LINEE GUIDA AZIENDALI E NORME COMPORTAMENTALI PER LA SICUREZZA INFORMATICA NEL TRATTAMENTO DEI DATI

Data	Ed.	Rev.	Oggetto	Autorizzato da
17/11/2025	01	00	Prima Stesura	Legale Rappr.

Sommario

1. INTRODUZIONE

Il presente documento ha l'obiettivo di **rendere edotti gli incaricati al trattamento dei pericoli associati all'utilizzo degli strumenti elettronici e di assicurare l'adozione delle misure di sicurezza nella gestione del trattamento dei dati aziendali**.

Si fissano inoltre le **linee guida cui debbono attenersi gli incaricati al trattamento dei dati** e viene altresì regolamentato l'utilizzo di internet , della posta elettronica e dei dispositivi portatili e personali per gli utenti di tali servizi nell'ambito della struttura aziendale della AISMA S.R.L..

Questo documento è adottato dall'Amministratore Unico di AISMA S.R.L., in conformità alla norma ISO/IEC 27001, al Codice della Privacy e al Regolamento Europeo 2016/679.

A tal proposito, allo scopo di rappresentare agli utenti il quadro normativo di riferimento si specifica che le principali fonti normative e legislative in materia sono le seguenti:
- Decreto Legislativo n.101/18 (di seguito "Codice");
- Norma tecnica ISO/IEC 27001 e 27017;
- Regolamento UE 2016/679

Copia del presente Regolamento viene consegnata a ciascun dipendente all'atto dell'assunzione ed a ciascun collaboratore ad inizio attività.

L'inosservanza delle norme sulla privacy può comportare sanzioni di natura civile e penale per l'incaricato e per l'azienda per cui si raccomanda di prestare la massima attenzione nella lettura delle disposizioni di seguito riportate.

2. CAMPO DI APPLICAZIONE

"**RENDERE EDOTTI GLI AUTORIZZATI AL TRATTAMENTO DEI DATI DEI PERICOLI ASSOCIATI ALL'UTILIZZO DEGLI STRUMENTI ELETTRONICI E DI ASSICURARE L'ADOZIONE DELLE MISURE DI SICUREZZA NELLA GESTIONE DEL TRATTAMENTO DEI DATI PERSONALI**"

Le presenti Istruzioni si applicano:
- a tutti i lavoratori dipendenti e a tutti i collaboratori della AISMA S.R.L. a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratori a progetto, agenti, stagisti, consulenti, ecc.) che si trovano ad operare sui dati aziendali e sui dati personali di cui la AISMA S.R.L. stessa è Titolare o Responsabile del Trattamento (di seguito "utenti");
- a tutte le attività o comportamenti comunque connessi all'utilizzo della rete Internet, della posta

elettronica, mediante strumentazione aziendale o di terze parti autorizzate all'uso dell'infrastruttura aziendale.

3. SICUREZZA INFORMATICA

La sicurezza informatica può essere definita come *"l'insieme delle misure, di carattere organizzativo e tecnologico, atte a garantire l'**autenticazione** dell'utente, la **disponibilità**, l'**integrità** e la **riservatezza** delle informazioni e dei servizi, **gestiti** o **erogati** in modo digitale*".

Da questa definizione si capisce come la sicurezza informatica sia applicabile, con le opportune differenze, sia a sistemi industriali, grandi, condivisi dinamici e distribuiti, sia a sistemi "micro", come il PC (*personal computer*), i Laptop e gli smartphone in dotazione ai lavoratori.

Importante capire **quali siano i rischi che corrono i nostri dati**. **Occorre prendere consapevolezza delle possibili minacce e delle relative e semplici azioni che possono essere fatte per prevenire e proteggerci da queste**.

Con la presente guida si intende quindi fornire una veloce panoramica della terminologia, delle possibili minacce e delle regole di comportamento da tenere per garantire un livello di "sicurezza" adeguato per il nostro patrimonio informativo digitale.

4. MALWARE

Con il termine ***malware*** (dalla contrazione delle due parole inglesi "*mal*icious" e "soft*ware*", letteralmente "programma maligno" o "codice maligno") si indica genericamente un qualsiasi *software*, ovvero un qualsiasi programma, creato con lo scopo di causare danni più o meno gravi ad un computer o a un qualsiasi sistema informatico su cui viene eseguito ed ai dati degli utenti ivi contenuti.

All'interno della categoria dei *malware* esistono una serie di programmi ognuno dei quali agisce con modalità differenti e con obiettivi specifici particolari. Spesso viene fatta confusione tra queste tipologie (per esempio, spesso si parla di *virus* come generico *malware*, ma, come descritto in seguito, il *virus* è, propriamente, un ben preciso tipo di *malware*); scopo dei paragrafi seguenti è fornire una descrizione delle principali tipologie di *malware*: ogni computer, soprattutto se è collegato alla rete, è esposto a pericoli quali *virus*, *worm* ("vermi" informatici) o *trojan* ("cavalli di Troia") nonché a *spyware*, che possono causare la perdita di dati con gravi pregiudizi alla sfera privata. D'altra parte anche la tecnica del *phishing* può portare alla perdita di informazioni personali estremamente delicate, mentre *hoax* o *spam* sono spesso solo fastidiosi, qualora si adottino le appropriate contromisure comportamentali.

4.1 Virus

Un **virus** è un programma informatico composto da una serie di istruzioni elementari, come qualsiasi altro programma. È solitamente composto da un numero molto ridotto di istruzioni ed è specializzato per eseguire soltanto poche e semplici operazioni ed ottimizzato per impiegare il minor numero di risorse, in modo da rendersi il più possibile invisibile. Caratteristica principale di un virus è quella di riprodursi e quindi diffondersi nel computer ogni volta che viene aperto un file infetto.
In analogia con un virus biologico, un virus non è un programma eseguibile a sé stante, ma per essere attivato deve infettare un programma ospite, o una sequenza di codice che viene lanciata automaticamente, come ad esempio i virus che sfruttano il "boot sector" che viene eseguito ad ogni avvio della macchina. La tecnica solitamente usata dai virus è quella di infettare i file eseguibili: il virus inserisce una copia di se stesso nel file .exe che deve infettare, ponendo tra le prime istruzioni un'istruzione di salto alla prima linea della sua copia ed alla fine di essa un altro salto all'inizio dell'esecuzione del programma originario. In questo modo quando un utente lancia un programma infettato viene comunque assicurata l'esecuzione del programma stesso: l'utente in questo modo non si accorge che il virus è in esecuzione e sta svolgendo, a sua insaputa, le operazioni contenute nel suo codice e per il quale è stato progettato.
Il virus, oltre ad auto-replicarsi, può procedere ad una serie di operazioni estremamente dannose, che

vanno dal semplice far apparire messaggi (per esempio *banner* o *popup* non richiesti), all'apertura di *backdoor* che possono consentire ad utenti esterni malintenzionati di accedere alla macchina, alla cattura di dati ed informazioni presenti sulla macchina, alla loro compromissione, fino ad arrivare alla loro distruzione.

4.2 Worm

Come i virus, i **worm** (dall'inglese: "vermi") sono dei programmi opportunamente progettati per danneggiare l'utente, ma, contrariamente ai virus, non necessitano di un programma ospite per funzionare, essendo essi stessi dei programmi completi. Essi sfruttano invece lacune di sicurezza (in gergo "**vulnerabilità**") o errori di configurazione del sistema operativo per propagarsi autonomamente da un computer all'altro. Obiettivo dei worm sono computer che presentano lacune di sicurezza o errori di configurazione e che sono collegati ad altri computer, tipicamente attraverso internet.

Anche in questo caso, il programma, una volta lanciato, può portare a conseguenze estremamente dannose per l'utente: dall'accesso non autorizzato alla macchina da parte di utenti malintenzionati, alla perdita di dati confidenziali, alla totale compromissione del computer.

4.3 Trojan

I **trojan** (letteralmente "cavalli di Troia") sono programmi che eseguono di nascosto operazioni nocive, nascondendosi all'interno di applicazioni e documenti utili per l'utente. Questi sfruttano lacune di sicurezza dei programmi utilizzati per aprire i file infetti per installarsi nel sistema ad insaputa dell'utente. Per esempio potrebbero trovarsi all'interno di brani musicali .mp3 e sfruttare una qualche vulnerabilità del programma di riproduzione, soprattutto qualora questo non fosse aggiornato all'ultima versione.

Spesso i trojan sono programmi scaricati da internet, altre volte vengono propagati per il tramite di allegati alle Email.

I pericoli sono gli stessi che si corrono con i classici virus: spionaggio di dati confidenziali (password, codici di accesso ai servizi bancari, pin ecc.) mediante registrazione e comunicazione inconsapevole al malintenzionato dei dati digitati sulla tastiera piuttosto che accesso non autorizzato al computer.

4.4 Spyware e Adware

Lo "**spyware**" (termine derivante dalla contrazione delle parole inglesi "*spy*" e "soft*ware*") è destinato a raccogliere all'insaputa dell'utente informazioni sulle sue abitudini di navigazione oppure sulle configurazioni di sistema per trasmetterle a un indirizzo predefinito. Il tipo di informazioni lette varia da uno spyware all'altro e può spaziare dalle abitudini di navigazione sino alle password.

Il termine di "**adware**" deriva invece dalla contrazione delle parole inglesi "*ad*vertising" (pubblicità) e "soft*ware*". In genere l'adware è utilizzato a scopi pubblicitari, nel senso che le abitudini di navigazione dell'utente vengono registrate e sfruttate per offrirgli prodotti corrispondenti (ad es. per il tramite di link personalizzati), pur senza che questi ne abbia fatto richiesta esplicita. Lo spyware e l'adware si installano solitamente sul computer quando si scaricano programmi.

In questo caso i pericoli vanno dallo spionaggio di dati confidenziali (dalle abitudini di navigazione fino alle password) con evidente pregiudizio della sfera privata alla pubblicità indesiderata, nel caso tipico degli adware.

4.5 Social Engineering

Gli attacchi di "**social engineering**" sfruttano la disponibilità, la buona fede e l'insicurezza delle persone per accedere per esempio a dati confidenziali o per indurre le vittime a effettuare determinate operazioni. Fra le tante possibilità di attacco, questa è ancora una delle più efficaci. Chi sfrutta il social engineering può per esempio accedere al nome di utente e alla password dei collaboratori di un'impresa facendosi per esempio passare al telefono come amministratore del sistema o come responsabile della sicurezza.
Abbagliata dal pretesto di gravi problemi informatici e dallo scambio di informazioni sul sistema (ad es. nome del superiore, processi di lavoro, ecc.), la vittima è resa insicura fino al punto da comunicare le informazioni richieste. Per la propagazione di virus e di cavalli di Troia vengono sovente applicati metodi di social engineering; ne è il caso quando il nome dell'allegato a un Email contenente un virus promette contenuti particolarmente interessanti. Il "phishing" è una speciale forma di attacco di social engineering.
Le conseguenze di un attacco di social engineering andato a buon fine sono la rivelazione di informazioni confidenziali attraverso l'inganno e, in taluni casi, la propagazione di virus o trojan.

4.6 Phishing

La parola **phishing** deriva dalla contrazione delle parole inglesi "password", "*harvesting*" (raccolta) e "*fishing*" (pesca): i malintenzionati tentano di accedere ai dati confidenziali di ignari utenti. Si può trattare per esempio, caso tipico, di dati di accesso a servizi bancari on-line. I truffatori sfruttano la buona fede e la disponibilità delle loro vittime inviando loro Email nei quali l'indirizzo del mittente è falsificato ed in cui si annuncia che le informazioni sul suo conto devono essere modificati avvalendosi del link integrato nell'Email. Il link non indirizza però alla pagina del presunto mittente, ma su una abilmente falsificata allestita dal truffatore. Grazie ai dati ottenuti (principalmente le credenziali di accesso), il truffatore può effettuare transazioni bancarie a nome della vittima entrando in maniera abusiva nel suo conto on-line, con evidente enorme danno immediato.

4.7 Vulnerabilità

Un "**programma**" informatico (**software**) è costituito da una serie di "istruzioni" (o "codice") che assegnano al computer operazioni da eseguire. Il software installato sui nostri personal computer comprende decine di migliaia di righe di codice: non deve quindi sorprendere che vi possano essere contenuti alcuni errori. Ogni giorno vengono scoperti e pubblicati errori di progettazione e di realizzazione dei programmi che correntemente vengono fatti funzionare sulle nostre macchine. La maggior parte di questi errori non ha alcun impatto sulla sicurezza del sistema ma alcuni sono tali da poter rendere possibile un accesso non autorizzato ai dati e al sistema. Si parla in questo caso di "**vulnerabilità**" del sistema, in quanto tali errori possono consentire ad utenti malintenzionati di accedere in qualche modo ai dati contenuti nel nostro computer.

4.8 Hoax

Le Email contenenti informazioni su nuovi virus o presunti tali sono quasi sempre notizie false ("**hoax**", termine inglese per designare scherzi o notizie false). In genere si viene messi in guardia contro nuovi virus estremamente pericolosi, impossibili da combattere anche con i normali antivirus e si viene invitati a diffondere la notizia a tutti i conoscenti o a seguire delle istruzioni per evitare la minaccia. Talvolta si parla anche di "catene di sant'Antonio", quando l'obiettivo è quello di far circolare il messaggio con un contenuto spesso assurdo e che fa generalmente leva su aspetti scaramantici o emotivi.

4.9 Spam

Con "**spam**" si indicano generalmente tutte le Email indesiderate, con un contenuto di vario genere, da quello pubblicitario, a quello più o meno fantasioso ed assurdo tipico delle catene di sant'Antonio. Lo "spammer" è il mittente di queste comunicazioni, mentre il fenomeno del loro invio è denominato "spamming".
Lo spammig porta ad una notevole perdita di tempo da parte di chi riceve il messaggio, anche per la sua sola cancellazione, oltre ad un inutile sovraccarico della infrastruttura tecnica (rete, server di posta ecc.).

4.10 Cookies

I **cookies** (dall'inglese, "biscotti") sono piccoli file di testo creati sul computer dell'utente quando visita una pagina web e sono nati per facilitare l'utente stesso. Ad esempio, per l'accesso a taluni servizi online sono necessari un nome di utente e una password: per non dover ripetere ogni volta l'immissione, queste informazioni sono registrate in un cookie locale e inserite automaticamente nei campi corrispondenti ad ogni visita della pagina. Altro esempio è quello fatto dai servizi di commercio on-line per il salvataggio temporaneo
del contenuto del carrello degli acquisti o per mostrare prodotti nuovi rispetto a quelli disponibili al momento dell'ultima visita. I cookies possono essere di "breve durata" ("**session** cookies") o di "lunga durata" ("**persistent** cookies"). I primi sono cancellati alla chiusura del browser, mentre i "persistent cookies", la data di scadenza viene stabilita dall'applicazione web, che utilizzerà il cookie sino a quella data.
Un utilizzo "improprio" dei cookies può portare pregiudizio alla riservatezza della propria sfera privata, rendendo possibile il tracciamento delle attività dell'utente ed un suo
inconsapevole "tracciamento".

4.11 Chat e Instant Messaging

Per **chat** si intende la possibilità di comunicazione offerta da Internet, grazie alla quale ci si può intrattenere in tempo reale con altri utenti. Diversamente dalle conversazioni telefoniche, la discussione non si svolge con la parola, bensì tramite digitazione delle informazioni. A seconda delle tematiche sono disponibili diversi spazi chat ("canali"). L'utente può comunicare contemporaneamente con tutti gli altri partecipanti oppure "ritirarsi" con un altro utente in uno spazio privato non accessibile agli altri. Per la loro apparente anonimità, i servizi chat (o di instant messaging) vengono spesso sfruttati per operazioni illegali (ed esempio adescamento) o possono essere utilizzati come vettori di infezione (virus, worm o trojan) quando i partecipanti alla chat sono invitati a cliccare su link o a

digitare comandi sconosciuti.

4.12 Wireless LAN

L'abbreviazione WLAN ("**Wireless Local Area Network**") significa "rete locale senza fili" in cui un apparato (ad es. un personal computer) comunica senza fili con un cosiddetto WLAN Access Point ("router"), collegato a sua volta a internet o a una rete. Grazie all'assenza del cablaggio, gli utenti degli apparati finali sono più mobili e questo costituisce il vantaggio di una WLAN.

Una configurazione imprudente del WLAN Access Point può determinare l'accesso illimitato a persone non autorizzate rendendo possibile l'accesso al computer e ai dati e l'utilizzazione abusiva del collegamento a internet. Inoltre una cifratura insufficiente dei collegamenti WLAN consente la lettura dei dati scambiati tra gli apparati ed i router attraverso strumenti relativamente semplici.

5. LINEE GUIDA PER IL TRATTAMENTO DEI DATI PERSONALI

Di seguito vengono descritte le norme a cui gli Incaricati devono attenersi nell'esecuzione dei compiti che implicano un trattamento di dati personali riferiti sia a persone fisiche che giuridiche.

Preliminarmente va evidenziato che, al fine di evitare che soggetti estranei possano venire a conoscenza dei dati personali oggetto del trattamento, l'Incaricato deve osservare le seguenti regole di ordinaria diligenza, nonché tutte le altre ulteriori misure ritenute necessarie per garantire il rispetto di quanto disposto dalla normativa in ambito privacy:

• tutte le operazioni di trattamento devono essere effettuate in modo tale da garantire il rispetto delle misure di sicurezza, la massima riservatezza delle informazioni di cui si viene in possesso considerando tutti i dati confidenziali e, di norma, soggetti al segreto d'ufficio;

• le singole fasi di lavoro e la condotta da osservare devono consentire di evitare che i dati siano soggetti a rischi di perdita o distruzione, che vi possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati stessi sono stati raccolti;

• in caso di allontanamento, anche temporaneo, dalla propria postazione di lavoro si devono porre in essere tutte le misure necessarie (es. blocco del pc) affinché soggetti terzi, anche se dipendenti, non possano accedere ai dati personali per i quali era in corso un qualunque tipo di trattamento, sia esso cartaceo che automatizzato;

• non devono essere eseguite operazioni di trattamento per fini non previsti tra i compiti assegnati dal diretto responsabile;

• devono essere svolte le sole operazioni di trattamento necessarie per il raggiungimento dei fini per i quali i dati sono stati raccolti;

• deve essere costantemente verificata l'esattezza dei dati trattati e la pertinenza rispetto alle finalità perseguite nei singoli casi.

Quanto sopra descritto impone, in altri termini, di operare con la massima attenzione in tutte le fasi di trattamento, dalla esatta acquisizione dei dati, al loro aggiornamento, alla conservazione ed eventuale distruzione.

6. REGOLE DI COMPORTAMENTO

Nei successivi paragrafi si riportano le norme che gli Incaricati devono adottare sia che trattino dati in formato elettronico che cartaceo.

6.1 Accesso ai dati dalla postazione di lavoro

La postazione di lavoro deve essere:

- utilizzata solo per scopi legati alla propria attività lavorativa;
- utilizzata in modo esclusivo da un solo utente;
- protetta, evitando che terzi possano accedere ai dati che si sta trattando

E' preciso dovere dell'Incaricato:

- non utilizzare in Azienda risorse informatiche private (PC, periferiche, token, ecc..);
- non installare alcun software;
- non lasciare sulla scrivania informazioni riservate su qualunque supporto esse siano archiviate (carta, CD, Pen Drive, ecc.);
- richiamare le funzioni di sicurezza del sistema operativo (con la sequenza dei tasti CTRL+ALT+CANC) ed assicurarsi della attivazione della funzione Lock Workstation in caso di abbandono momentaneo del proprio PC o, in alternativa, impostare lo screen saver con password in modo che si attivi dopo massimo 5 minuti di inattività;
- non lasciare il computer portatile incustodito sul posto di lavoro (al termine dell'orario lavorativo, durante le pause di lavoro, o durante riunioni lontane dalla propria postazione);
- non lasciare incustoditi cellulari e tablet;
- non utilizzare fax e/o telefono per trasmettere informazioni riservate e personali se non si è assolutamente certi dell'identità dell'interlocutore o del destinatario e se esso non è legittimato a riceverle

6.2 Gestione delle Password

Sono molti i servizi che richiedono l'uso di una password di accesso. La scelta poco avveduta di una password costituisce un notevole incremento dei rischi per la sicurezza.

Cambio password alla prima assegnazione

Modificare, alla prima connessione, quella che l'Area IT ha attribuito di default.

Lunghezza minima

La lunghezza minima di una password è di 8 caratteri. Tuttavia per incrementare il livello di Sicurezza è meglio settare una password con 12 o 16 digit. Essa deve essere composta sempre in parte di lettere dell'alfabeto miniscole e Maiuscole, in parte di cifre ed in parte di caratteri speciali (@-#!£$%, ecc.)

Facilità di memorizzazione

La password deve essere scelta in modo che possa essere memorizzata facilmente senza annotarla per scritto. Buone password sono frasi/parole compiute che contengono anche segni speciali; ad esempio : "m1_ch1am0%P1pp0!". Sono disponibili diversi programmi con l'ausilio dei quali potete collaudare la robustezza di una password (non effettuare mai questi test con password originali, ma con password similari)

Un servizio, una password

Utilizzare password diverse per cope diversi. Nel caso dell'utilizzazione di servizi online si raccomanda fortemente di utilizzare per ognuno di essi una password diversa.

Modifica regolare

La password deve essere modificata a intervalli regolari (consigliata la modifica ogni mese con massimo intervallo di modifica a tre mesi), ed immediatamente quando si presume che possa essere conosciuta da terzi.

Password nettamente diversa dalla precedente

La nuova password deve essere nettamente diversa dalla precedente.

Password non deve contenere riferimenti personali

La nuova password non deve contenere riferimenti personali come ad esempio nome, cognome, data di nascita, codice fiscal ecc..

Evitare di annotare la password su fogliettini lasciati in prossimità dei device

La password non deve essere trascritta su supporti (es. fogli, post-it) facilmente accessibili a terzi, né lasciata memorizzata sul proprio PC.

Riservatezza nella gestione delle password

La password non deve essere mai comunicata a nessuno per qualsivoglia motivo.

Riservatezza nell'inserimento delle password
La password non deve essere mai inserita quando qualcuno può osservare.

Identificativo utente strettamente personale
Non permettere ad altri utenti (es. colleghi) di operare con il proprio identificativo utente.

6.3 Gestione delle Email

La prudenza nella gestione delle Email ricevute contribuisce in grande misura alla sicurezza dei vostri dati e dei vostri devices. Il rispetto delle semplici regole che seguono sono una ottima protezione contro gran parte delle attuali minacce.

Prudenza nella apertura di Email con mittente ignoto
Diffidare delle Email di cui non si conosce l'indirizzo del mittente. In questo caso non aprire mai gli allegati o i programmi ivi contenuti, **né selezionare i link indicati.**
Visualizzare preventivamente il contenuto tramite utilizzo della funzione "Riquadro di lettura" (o preview) e, nel caso si riscontri un contenuto sospetto, non aprire il messaggio.

Verifica dell'affidabilità della fonte
Aprire unicamente i file o i programmi provenienti da fonti affidabili e solo previa verifica con un programma antivirus aggiornato.

Prestare attenzione ai file con due estensioni
Non aprire mai gli allegati ad Email provvisti di due estensioni (ad es. picture.bmp.vbs) e non lasciarsi ingannare dall'icona di simili file. Disattivare nelle opzioni del browser, dove presente, l'opzione "nascondi le estensioni per i tipi di file conosciuti"

Aggiornamento del software
Anche i programmi di gestione delle Email possono presentare vulnerabilità: sincerarsi regolarmente di aver installato l'ultima versione disponibile del software

Comunicazione del proprio indirizzo Email
Per limitare lo spam, è sempre opportuno comunicare il proprio indirizzo Email alle **sole** persone necessarie

Non rispondere agli spam
Rispondere ad un messaggio di spam equivale ad informare lo spammer che l'indirizzo Email è valido e quindi questi invierà ulteriori spam oppure metterà il vostro indirizzo a disposizione di altri spammer.

Particolare attenzione va portata agli spam con l'opzione di "cancellazione dall'elenco" in cui si promette la cancellazione dall'elenco di distribuzione tramite l'invio di un Email con un determinato contenuto. Da questo punto di vista va data particolare attenzione alle Email di risposta automatica in caso di assenza per vacanze. Tali risposte automatiche dovrebbero essere attivate unicamente per gli indirizzi conosciuti

Hoax

Nella maggior parte dei casi gli avvertimenti di pericolo di virus inviati tramite Email sono false informazioni (hoax): non eseguire mai, in nessun caso, le raccomandazioni ivi contenute. Questo con particolare riferimento a: cancellazione di file, installazione di un determinato programma, inoltro dell'informazione ai conoscenti. In caso di dubbio consultate le pagine web ufficiali dei produttori di programmi antivirus.

Analoghe considerazioni sono valide nel caso delle catene di “sant'Antonio”

Divieto di comunicazione di informazioni riservate

E’ vietato l’utilizzo della posta elettronica per comunicare informazioni riservate, dati personali o dati critici, senza garantirne l’opportuna protezione.

Verifica dei destinatari dei messaggi di posta elettronica

Occorre sempre accertarsi che i destinatari della corrispondenza per posta elettronica siano autorizzati ad entrare in possesso dei dati che ci si appresta ad inviare.

Impostazione del messaggio “Fuori Sede”

L’utente, in caso di assenza programmata (ad esempio per ferie o attività di lavoro fuori sede) deve attivare l’apposita funzionalità di sistema (cd. “Fuori Sede”) che consente di inviare automaticamente ai mittenti un messaggio di risposta contenente le “coordinate” (anche elettroniche o telefoniche) di un altro utente o altre modalità utili di contatto della struttura.

La formulazione dei messaggi

La formulazione dei messaggi deve pertanto far uso di un linguaggio appropriato, corretto e rispettoso che tuteli la dignità delle persone, l’immagine e la reputazione dell’Azienda.

Errore nella spedizione / ricezione dei messaggi

In caso di errore nella spedizione o ricezione, contattare rispettivamente il destinatario cui è stata trasmessa per errore la comunicazione o il mittente che, per errore, l’ha spedita, eliminando quanto ricevuto (compresi allegati) senza effettuare copia.

6.4 Navigazione in internet

Gran parte dei pericoli per la sicurezza del proprio computer vengono corsi durante la navigazione in internet. Molti di questi pericoli possono essere evitati adottando opportune misure comportamentali che vengono riportate di seguito.

Aggiornamento del software dai siti dei produttori

Scaricare gli aggiornamenti di software e driver **esclusivamente** dalla pagina web dei relativi produttori. È sempre buona norma anche verificarli successivamente con un programma antivirus aggiornato.

Prudenza nella trasmissione di informazioni

Non comunicare **mai** a nessuno le proprie credenziali di accesso (nome di utente e password). Nessun fornitore di servizi serio chiederà la vostra password (nemmeno telefonicamente). Questo vale anche quando la richiesta appare credibile. Nel caso di transazioni online, rivolgersi solo a fornitori seri: comunicare il numero della carta di credito unicamente per il tramite di pagine web che garantiscono la cifratura dei dati. Tale garanzia è riconoscibile da un lucchetto dorato che appare all'interno del browser oppure dal protocollo utilizzato (tipicamente "https" invece di "http")

Chiudere le applicazioni

Utilizzare sempre l'apposita notifica di chiusura ("logout") quando si esce da un'applicazione web che abbia richiesto l'introduzione delle proprie credenziali di accesso.

Riservatezza nella divulgazione delle informazioni personali

Evitate di rivelare dati personali durante la compilazione di moduli Web o la fornitura di contributi a newsgroup, forum o registri di visitatori

Attenzione alla configurazione del browser

Molte delle minacce che si incontrano durante la navigazione in internet sono legate all'utilizzo dei componenti "dinamici" delle pagine web tipicamente realizzati tramite controlli ActiveX o funzioni JavaScript. Tali funzionalità sono spesso indispensabili per il corretto funzionamento della pagina, ma spesso vengono utilizzate in maniera malevola da parte di malintenzionati per il lancio di malware sulla macchina ospite.

Una possibile contromisura può essere la limitazione di JavaScript o dei ActiveX.

Mantenere tendenzialmente le opzioni di sicurezza automatiche (per la configurazione delle quali si rimanda alla documentazione del browser che si utilizza) sul valore "alto".

Navigazione sui siti internet

E' consentita la navigazione internet solo in siti attinenti e necessari per lo svolgimento delle mansion assegnate.

Download software
Non è consentito scaricare software gratuiti (freeware o shareware) prelevati da siti Internet.

6.5 Gestione dei dispositivi portatili e personali

Tra i dispositivi portatili o mobili si annoverano: Pc portatili, Tablet, smrtphone, chiavi USB e Smart card.
Ciascuno di questi device può essere perso o rubato.
Detti oggetti vengono assegnati attraversio un puntuale e preciso processo autorizzativo.
Ai dispositivi portatili si devono applicare le medesime misure di Sicurezza dei normali PC descritte nei precedentio paragrafi.

Si rammentano i principali controlli.

Blocco con password
Bloccare i dispositivi con password se non utilizzati.

Vietato lasciarli incustoditi
Non lasciare mai i dispositivi incustoditi al fine di evitare i furti specialmente in automobile e nelle area di sosta austostradali.

Evitare di usarli in luoghi pubblici
Evitare di lavorare in luoghi pubblici con la possibilità che altri osservino i dati visualizzati a video.

Vietato l'utilizzo a persone non autorizzate
Vietato far utilizzare i dispositivi a persone non autorizzate per evitare che li danneggino e compromettano la Sicurezza dei dati deliberatamente o per errore.

Riservatezza nelle conversazioni in luoghi pubblici
Evitare di intrattenere conversazioni riservate in luoghi pubblici.

Cifrare l'hard disk della chiavetta USB
Creare una partizione cifrata dentro la quale inserire i file da proteggere.

Impostare una password per ogni singolo file presente nella chiavetta USB

Per ogni file occorre impostare una password di protezione.

Blocco schermo degli Smartphone

Il codice di sblocco dello schermo consente di "frapporre" una barriera di sicurezza nei confronti di curiosi o malintenzionati.

Sono tre le modalità di blocco schermo "classiche" a disposizione (pià o meno) su qualunque dispositivo mobile: sequenza di sblocco, codice numerico o password. Nel primo caso l'utente dovrà "disegnare" una figura geometrica (una sequenza) sul display per poter accedere alle funzionalità del telefono; negli altri due casi, invece, si dovrà inserire un PIN numerico o una password alfanumerica. Alcuni dispositivi (gli ultimi modelli di iPhone e gli smartphone Android di fascia alta) mettono a disposizione l'autenticazione tramite scansione dell'impronta digitale (tecnica biometrica, come il Touch ID di Apple).

L'utente dovrà impostare un codice di blocco schermo tra quelli più sicuri in dotazione al suo smartphone.

Divieto di utilizzare il Wi-Fi pubblico

Anche se utile quando si è fuori casa o all'estero, il Wi-Fi pubblico può essere uno dei mezzi più semplici da sfruttare per entrare all'interno dei device e trafugare le informazioni contenute al suo interno. Quando possibile, quindi, è consigliabile collegarsi utilizzando la connessione dati tramite chiavette aziendali oppure attendere di tornare a casa per connettersi a una rete Wi-Fi sicura.

Vietato scaricare App

Gli smartphone Android (e in misura minore anche l'iPhone) sono suscettibili di essere infettati da virus e malware di ogni tipo. Evitare di scaricare App di qualsiasi tipo.

Attivare le applicazioni antitheft e di tracciamento

Le applicazioni antitheft e di tracciamento possono tornare molto utili quando non si trova più il telefono. Servizi come Gestione dispositivi Android o Find my iPhone sfruttano il sensore GPS del telefonino per tracciarne gli ultimi spostamenti e, se accesi, segnalarne la posizione in diretta. In questo modo si potrà visualizzare dove si trova il dispositivo mobile ed, eventualmente, cancellare tutti i dati contenuti al suo interno.

Cliccare su link sconosciuti in arrivo via messaggistica elettronica

Sul web e sui social network capita di imbattersi in link abbreviati (i cosiddetti short link) molto utilizzati dagli iscritti di Twitter. A volte, però, dietro link brevi e "anonimi" si nascondono collegamenti a siti di phishing o portali infettati: vietato cliccare su link sconosciuti.

Installare gli aggiornamenti dello smartphone

Gli aggiornamenti sono fondamentali per garantire alti standard di sicurezza dello smartphone, infatti, al loro interno è possibile trovare nuove funzionalità di sicurezza o "pezze" per falle e bug che potrebbero essere sfruttate dagli hacker per entrare nel dispositivo e rubare le informazioni al suo interno.

Reti Bluetooth

-attivare Bluetooth solo quando necessario e disattivarlo dopo l'uso
-utilizzare Bluetooth soltanto in ambiente "sicuro" (possibilmente non in luogo pubblico) e se indispensabile
-attivare la visibilità Bluetooth dell'apparecchio solo se necessario
-utilizzare sempre le opzioni di sicurezza, attivando quando possibile le opzioni di autenticazione e cifratura

7. RESPONSABILITÀ E SANZIONI

L'utente, al fine di non esporre sé stesso e l'Azienda a rischi sanzionatori, è tenuto ad adottare comportamenti puntualmente conformi alla normativa vigente ed alla regolamentazione aziendale.
Gli utenti sono responsabili del corretto utilizzo dei servizi di Internet e Posta Elettronica. Pertanto sono responsabili per i danni cagionati al patrimonio, alla reputazione e alla Committenza.
Tutti gli utenti sono pertanto tenuti ad osservare e a far osservare le disposizioni contenute nel presente Regolamento il cui mancato rispetto o la cui violazione, costituendo inadempimento contrattuale potrà comportare:
- per il personale dipendente oltre che l'adozione di provvedimenti di natura disciplinare previsti dal Contratto Collettivo Nazionale di Lavoro tempo per tempo vigente, le azioni civili e penali stabilite dalle leggi tempo per tempo vigenti;
- per i collaboratori esterni oltre che la risoluzione del contratto, le azioni civili e penali stabilite dalle leggi tempo per tempo vigenti.