del personale, devono essere dotati di un sistema antivirus approvato dal responsabile della sicurezza dell'Amministrazione ed aggiornato.

Il personale deve usare la massima attenzione nell'apertura dei file allegati alla posta elettronica ricevuta da sconosciuti perché possono contenere virus, bombe logiche e cavalli di Troia.

Non permettete ai colleghi, né tanto meno ad esterni, di operare sulla vostra postazione di lavoro con le vostre credenziali. Sempre voi risultate autori di qualunque azione.

L'Amministrazione adotta specifiche istruzioni operative per la selezione e gestione sicura delle parole chiave.

6 POLITICHE - ANTIVIRUS

6.1 Generalità

I virus informatici costituiscono ancora oggi la causa principale di disservizio e di danno delle Amministrazioni.

I danni causati dai virus all'Amministrazione, di tipo diretto o indiretto, tangibili o intangibili, secondo le ultime statistiche degli incidenti informatici, sono i più alti rispetto ai danni di ogni altra minaccia.

I virus, come noto, riproducendosi autonomamente, possono generare altri messaggi contagiati, capaci di infettare, contro la volontà del mittente, altri sistemi con conseguenze negative per il mittente in termini di criminalità informatica e tutela dei dati personali.

E' importante stabilire i requisiti che devono essere soddisfatti per collegare le risorse elaborative ad Internet/Intranet/Extranet dell'Amministrazione al fine di assicurare efficaci ed efficienti azioni preventive e consuntive contro i virus informatici.

Queste politiche riguardano tutte le apparecchiature di rete, di sistema ed utente (PC) collegate ad Internet/Intranet/Extranet.

Tutto il personale dell'Amministrazione è tenuto a rispettare le politiche di seguito richiamate.

6.2 Politiche per le azioni preventive

1. Deve essere sempre attivo su ciascuna postazione di lavoro un prodotto antivirus aggiornabile da un sito disponibile sulla Intranet dell'Amministrazione.
2. Su ciascuna postazione deve essere sempre attiva la versione corrente e aggiornata con la più recente versione resa disponibile sul sito centralizzato.
3. Non aprire mai file o macro ricevuti con messaggi dal mittente sconosciuto, sospetto, ovvero palesemente non di fiducia. Cancellare immediatamente tali oggetti sia dalla posta che dal cestino.
4. Non aprire mai messaggi ricevuti in risposta a messaggi "probabilmente" mai inviati.
5. Cancellare immediatamente ogni messaggio che invita a continuare la catena di messaggi, o messaggi spazzatura.
6. Non scaricare mai messaggi da siti o sorgenti sospette.
7. Evitate lo scambio diretto ed il riuso di supporti rimovibili (floppy disk, CD, DVD, tape, pen drive, etc.) con accesso in lettura e scrittura a meno che non sia espressamente formulato in alcune procedure dell'amministrazione e, anche in questo caso, verificare prima la bontà del supporto con un antivirus.
8. Evitare l'uso di software gratuito (freeware o shareware) o documenti di testo prelevati da siti Internet o copiato dai CD/DVD in allegato a riviste.
9. Evitare l'utilizzo, non controllato, di uno stesso computer da parte di più persone.
10. Evitare collegamenti diretti ad Internet via modem.
11. Non utilizzare il proprio supporto di archiviazione rimovibile su di un altro computer se non in condizione di protezione in scrittura.

12. Se si utilizza una postazione di lavoro che necessita di un "bootstrap" da supporti di archiviazione rimovibili, usare questo protetto in scrittura.
13. Non utilizzare i server di rete come stazioni di lavoro.
14. Non aggiungere mai dati o file ai supporti di archiviazione rimovibili contenenti programmi originali.
15. Effettuare una scansione della postazione di lavoro con l'antivirus prima di ricollegarla, per qualsiasi motivo (es, riparazione, prestito a colleghi o impiego esterno), alla Intranet dell'Organizzazione.

Di seguito vengono riportati ulteriori criteri da seguire per ridurre al minimo la possibilità di contrarre virus informatici e di prevenirne la diffusione, destinati a tutto il personale dell'Amministrazione ed, eventualmente, all'esterno:

1. Tutti gli incaricati del trattamento dei dati devono assicurarsi che i computer di soggetti terzi, esterni, qualora interagiscano con il sistema informatico dell'Amministrazione, siano dotati di adeguate misure di protezione antivirus.
2. Il personale delle ditte addette alla manutenzione dei supporti informatici deve usare solo supporti rimovibili preventivamente controllati e certificati singolarmente ogni volta.
3. I supporti di archiviazione rimovibili provenienti dall'esterno devono essere sottoposti a verifica da attuare con una postazione di lavoro dedicata, non collegata in rete (macchina da quarantena).
4. Il personale deve essere a conoscenza che la creazione e la diffusione, anche accidentale dei virus è punita dall'Articolo 615 quinquies del Codice penale concernente la "Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico… [omissis]…che prevede la reclusione sino a due anni e la multa sino a lire venti milioni".
5. Il software acquisito deve essere sempre controllato contro i virus e verificato perché sia di uso sicuro prima che sia installato.
6. È proibito l'uso di qualsiasi software diverso da quello fornito dall'Amministrazione.
7. In questo ambito, al fine di minimizzare i rischi di distruzione anche accidentale dei dati a causa dei virus informatici, il RSP stabilisce le protezioni software da adottare sulla base dell'evoluzione delle tecnologie disponibili sul mercato.

6.3 Politiche per le azioni consuntive

Nel caso in cui su una o più postazioni di lavoro dovesse verificarsi perdita di informazioni, integrità o confidenzialità delle stesse a causa di infezione o contagio da virus informatici, il titolare della postazione interessata deve immediatamente isolare il sistema e poi notificare l'evento al responsabile della sicurezza, o suo delegato, che deve procedere a:

1. verificare se ci sono altri sistemi infettati con lo stesso Virus Informatico;
2. verificare se il virus ha diffuso dati;
3. identificare il virus;
4. attivare l'antivirus adatto ad eliminare il virus rilevato e bonificare il sistema infetto;
5. installare l'Antivirus adatto su tutti gli altri sistemi che ne sono sprovvisti;
6. diffondere la notizia dell'evento, all'interno dell'Amministrazione, nelle forme opportune.

7 POLITICHE – USO NON ACCETTABILE

7.1 Generalità

Le seguenti attività sono in generale proibite. Il personale può essere esentato da queste restrizioni in funzione del ruolo ricoperto all'interno dell'Amministrazione (ad esempio, nessuno può disconnettere e/o disabilitare le risorse ad eccezione degli amministratori di sistema o di rete).

In nessun caso o circostanza il personale è autorizzato a compiere attività illegali utilizzando le risorse di proprietà dell'Amministrazione.

L'elenco seguente non vuole essere una lista esaustiva, ma un tentativo di fornire una struttura di riferimento per identificare attività illecite o comunque non accettabili.

7.2 Attività di rete e di sistema

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione:

1. Violazioni dei diritti di proprietà intellettuale di persone o società, o diritti analoghi includendo, ma non limitando, l'installazione o la distribuzione di copie pirata o altri software prodotti che non sono espressamente licenziati per essere usati dall'Amministrazione.
2. Copie non autorizzate di materiale protetto da copyright (diritto d'autore) includendo, ma non limitando, digitalizzazione e distribuzione di foto e immagini di riviste, libri, musica e ogni altro software tutelato per il quale l'Amministrazione o l'utente finale non ha una licenza attiva.
3. È rigorosamente proibita l'esportazione di software, informazioni tecniche, tecnologia o software di cifratura, in violazione delle leggi nazionali ed internazionali.
4. Introduzione di programmi maliziosi nella rete o nei sistemi dell'Amministrazione.
5. Rivelazione delle credenziali personali ad altri o permettere ad altri l'uso delle credenziali personali, includendo in ciò i familiari o altri membri della famiglia quando il lavoro d'ufficio è fatto da casa o a casa.
6. Usare un sistema dell'Amministrazione (PC o server) per acquisire o trasmettere materiale pedo-pornografico o che offende la morale o che è ostile alle leggi e regolamenti locali, nazionali o internazionali.
7. Effettuare offerte fraudolente di prodotti, articoli o servizi originati da sistemi dell'Amministrazione con l'aggravante dell'uso di credenziali fornite dall'Amministrazione stessa.
8. Effettuare affermazioni di garanzie, implicite o esplicite, a favore di terzi ad eccezione di quelle stabilite nell'ambito dei compiti assegnati.
9. Realizzare brecce nelle difese periferiche della rete del sistema informativo dell'Amministrazione o distruzione della rete medesima, dove per brecce della sicurezza si intendono, in modo riduttivo:
    a. accessi illeciti ai dati per i quali non si è ricevuta regolare autorizzazione,
    b. attività di "sniffing";
    c. disturbo della trasmissione;
    d. spoofing dei pacchetti;
    e. negazione del servizio;

f. le modifiche delle mappe di instradamento dei pacchetti per scopi illeciti;
g. attività di scansione delle porte o del sistema di sicurezza è espressamente proibito salvo deroghe specifiche.

10. Eseguire qualsiasi forma di monitor di rete per intercettare i dati in transito.
11. Aggirare il sistema di autenticazione o di sicurezza della rete, dei server e delle applicazioni.
12. Interferire o negare l'accesso ai servizi di ogni altro utente abilitato.
13. Usare o scrivere qualunque programma o comando o messaggio che possa interferire o con i servizi dell'Amministrazione o disabilitare sessioni di lavoro avviate da altri utenti di Internet/Intranet/Extranet.
14. Fornire informazioni o liste di impiegati a terze parti esterne all'Amministrazione.

7.3 Attività di messaggistica e comunicazione

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

1. Inviare messaggi di posta elettronica non sollecitati, includendo "messaggi spazzatura", o altro materiale di avviso a persone che non hanno specificamente richiesto tale materiale (spamming).
2. Ogni forma di molestia via e-mail o telefonica o con altri mezzi, linguaggio, durata, frequenza o dimensione del messaggio.
3. Uso non autorizzato delle informazioni della testata delle e-mail,
4. Sollecitare messaggi di risposta a ciascun messaggio inviato con l'intento di disturbare o collezionare copie.
5. Uso di messaggi non sollecitati originati dalla Intranet per altri soggetti terzi per pubblicizzare servizi erogati dall'Amministrazione e fruibili via Intranet stessa.
6. Invio di messaggi non legati alla missione dell'Amministrazione ad un grande numero di destinatari utenti di news group (news group spam).

7.4 Uso della posta elettronica e della rete internet

Ai sensi del Provvedimento del Garante per la protezione dei dati personali del 1 marzo 2007, pubblicato sulla Gazzetta Ufficiale n. 58 del 10 marzo 2007, questa Amministrazione comunale adotta il "*Disciplinare per l'uso della posta elettronica e della rete internet nel rapporto di lavoro*".

8 POLITICHE - SELEZIONE E GESTIONE SICURA DELLE PAROLE CHIAVE

8.1 Generalità

Tutte le parole chiave a livello di sistema, come ad esempio quelle dell'amministratore di un sistema operativo, 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 (ogni mese)

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 e giudiziari.

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 compromessa.

È fatto assoluto divieto di inserire parole chiave in messaggi di posta elettronica od altre forme di comunicazione elettronica.

8.2 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 aziendale.

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 di casella elettronica vocale, e simili.

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 buona nota delle modalità con cui è possibile selezionare parole chiave di difficile individuazione.

8.2.1 Parole chiave deboli

Le parole chiave di facile individuazione 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 un 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 ritenersi 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.

8.2.2 Parole chiave sicure

Per contro, sono da ritenersi 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 miscela 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 surrettiziamente 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:

1. 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";
2. La parola chiave può essere formata abbreviando una intera frase come ad esempio "che gelida manina" diventa "chegemani"

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

8.3 Raccomandazioni per la protezione delle parole chiavi

Non utilizzare la stessa parola chiave per sistemi di autenticazione interni all'Ente e per sistemi di autenticazione esterni, come ad esempio l'accesso al proprio conto corrente bancario ed altre attività non legate all'attività lavorativa.

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 ed una parola chiave separata per l'accesso alla contabilità)

La parola chiave prescelta non dev'essere condivisa con alcun soggetto, interno o esterno all'Ente, ivi inclusi i superiori, a qualsiasi livello.

Tutte le parole chiavi 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:

1. Non rivelare una parola chiave attraverso il telefono a chicchessia;
2. Non scrivere una parola chiave in un messaggio di posta elettronica;
3. Non rivelare la parola chiave al proprio superiore;

4. Non parlare di parole chiave di fronte a terzi;
5. Non dare alcuna indicazione in merito al formato ed alla lunghezza della parola chiave che si utilizza;
6. Non svelare la parola chiave su questionari o su formulari di sicurezza;
7. Non rivelare la parola chiave a membri della famiglia;
8. Non rivelare la parola chiave ad un proprio collega di lavoro mentre si è in vacanza;

Se qualcuno insiste per conoscere la sua parola chiave con un incaricato, quest'ultimo deve dapprima fare riferimento a questo documento e successivamente informare immediatamente il responsabile della sicurezza logica o il suo titolare o responsabile.

Non utilizzare mai la caratteristica, offerta da parecchie applicazioni, di ricordare la parola chiave.

Non scrivere la parola chiave su un qualsiasi documento e non nasconderlo in alcun posto del proprio ufficio.

Non archiviare 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.

Ricordarsi di cambiare la parola chiave almeno una volta ogni sei mesi; quest'intervallo viene ridotto a tre mesi in caso la parola chiave consenta l'accesso al trattamento di dati sensibili e giudiziari.

Se si ha anche solo il minimo sospetto che la propria parola chiave sia stata in qualche modo compromessa o sia venuta a conoscenza di terzi, si provveda immediatamente alla sostituzione della stessa e si riferisca l'accaduto al responsabile della sicurezza logica, oppure al titolare o 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 parola chiave di qualche incaricato. Nel caso il tentativo abbia esito positivo, verrà chiesto a costui di sostituire immediatamente la parola chiave.

8.4 Istruzioni speciali per chi gestisce le applicazioni software

I responsabili della gestione delle applicazioni sw devono accertarsi che i loro programmi siano dotati delle seguenti caratteristiche di sicurezza:

- Le applicazioni devono essere in grado di autenticare i singoli individui e non i gruppi;
- Le applicazioni non devono archiviare le parole chiave in chiaro od in una forma facilmente intelligibile;
- Le applicazioni devono avere la possibilità di introdurre la figura di un gestore di livello superiore, di modo che un utente possa subentrare alle funzioni di un altro, senza dover conoscere la sua parola chiave.

8.5 Frasi chiave

Le frasi chiave possono essere utilizzate per l'autenticazione remota di un utente, utilizzando gli 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, 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.

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 è 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.

8.6 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 va automaticamente disattivato.

Per riprendere l'operatività, l'incaricato deve prendere contatto con il titolare o responsabile del trattamento di dati personali.

8.7 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 l'operatività, l'incaricato deve prendere contatto con il titolare od il responsabile del trattamento di dati personali.

8.8 Interventi di emergenza

Il disciplinare tecnico in materia di misure minime di sicurezza prevede esplicitamente che sia possibile, per il titolare o 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 appresso illustrata 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 soprariportata, 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 titolare o al responsabile del trattamento dei dati personali e il suo contenuto deve essere costantemente aggiornato, ogniqualvolta l'incaricato decida di sostituire la propria parola chiave.

È facoltà del titolare o del responsabile, in presenza dell'incaricato, aprire la busta sigillata e verificare che la parola chiave presente sul foglio di carta corrisponda a quella effettivamente in uso.

È fatto obbligo al titolare o al responsabile del trattamento dei dati personali di verbalizzare in apposito registro, con controfirma di garanzia da parte di terzi (precisare), l'avvenuta apertura della busta e la presa di conoscenza della parola chiave.

Resta inteso che dal momento in cui il titolare o 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 e di assumersi, quindi, nuovamente la piena responsabilità del corretto utilizzo. In tale occasione ci si rammenti di inserire la nuova parola chiave nella busta sigillata, come precedentemente illustrato.

8.9 Sanzioni

Un incaricato che abbia violato queste istruzioni 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 comunale.

8.10 Allegati

Moduli	Oggetto
MO – NOMINA CUSTODE PASSWORD	Lettera d'incarico al Custode Password
MO – RICHIESTA PASSWORD	Richiesta Password
MO – COMUNICAZIONE PASSWORD	Comunicazione password