Linee Guida per la sicurezza nel trattamento dei dati personali

Persone autorizzate al trattamento

Titolo:	Linee Guida	**Aggiornamento**	Giugno 2022
Codice:	P02	**Revisione:**	/
File:	P02 Linee Guida sicurezza per Persone autorizzate al trattamento.doc		

Indice

Definizioni

Ai fini del presente documento valgono le seguenti definizioni:

- per "**Amministratori di Sistema**", i soggetti cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di basi di dati e di consentirne l'utilizzazione (ovvero, le persone autorizzate all'uso delle password di "*administrator*" dei sistemi operativi);
- per "**Banca Dati**", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti, ivi incluse – a titolo di esempio - le directory contenenti documenti di office, i database MS Access o Excel, gli archivi cartacei;
- per "**Categorie particolari di dati**", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- per "**Comunicazione**", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dalle persone autorizzate, in qualunque forma, anche mediante la loro messa a disposizione o consultazione (forme di comunicazione sono: la posta, il telefax, l'e-mail);
- per "**Dati Anonimi**", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- per "**Dati Identificativi**", i dati personali che permettono l'identificazione diretta dell'interessato, come il nome e il cognome, un numero di identificazione;
- per "**Dati Personali**", qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- per **"Dati Biometrici",** i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- Per **"Dati Genetici"**, i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- per "**Dati relativi a condanne penali e reati**", i dati personali idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato;

- per **"Dati relativi alla salute",** i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- per "**Diffusione**", il dare conoscenza dei Dati Personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione (per esempio: trasmissioni radiofoniche o televisive, stampa, pubblicazione su pagine WEB ad accesso non selezionato);
- per "**Gestori delle Password**", i soggetti cui è conferito il compito di custodire le password utilizzate in azienda o accedere alle informazioni ad esse relative e gestire le relative procedure (ovvero, le persone autorizzate all'uso delle password di "*administrator*" dei sistemi operativi);
- per "**Interessato**", la persona fisica cui si riferiscono i Dati Personali o particolari.
- per "**Misure di Sicurezza**", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza, previste dalla normativa vigente ed esplicitate in documentazione ufficiale della società (Incarichi, autorizzazazioni a trattare dati, Linee Guida, ecc.), che configurano il livello di protezione adeguato in relazione ai i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- per "**Responsabili del trattamento**", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che tratta dati personali per conto del Titolare;
- per "**Personale autorizzato**", le persone fisiche autorizzate a compiere operazioni di trattamento (vedi "**Trattamento**") sotto l'autorità del Titolare o del Responsabile (ovvero, tutto il personale che abbia accesso a Dati Personali e, in quanto tale, individuato per iscritto come autorizzato a trattare dati da parte del Responsabile del trattamento competente per l'UO di riferimento).
- per "**Strumenti**", i mezzi elettronici o comunque automatizzati con cui si effettua il trattamento (elaboratori, supporti, apparecchi di telecomunicazioni, ecc.);
- per "**Titolare del trattamento**", la nostra organizzazione, quale soggetto giuridico cui competono le decisioni in ordine alle finalità ed ai mezzi del trattamento di Dati Personali, ivi compreso il profilo della sicurezza;
- per "**Trasferimento all'estero**", il trasferimento dei Dati Personali aziendali fuori dal territorio dell'UE, con qualunque mezzo o sistema effettuato, quale, a mero titolo di esempio, l'invio tramite e-mail di liste e/o elenchi di Interessati con o senza ulteriori informazioni; il trasporto di liste e/o elenchi di Interessati con o senza ulteriori informazioni tramite personal computer portatile, CD Rom, o altri idonei supporti; l'inoltro di Fax, lettere o altri documenti cartacei contenenti liste e/o elenchi di Interessati con o senza ulteriori informazioni;
- per **"Trattamento"** si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione,

l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

- per "**Unità Organizzative**", o UO, si intendono gli uffici in cui è organizzata l'azienda ai fini della normativa, come indicato nel presente documento;
- per "**Ufficio del Personale**", si intende l'UO che si occupa precipuamente della gestione del personale.

1. Introduzione

Questo documento intende formalizzare alcune linee guida per garantire l'osservanza della vigente normativa in materia di riservatezza dei dati personali e la sicurezza dei sistemi informativi aziendali rispetto ai rischi di distruzione o perdita delle informazioni, accesso non autorizzato e trattamento non consentito.

Conformare il proprio comportamento a quanto di seguito indicato contribuirà al raggiungimento degli obiettivi della sicurezza, riassumibili nei tre aspetti distinti:

Disponibilità: ovvero, garantire l'accesso alle informazioni e ai servizi di rete da parte del personale autorizzato in relazione alle esigenze lavorative;

Riservatezza: ovvero, garantire la prevenzione di accessi abusivi o non autorizzati alle informazioni, ai servizi e ai sistemi;

Integrità: ovvero, garantire che le informazioni non siano state alterate da incidenti o abusi.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche gli opportuni meccanismi organizzativi; infatti, le misure tecniche, per quanto sofisticate, non saranno efficienti se non utilizzate propriamente.

In particolare, le precauzioni di tipo tecnico/informatico possono proteggere le informazioni durante il loro transito attraverso i sistemi ed anche quando queste sono registrate su un disco fisso di un elaboratore; ma nel momento in cui esse raggiungono l'utente autorizzato, la loro protezione dipende esclusivamente dall'operato quest'ultimo e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto di alcune semplici norme di comportamento.

2. Linee guida per la sicurezza nel trattamento

2.1. Utilizzo delle chiavi ed accesso agli uffici e agli archivi

Il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo e richiede comunque uno sforzo volontario e non banale per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso e prendere visione o sottrarre documenti. Per questo motivo, ove possibile l'accesso ai locali deve essere protetto dalla presenza di porte chiuse a chiave, e la chiave affidata alle Persone autorizzate al trattamento degli uffici stessi.

Questi ultimi dovranno quindi custodire la propria chiave con la massima riservatezza e scrupolo. Naturalmente la persona autorizzata non dovrà in nessun caso affidarla a terzi (anche se Persone autorizzate al trattamento). Al termine della giornata di lavoro, sarà compito di ciascun soggetto autorizzato di assicurarsi della chiusura della porta di accesso agli uffici operativi, assicurandosi altresì di aver riposto i documenti nei cassetti della propria scrivania o nei rispettivi archivi. Tali operazioni dovranno rispettarsi ogni volta che il soggetto autorizzato stesso lo ritenga opportuno in considerazione della natura dei dati trattati e del periodo di tempo per il quale il soggetto autorizzato medesimo sarà lontano dalla propria postazione di lavoro.

L'accesso agli archivi contenenti dati sensibili o giudiziari è permesso esclusivamente alle Persone autorizzate al trattamento. L'accesso a tali archivi deve essere controllato da parte di tutto il personale. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, devono essere identificate e registrate per mezzo dell'apposito registro.

Nell'ipotesi in cui gli atti e i documenti contenenti dati personali sensibili o giudiziari siano affidati alle persone autorizzate del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti devono essere controllati e custoditi dalle persone autorizzate al trattamento - fino alla restituzione - in maniera che ad essi non accedano persone prive di autorizzazione e siano restituiti al termine delle operazioni affidate.

2.2. Conservazione dei supporti (CD Rom, copie cartacee, fascicoli, ecc.) in un luogo sicuro

Per quanto concerne i supporti che contengono dati personali, si applicano gli stessi criteri di attenzione e protezione descritti al precedente punto in tema di accesso ai locali e agli archivi. Per tali supporti esiste l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) possa passare più facilmente inosservato. Pertanto, salvo il caso in cui la persona autorizzata sia certa che i supporti contengano solamente dati pubblici o conoscibili da chiunque, anche tali supporti dovranno essere riposti in

un contenitore o cassetto munito di serratura non appena ne sia terminato l'utilizzo (per il caso di copie cartacee, le stesse dovranno essere riposte nell'archivio di provenienza).

Naturalmente, maggior attenzione dovrà essere posta per quei particolari tipi di dati denominati "sensibili e/o giudiziari" (stato di salute, vita sessuale, adesione o opinioni religiose, politiche o sindacali, origini razziali o etniche, dati provenienti dal casellario giudiziale, ecc.). Per tali ultimi dati e per dati di altra natura (anagrafici, economici, ecc.) ma di particolare importanza o riservatezza, in caso di trattamento informatico si raccomanda il salvataggio nelle apposite directory di rete ad accesso selezionato; qualora sia necessario il salvataggio su supporti magnetici od ottici, si raccomanda il salvataggio del file sul supporto con protezione tramite password (ed il back-up del file stesso nella directory di rete ad accesso selezionato senza password di protezione), ovvero tramite sistemi di cifratura resi disponibili dal sistema operativo; tali supporti devono comunque essere conservati in contenitori o armadi muniti di serratura.

Il riutilizzo di un supporto magnetico od ottico è consentito a condizione che i dati in esso precedentemente contenuti siano irrecuperabili. Per garantire il rispetto di tale principio è quindi necessario procedere alla formattazione di basso livello del supporto prima del riutilizzo dello stesso; alternativamente il supporto dovrà essere distrutto, affinché i dati in esso contenuti risultino essere irrecuperabili.

Le riproduzioni di documenti contenenti dati sensibili e/o informazioni relative al trattamento di dati personali devono essere conservati e custoditi con le medesime modalità previste per i documenti originali.

2.3. Utilizzo di Stampanti, Fotocopiatrici e Fax

Le stampanti, le fotocopiatrici e i fax/telefax sono beni aziendali e devono essere utilizzati dal personale esclusivamente per attività di carattere lavorativo e non per scopi di natura personale.

Per quanto concerne l'utilizzo delle stampanti alle persone autorizzate devono stampare tutte le informazioni di natura sensibile o particolarmente riservata esclusivamente su stampanti presenti all'interno dei propri uffici o in uffici in cui le persone autorizzate lo siano anche per il trattamento dei medesimi dati, assicurandosi di non lasciare incustoditi i documenti sulla stampante. Nel caso di utilizzo di stampanti di rete ubicate in corridoi o locali di comune utilizzo, le persone autorizzate devono provvedere al tempestivo ritiro dei documenti.

Le persone autorizzate che si accorgano di aver commesso un errore nella stampa devono procedere all'annullamento. Le persone autorizzate che non siano riusciti ad annullare la stampa e si accorgano, al momento del ritiro della stampa, di errori che rendono inutilizzabili i documenti, devono provvedere alla distruzione dei medesimi nei propri uffici.

Per quanto concerne l'utilizzo delle fotocopiatrici le persone autorizzate devono effettuare copie nel numero strettamente necessario e non sovrabbondante.

Le copie possono essere consegnate solo a persone autorizzate a trattare la determinata tipologia di dati contenuta nei documenti; qualora si effettuino copie di documenti che contengono dati sensibili ma non sia assolutamente necessaria la conoscenza di questi, la persona autorizzata deve renderli illeggibili prima di porre il documento nella fotocopiatrice;

Qualora la persona autorizzata effettui copie di documenti contenenti dati sensibili, non deve allontanarsi dalla macchina durante la copiatura, per evitare che persone non autorizzate entrino in contatto con i dati.

Le copie ottenute devono essere sottoposte alle stesse misure di sicurezza dei documenti originali da cui sono state tratte.

Per quanto concerne l'utilizzo di fax/telefax, le persone autorizzate devono garantire, nella fase di *invio* di documenti di natura sensibile o riservata, la massima riservatezza delle informazioni.
La persona autorizzata che dopo l'invio richieda il "*rapporto di trasmissione*", deve riportare in ufficio sia il documento inviato sia il "rapporto di trasmissione" e deve assicurarsi di non lasciare nulla presso il centralino.

Nel caso di fax erroneamente indirizzati, le persone autorizzate del centralino/reception devono trattare tali documenti con la massima riservatezza in quanto potrebbero contenere dati personali o informazioni riservate appartenenti a terzi soggetti. Soltanto dopo aver contattato il mittente o il destinatario del fax potranno eliminare definitivamente il documento ricevuto, utilizzando un dispositivo distruggi – documenti.

2.4. Fasi del trattamento di dati personali

Durante le fasi del trattamento di dati personali le persone autorizzate dovranno fare quanto ragionevolmente possibile per garantire il livello di riservatezza richiesto dal legislatore. In quest'ottica, in fase di raccolta dei dati, occorrerà:

- accertarsi che in fase di raccolta dei dati personali a viva voce o per telefono, estranei o persone non autorizzate non possano ascoltare la conversazione;
- accertarsi che mentre l'interessato compila un formulario con dati personali, estranei e/o non autorizzati possano osservare;
- raccogliere tutti i formulari e/o i moduli di raccolta del consenso al trattamento dei dati personali in cassetti o armadi da tenere sempre chiusi a chiave;
- accertarsi che i moduli e/o i formulari e/o i documenti contenenti dati personali e/o sensibili non vengano abbandonati incustoditi sui tavoli;

- non consentire l'ingresso di estranei o non autorizzati in aree ove vengano trattati o custoditi dati personali e/o rientranti in categorie particolari;
- non gettare fogli contenenti dati personali senza aver prima reso illeggibili gli stessi.

Nel caso di trattamenti informatici di dati personali:

- cambiare spesso la password di accesso ai sistemi;
- non lasciare visualizzati sullo schermo dati personali in propria assenza;
- cancellare sempre tutti i dati residui presenti nell'elaboratore quando non più utilizzati;
- informare subito il responsabile dell'area se si evidenzia un accesso a dati non di vostra competenza;
- tenere sotto controllo l'accesso fisico all'elaboratore e consentire l'eventuale utilizzo solo ad altri soggetti autorizzati;
- accertare che vengano eliminati o distrutti in modo sicuro gli oggetti o supporti informatici utilizzati per archiviare dati personali e/o sensibili (prestare anche attenzione a cancellare i dati archiviati in aree di memoria del computer ad es. cestino di Windows).

Nel caso di comunicazioni di dati personali:

- se vengono richiesti via telefono dati personali, accertarsi sempre che il richiedente abbia titolo a farlo, in caso di dubbio o di richiesta di dati sensibili, ove possibile, valutare la possibilità di utilizzare mezzi più sicuri di comunicazione;
- nel caso vengano comunicati dati personali e/o sensibili via fax, prelevare il fax senza lasciarlo in mostra in attesa di essere prelevato;
- prima di inviare ad un corrispondente via fax dati personali e/o sensibili accertarsi che sia personalmente pronto a riceverli e che non vengano abbandonati presso la macchina ricevente in attesa di essere prelevati.

Prima di procedere a trasmissioni di dati sensibili mediante strumenti telematici o supporti magnetico/ottici, richiedere al proprio responsabile dell'area o al personale specializzato possibili soluzioni di cifratura dei dati trasmessi.

3. Le chiavi di accesso ai dati informatici, in particolare le password

La conformità dei sistemi informatici aziendali alle disposizioni legislative in tema di sicurezza è garantita dall'utilizzo corretto da parte degli utenti/persone autorizzate di diverse chiavi di accesso (user ID e Password, o semplice password) alle risorse informatiche contenenti dati personali.

L'utilizzo combinato di user ID e password permette ai sistemi informatici di riconoscere l'accesso logico come proveniente da una determinata persona e, conseguentemente, attribuire a tale persona i diritti di

accesso preconfigurati in base alle relative esigenze lavorative. Per questo motivo è importante non comunicare a terzi, ancorché colleghi, la propria password di autenticazione (in tal caso, infatti, terze persone accederebbero alle risorse di rete sotto l'identità digitale delle persone autorizzate e qualsiasi operazione abusiva venisse effettuata sarebbe attribuita alla responsabilità della persona autorizzata identificata dalla chiave di accesso).

Come detto, l'autenticazione della persona autorizzata/utente avviene a mezzo della password. In merito, Vi sono diverse categorie di password, ognuna con una propria funzione precisa:

- Le chiavi di accesso (user ID e password) alla rete LAN aziendale permettono alla persona autorizzata di essere riconosciuto come tale dal sistema di rete e, di conseguenza, di accedere alle risorse in esso contenute in base al proprio profilo d'utenza legato alla particolare chiave d'accesso. L'uso di tali chiavi di accesso, peraltro, impedisce che terzi non autorizzati possano accedere da una postazione alle risorse della rete.
- Le password di accesso dei programmi specifici (applicativi) permettono di restringere l'accesso ai dati processati da tali programmi al solo personale autorizzato.
- La password del salvaschermo, infine, impedisce l'accesso non autorizzato al proprio elaboratore (e alle risorse da questo accessibili) in caso di momentanea assenza della persona autorizzata dalla propria postazione di lavoro.

Per quanto concerne la scelta delle password si rimanda alle indicazioni della sezione successiva.
I files contenenti dati sensibili (stato di salute, vita sessuale, opinioni politiche, religiose, sindacali, origini razziali o etniche, dati provenienti dal casellario giudiziale) se per necessità di lavoro devono essere salvati oltre che nelle apposite directory di rete, anche su supporti magnetici od ottici (CD Rom, chiavette USB ecc.), devono essere protetti con password di accesso al documento o con sistemi di cifratura.

Custodia delle password

Le password devono essere mantenute segrete. Le persone autorizzate non devono scrivere la password in luoghi facilmente accessibili, né vicino alla postazione di lavoro. Se per esigenze di manutenzione dovesse essere necessario comunicare la propria password alle persone autorizzate della manutenzione, al termine dei lavori di questi ultimi sarà necessario modificare la propria password.

In caso di assenza di una persona autorizzata, il recupero di file, documenti o dati cui la stessa persona autorizzata aveva accesso esclusivo tramite le proprie credenziali di autenticazione, deve avvenire senza comunicazioni di password tra colleghi. In tali casi, deve essere informato l'Amministratore di sistema che, previa autorizzazione del Dirigente e comunicazione alla persona autorizzata assente, recupera i file, documenti o dati, rendendoli disponibili per le esigenze lavorative di terzi autorizzati.

Regole inerenti le password

Il più semplice metodo per l'accesso illecito a un sistema informatico consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è quindi parte essenziale della sicurezza informatica.

Di seguito vengono riportate alcune regole, che rappresentano lo standard in materia. Sebbene riportino alcune ripetizioni rispetto a quanto già detto in precedenza, si è ritenuto opportuno segnalare nuovamente il principio al fine di sensibilizzare l'utenza dei servizi di rete.

COSA NON FARE

1. **NON** comunicare a nessuno la propria password: lo scopo principale per cui le password sono usate è assicurare che nessun altro possa utilizzare le risorse affidate alla persona autorizzata o che terzi possano farlo a nome della persona autorizzata stessa.
2. **NON** scrivere la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer.
3. Quando si immettete la password nei form di richiesta, **evitare** che altri possano vedere i tasti che si battono sulla tastiera.
4. **NON** scegliere come password parole che si possano trovare in un dizionario delle principali lingue mondiali. Alcuni sistemi di forzatura delle password consistono in strumenti software che "provano" tutte le parole contenute nei dizionari per vedere quale sia quella giusta.
5. **NON** usare come password parole che possano in qualche modo essere legate alla propria persona come, ad esempio, il proprio nome o altri dati anagrafici o di identificazione, dati del coniuge o familiari, ecc.

COSA FARE

1. **Cambiare la password** ogni qual volta richiesto dal sistema. Chiedere agli Amministratori di Sistema quali sono le raccomandazioni sulla frequenza del cambio; in ogni caso, la password deve essere sostituita almeno ogni 90 giorni.
2. Usare password lunghe almeno **8 caratteri** e, preferibilmente, con un misto di lettere, numeri e segni di interpunzione, ovvero – laddove i sistemi gestiscano solo password di lunghezza inferiore – utilizzare password della lunghezza massima consentita dal sistema stesso.
3. Utilizzare password distinte per sistemi con diverso grado di sensibilità. In alcuni casi, le password viaggiano in chiaro sulla rete e possono essere quindi intercettate. Per cui, oltre a cambiarla spesso, è importante che sia diversa per quella usata da sistemi "sicuri". Il tipo di password in assoluto più sicura è quella associata a un supporto di identificazione come un dischetto o una carta a microprocessore; la password utilizzata su un sistema di questo tipo non deve essere usata in nessun altro sistema. In caso di dubbio, consultare gli Amministratori di sistema.

4. Qualora la persona autorizzata abbia notizia o timore che la propria password abbia perso la propria riservatezza deve modificarla immediatamente, avvertendo gli Amministratori di sistema.

4. Traccia dei dati riservati

La cancellazione di un file da un supporto non comporta l'effettiva cancellazione delle informazioni in esso contenute: in altre parole, i dati non vengono effettivamente cancellati ma soltanto marcati come non utilizzati e sono facilmente recuperabili. Neanche la formattazione assicura l'eliminazione effettiva dei dati; solo l'utilizzo di un programma apposito (da richiedere agli Amministratori di sistema) garantisce che sul supporto non resti traccia dei dati precedenti.

5. Utilizzo di elaboratori portatili

I PC portatili sono un facile bersaglio per i furti. Se una persona autorizzata ha necessità di gestire dati riservati su un portatile, è necessario salvare i documenti contenenti tali dati con password di protezione, ovvero, in caso di dati particolarmente riservati, è consigliabile l'utilizzo di un programma di cifratura del disco rigido. In tali circostanze sarà inoltre necessario procedere al salvataggio di backup dei dati in rete, al fine di garantire il loro recupero in caso di dimenticanza della password o di perdita del sistema di decriptazione.
I PC portatili sono un bene aziendale per cui è vietato installare qualsivoglia programma e/o software diverso da quelli installati all'origine dall'Amministratore di sistema. È vietato altresì modificare, alterare e/o eliminare le misure di sicurezza di cui è stato dotato il PC (es. antivirus).
Gli utenti sono tenuti ad assicurare che, durante la loro assenza dal posto di lavoro, le apparecchiature a loro assegnate siano in condizioni di sicurezza attuando, ove applicabili, le seguenti precauzioni:

- non lasciare visualizzate informazioni aziendali riservate;
- bloccare il personal computer con il comando Ctrl-Alt-Canc e selezionare "blocca"
- conservare in luogo sicuro i supporti magnetici contenenti i dati sensibili o particolarmente riservati;
- chiudere a chiave l'apparecchiatura quando sono disponibili appositi meccanismi.

6. Divieto di utilizzo del computer da parte di personale esterno

Salvo il caso di espressa autorizzazione da parte degli Amministratori di Sistema, personale esterno non autorizzato non deve accedere ad elaboratori aziendali. In caso di interventi di manutenzione (installazione di nuovo software/hardware nel computer), il soggetto autorizzato dovrà assicurarsi dell'identità della persona e delle autorizzazioni ad operare sul PC.

7. Divieto di installazione e utilizzazione di apparecchi non autorizzati

L'installazione e l'utilizzo di apparecchi non autorizzati (in particolare apparecchi di comunicazione quali modem e schede di rete e fax) su postazioni di lavoro collegati alla rete LAN aziendale offre una porta d'accesso dall'esterno non solo al computer, ma a tutta la rete aziendale senza protezioni.

Tale circostanza, espone a rischio di accesso abusivo tutti gli apparati e gli elaboratori connessi in rete e rende vani gli investimenti tecnologici effettuati dall'organizzazione per garantire la sicurezza di tutti gli asset del sistema informativo (firewall, sistemi di intrusion detection, ecc.).

È quindi vietata l'installazione da parte delle persone autorizzate/utenti di apparecchi non autorizzati dagli Amministratori di sistema in elaboratori aziendali. Per l'installazione e/o l'utilizzo di apparecchi originariamente non implementati nell'elaboratore affidato alla persona autorizzata/utente, quest'ultimo potrà farne richiesta al proprio Responsabile d'Ufficio e al Responsabile per i Sistemi informativi ed ottenere da questi specifica autorizzazione, sulla base delle vigenti procedure aziendali.

L'installazione dovrà essere curata dal personale tecnico autorizzato, in base alle vigenti procedure di sicurezza.

8. Divieto di utilizzazione di programmi non autorizzati

L'elaboratore è consegnato alla persona autorizzata con alcuni programmi preinstallati. Tali programmi permettono l'esecuzione delle operazioni di trattamento cui è preposta la persona autorizzata. Solo tali programmi e/o quelli successivamente installati dagli Amministratori di sistema, previa verifica della licenza d'uso, sono autorizzati.

Qualora per l'espletamento delle proprie mansioni sia necessario o utile l'utilizzo di programmi specifici, i soggetti autorizzati dovranno fare richiesta al Responsabile dell'area – tramite il proprio Responsabile d'Ufficio – ed ottenere da questi specifica autorizzazione, sulla base delle vigenti procedure aziendali.

L'installazione dovrà essere curata dal personale tecnico autorizzato, in base alle vigenti procedure di sicurezza. In ogni caso, è assolutamente vietata l'installazione di programmi sugli elaboratori da parte delle persone autorizzate e ciò a prescindere dal tipo di licenza (shareware o freeware) che ne regolamenti l'utilizzo.
Resta inteso poi che i programmi installati sugli elaboratori dovranno essere utilizzati per svolgere le proprie mansioni lavorative e non per un utilizzo personale.

9. Linee guida per la prevenzione delle infezioni da Virus

La prevenzione dalle infezioni da virus è molto più facile e comporta un impiego di tempo molto minore della correzione degli effetti di un virus; tra l'altro, permette di evitare conseguenze quali la perdita irreparabile di dati.
Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

Come si trasmettono i virus degli elaboratori

I virus si trasmettono:

- Attraverso programmi provenienti da fonti non ufficiali;
- Attraverso le macro dei programmi di automazione d'ufficio;
- Attraverso mail o risorse Internet.

Quando il rischio è alto

Il rischio di infezione da virus informatici è più elevato:

- Quando si installano programmi;
- Quando si copiano dati da supporti esterni quali chiavi USB, CD rom ecc.;
- Quando si scaricano dati o programmi da Internet;
- Quando si aprono allegati provenienti da mittenti sconosciuti e/o non sicuri.

Effetti dei virus

Gli effetti tipici dei virus posso essere rappresentati dal fatto che:

- Effetti sonori e messaggi sconosciuti appaiono sul video;
- Nei menù appaiono funzioni extra finora non disponibili;
- Lo spazio disco residuo si riduce inspiegabilmente;
- Alcuni documenti vengono cancellati o rinominati.

Come prevenire i virus

Di seguito vengono evidenziate alcune linee guida per la prevenzione da virus informatici.

Utilizzare soltanto programmi installati dagli Amministratori di Sistema

Copie non ufficiali di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. È vietato l'uso di programmi non autorizzati (es. videogiochi spesso utilizzati per veicolare virus).

Sottoporre a scansione i supporti removibili

Prima di utilizzare o recuperare un file da un supporto removibile sottoporlo a scansione tramite il software antivirus, a maggior ragione se il supporto proviene dall'esterno dell'azienda. In ogni caso, non utilizzare mai un supporto removibile quando la sua provenienza non sia più che certa ed affidabile.

Utilizzo di Software antivirus aggiornati

La tempestività nell'azione di bonifica è essenziale per limitare i danni che un virus può causare; inoltre è vitale che il programma antivirus conosca gli ultimi aggiornamenti sulle "impronte digitali" dei nuovi virus. Questi file di identificativi sono rilasciati, di solito, con maggiore frequenza rispetto alle nuove versioni dei motori di ricerca dei virus. Su tutti gli elaboratori deve essere quindi installato ed attivo un software antivirus, che deve essere continuamente aggiornato. Questa regola rappresenta una misura minima di sicurezza imposta per legge. È fatto quindi assoluto divieto di disattivare e o modificare detto software. Il personale preposto alla gestione dei sistemi informativi provvede a curare un sistema di aggiornamento automatico degli antivirus installati sulle macchine assegnate alle persone autorizzate/utenti e ad effettuare verifiche in merito. Qualora una persona autorizzata/utente si accorgesse del mancato funzionamento od aggiornamento del software antivirus installato sul proprio elaboratore è pregato di darne immediata comunicazione personale preposto alla gestione dei sistemi informativi.

10.Politica locale relativa ai back-up

Come regola generale, le persone autorizzate devono salvare i documenti utilizzati per finalità lavorative nella rispettiva directory di rete, evitando il salvataggio degli stessi sui dischi fissi degli elaboratori.

Qualora le persone autorizzate abbiano documenti salvati sui dischi fissi è necessario che gli stessi almeno settimanalmente effettuino un salvataggio in rete dei medesimi documenti (i dati custoditi in rete, infatti, vengono quotidianamente sottoposti a procedure di backup). In ogni caso, si ricorda, i files contenenti dati sensibili (stato di salute, vita sessuale, opinioni politiche, religiose, sindacali, origini razziali o etniche, dati provenienti dal casellario giudiziale) devono essere salvati in rete e, qualora salvati su diversi supporti, protetti con password di accesso al documento, ovvero cifrati.

La persona autorizzata che, contravvenendo a quanto sopra, salvi dei dati sul proprio disco fisso sarà completamente responsabile della perdita di dati aziendali in caso di guasti al proprio elaboratore.