

**REGIONE SICILIANA**  
**CEFPAS**  
**CENTRO PER LA FORMAZIONE PERMANENTE**  
**E L'AGGIORNAMENTO DEL PERSONALE DEL SERVIZIO SANITARIO**  
**CALTANISSETTA**

N. 474

**DELIBERAZIONE DEL DIRETTORE DEL CENTRO**

OGGETTO: Adozione Piano per la Sicurezza Informatica (PSI) del CEFPAS

L'anno duemilasedici il giorno 3 del mese di maggio, presso la sede del CEFPAS in Caltanissetta, via Mulè n. 1,

**IL DIRETTORE DEL CENTRO**

Dott. Angelo Lomaglio, nominato con D.P.reg. 5 maggio 2014, n. 138, procede alla adozione della presente deliberazione:

VISTA la legge 23.12.1978, n. 833, istitutiva del S.S.N.;

VISTA la legge regionale 3.11.1993, n. 30, istitutiva del Centro;

VISTO lo Statuto del Centro adottato con deliberazione consiliare n. 1 del 20 settembre 1997, modificato con deliberazione del C.d.A. 12 luglio 2000, n. 20, e approvato con Decreto Assessore per la Sanità 14/03/2001, n. 34145;

VISTO il decreto legislativo 12 febbraio 1993, n. 39, recante norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dell'articolo 2, comma 1, lettera *mm*), della legge 23 ottobre 1992, n. 42

VISTO il decreto legislativo 30 giugno 2003, n. 196, recante codice in materia di protezione dei dati personali;

VISTO il D.P.C.M. 3 dicembre 2013 Regole tecniche per il protocollo informatico;

VISTA la nota di trasmissione del Sistema Informativo Aziendale numero prot. 4270 del 29/04/2016 e il Piano per la Sicurezza Informatica ad essa allegato;

CONSIDERATO che le recenti disposizioni normative accrescono gli obblighi delle Pubbliche amministrazioni in tema di sicurezza e rispetto delle norme della privacy;

CONSIDERATO che il Piano di sicurezza Informatica è composto di due parti una pubblica ed una riservata;

SENTITI i pareri favorevoli del direttore amministrativo e del direttore della formazione, per le motivazioni di cui in premessa,

**DELIBERA**

1



Di approvare il "Piano per la Sicurezza Informatica" facente parte integrante del presente provvedimento.

Dare atto che il presente provvedimento non comporta oneri aggiuntivi di spesa per il Centro.

Di rendere pubblico il Piano di Sicurezza Informatica escludendo le schede tecniche allegate.

Dare mandato ai Direttori delle aree Amministrativa e Formazione di dare diffusione ai dipendenti del Centro della parte pubblica del "Piano per la Sicurezza Informatica" e in particolare far si che gli stessi possano osservare i comportamenti e le regole illustrati nel paragrafo 9.

  
IL DIRETTORE DEL CENTRO  
(Dott. Angelo Lomaglio)

PARERE DEL DIRETTORE AMMINISTRATIVO

FAVOREVOLE

NON FAVOREVOLE

IL DIRETTORE AMMINISTRATIVO (Dott. Calogero Muscarnera) 


PARERE DEL DIRETTORE DELLA FORMAZIONE

FAVOREVOLE

NON FAVOREVOLE

IL DIRETTORE DELLA FORMAZIONE (Dott. Pier Sergio Caltabiano) 

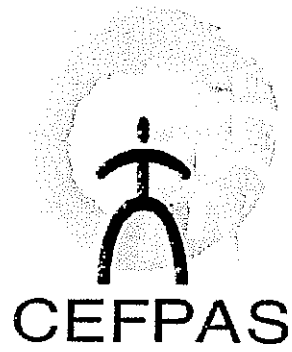
Il funzionario istruttore

(Dott.ssa Alessandra Catino) 

ANNOTATA AL N.

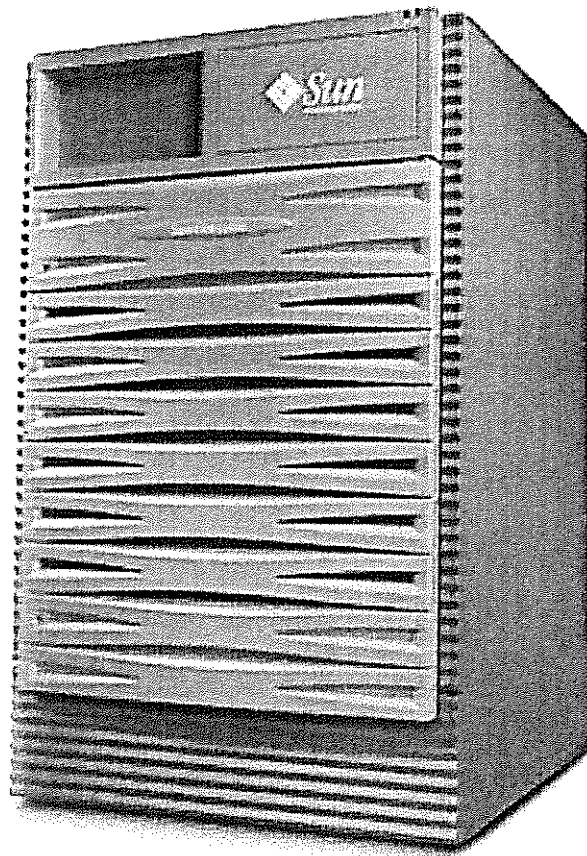
Si certifica che la presente deliberazione è stata pubblicata nell'albo di questo ente dal \_\_\_\_\_ al \_\_\_\_\_ e che contro di essa non sono state prodotte opposizioni.

Area Funzionale Affari Generali  
Dott.ssa Mariassunta Saia  
giusta delega prot. n. 7296 del 17 luglio 2015



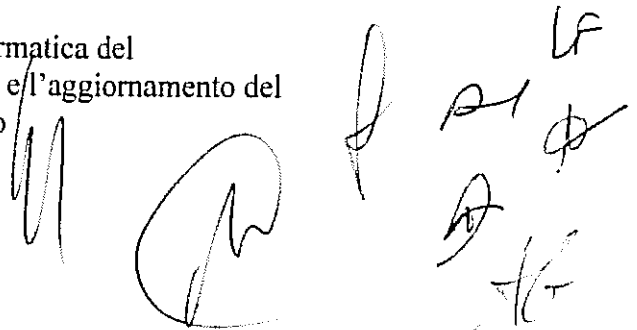
PIANO PER LA SICUREZZA INFORMATICA  
D.Lgs. n.196 del 30/06/2003

---



---

Piano per la Sicurezza Informatica del  
Centro per la Formazione Permanente e l'aggiornamento del  
Servizio Sanitario  
- CEFPAS -  
(PSI)



## PREMESSA

Il presente documento viene redatto dal SIA, dietro incarico della Direzione Aziendale, al fine di definire le regole per l'utilizzo di strumenti informatici e dei dati riguardanti i corsisti, docenti e personale interno nonché dei collaboratori/fornitori e tutti i soggetti con i quali l'Ente intrattiene rapporti giuridici. Tutto al fine di ottenere maggiore "sicurezza" nei suoi aspetti fondamentali, in termini di integrità, riservatezza e disponibilità dei dati.

Si devono quindi definire ed adottare adeguate misure tecnologiche e organizzative affinché:

- i dati riservati trattati siano protetti nei riguardi di ogni tipo di accesso e di consultazione illeciti. In questi casi, deve essere possibile risalire con certezza all'autore degli stessi;
- tutti i dati trattati siano protetti da modifiche non autorizzate. Nel caso in cui comunque questo evento dovesse verificarsi, è necessario che siano state prese misure preventive atte a ripristinare il dato al suo valore corretto, ed individuare inequivocabilmente l'autore delle modifiche;
- i dati siano disponibili a chi ne ha la facoltà di consultarli con un livello di disponibilità non inferiore a quanto concordato con i rispettivi responsabili. In caso di guasti o malfunzionamenti devono essere messe in atto tutte le contromisure per garantire il ripristino tempestivo degli stessi.

A tal fine si fa presente che l'ente ha in corso di definizione un piano di aggiornamento tecnologico hardware/software che si inquadra nella più ampia riorganizzazione aziendale volta, quest'ultima, a potenziare e migliorare la qualità, l'efficienza e la sicurezza dell'intera infrastruttura tecnologica. Al contempo appare necessario avviare un'attività di formazione e informazione per tutte le figure dirigenziali e non, del Centro in vista di nuove scelte e investimenti concernenti la gestione della sicurezza tecnologica e per rendere tutto il personale aziendale consapevole, in misura adeguata alle mansioni svolte, dei rischi che comporta l'uso improprio delle tecnologie informatiche. Il personale del Cefpas sarà dotato di un codice scritto che indichi i comportamenti corretti da adottare e le attività da svolgere in caso di mal funzionamento o guasto come previsto al capitolo 9 del presente PSI.

Il raggiungimento di questi obiettivi richiede, pertanto, non solo l'utilizzo in tempi brevi dei nuovi ed appropriati strumenti tecnologici richiesti ma anche di opportuni meccanismi organizzativi; misure soltanto tecniche, per quanto sofisticate, non saranno efficienti se non usate propriamente. A tal proposito si ricorda che le precauzioni di tipo tecnico cercano di proteggere le informazioni durante il loro transito tra i vari sistemi e, nel momento in cui esse raggiungono gli utenti finali, la loro protezione dipende esclusivamente da questi ultimi; nessuno strumento tecnologico può sostituirsi al senso di responsabilità ed al rispetto delle norme. Si raccomanda pertanto, a tutti gli utenti, di attenersi alle linee guida indicate al par.9 al fine di fare tutto il possibile per la "sicurezza" dei dati ed evitare l'appropriazione indebita di informazioni da parte di terzi.



## 1. OGGETTO DEL PRESENTE DOCUMENTO

Il presente documento costituisce il riferimento interno del Centro per la Formazione Permanente e l'Aggiornamento del Personale del Servizio Sanitario (CEFPAS) in materia di misure di sicurezza per il trattamento dei dati personali, a norma del D.Lgs. n.196 del 30/06/2003.

Si riepilogano di seguito i riferimenti normativi:

- decreto legislativo 12 febbraio 1993, n. 39, recante norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dell'articolo 2, comma 1, lettera mm), della legge 23 ottobre 1992, n. 421;
- D.P.R 28 luglio 1999, n. 318 recante norme per l'individuazione delle misure di sicurezza minime per il trattamento dei dati personali a norma dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675.
- direttiva P.C.M. del 16 gennaio 2002 recante Sicurezza informatica e delle telecomunicazioni;
- decreto legislativo 30 giugno 2003, n. 196, recante codice in materia di protezione dei dati personali;
- D.Lgs. 1 agosto 2003, n. 259 – Codice delle comunicazioni elettroniche
- decreto legislativo 28 febbraio 2005, n. 42, recante istituzione del sistema pubblico di connettività e la rete internazionale della pubblica amministrazione, a norma dell'articolo 10 della legge 23 luglio 2003, n. 229;
- decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale
- decreto legislativo 4 aprile 2006, n. 159 recante disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82
- delibera n. 13 del 1° marzo 2007 del Garante recante le linee guida per posta elettronica e internet
- direttiva 02/09 del 26/05/2009 del Ministro Renato Brunetta
- D.P.C.M. 3 dicembre 2013 Regole tecniche per il protocollo informatico

Il documento viene pertanto redatto per le seguenti finalità:

- individuare i dati trattati mediante strumenti informatici ed il personale che ad essi può o deve accedere per l'espletamento dei propri compiti istituzionali;
- individuare i locali di particolare rilevanza dal punto di vista della conservazione dei dati gestiti tramite strumenti informatici.
- definire l'insieme minimo ed adeguato delle norme di sicurezza necessarie alla protezione dei dati trattati per mezzo di strumenti informatici.

Il contenuto del presente documento verrà periodicamente verificato, modificato ed integrato in modo da garantire la massima sicurezza possibile nel trattamento dei dati memorizzati, compatibilmente alle risorse ed ai mezzi a disposizione del Centro.

E in particolare con riferimento alle funzioni e i compiti assegnati con disposizioni di servizio interne relativamente alla tecnologia hardware, software ed ogni tecnologia informatica in dotazione al Centro

## 2. SISTEMA INFORMATIVO AZIENDALE

Il Sistema Informativo Aziendale (SIA) istituito e reso operativo con disposizione di servizio n.392 del 2015 è il servizio del CEFPAS che supporta tutte le aree, i servizi e gli uffici del Centro fornendo una visione unitaria ed integrata delle informazioni e delle procedure necessarie allo svolgimento delle attività istituzionali. È costituito dall'insieme delle risorse informatiche (hardware, software, infrastrutturali) ed umane e professionali individuate nel SIA, come precisato nella predetta disposizione, alla quale si fa espresso rinvio per l'individuazione delle funzioni e aree di attività presidiate da ciascun componente, anche con riferimento al presente PSI.

## 3. COMPONENTI SISTEMA INFORMATIVO

### 3.1 Hardware

Il Centro dispone di Server, Workstation, notebook, attrezzature di rete, stampanti laser ed inkjet (si rimanda all'inventario per i dettagli - scheda tecnica n.1) dislocati all'interno del Campus (Centro Elaborazione Dati, Centro di Simulazione – CEMEDIS -, Hotel, padiglioni ed aule didattiche). Per i dettagli tecnici sulla toponomastica di rete si rimanda alla scheda tecnica n.2.

### 3.2 Software

Il Centro dispone dei seguenti prodotti software che generano i dati necessari allo svolgimento delle proprie attività istituzionali:

- a. Software per il rilevamento delle presenze del personale dipendente - JobTIME;
- b. Software per la gestione della contabilità analitica per centri di costo - Oliamm;
- c. Software per la gestione della Banca Dati corsisti, docenti e corsi – Access interno;
- d. Software di gestione alberghiera – Nuconga;
- e. Software Protocollo - DigitalPro;
- f. CMS per la gestione delle piattaforme e-learning FAD – Moodle
- g. CMS Joomla per la gestione del sito istituzionale
- h. CMS Wordpress per la gestione del portale della Trasparenza (trasparenza.cefpas.it)

Le procedure informatiche in uso producono dati che vengono immagazzinati su supporti magnetici situati sui server. Le operazioni di backup vengono effettuate differentemente in base ai servizi erogati come descritto al capitolo 5 e nella scheda tecnica n.1.

L'accesso ai server avviene in maniera autenticata da dispositivi per la maggior parte dotati di sistema operativo di tipo Microsoft Windows.

Al CEMEDIS è annesso un laboratorio multimediale, interfacciato alla rete centrale con collegamento in fibra.

### 3.3 La Rete aziendale

La rete del centro è gestita dai periti informatici del SIA che si occupano di effettuare le quotidiane attività di gestione e manutenzione ed intervengono, in caso di guasti e/o malfunzionamenti, limitatamente alle loro competenze utilizzando le attrezzature di diagnostica in loro possesso.

La parte di rete in fibra, viene gestita con incarico a ditta specializzata esterna.

I PC in rete LAN accedono ad Internet in maniera centralizzata attraverso un server proxy, a seguito di procedura di autenticazione utente attraverso il PDC (Primary Domain Controller). L'attuale implementazione necessita però di un urgente piano di riammodernamento poiché i

sistemi hardware e software attualmente in uso non sono più idonei a garantire buoni livelli di performance e sicurezza.

#### 4. RUOLI ED ACCESSI

Ai fini del presente documento sono considerate rilevanti tre diverse tipologie di personale, caratterizzate dalla possibilità di accesso su diversi livelli di autorizzazione al sistema informatico e precisamente:

- I periti informatici del SIA ;
- I dipendenti e collaboratori del Centro;
- Il personale di aziende esterne, addetto alla manutenzione.

##### 4.1 I periti informatici del SIA

Sui periti informatici del SIA ricadono le funzioni descritte nella disposizione di servizio n.392 del 2015 e sono coloro i quali mettono in atto tutte le attività espressamente definite in questo documento.

##### 4.2 Dipendenti e collaboratori del Centro

I dipendenti del Centro accedono alla rete del sistema informativo, dalle postazioni a loro assegnate, a seguito di procedura di autenticazione, inserendo nome utente e password. L'accesso ai dati e la tipologia delle operazioni consentite sugli stessi dipende dal livello di autorizzazione a loro concesse, distinte secondo ruoli, funzioni ed aree di appartenenza.

##### 4.3 Altre figure aventi accesso al Sistema

L'accesso al sistema informatico è consentito anche al personale tecnico delle Aziende fornitrici di software a cui spetta la manutenzione e l'aggiornamento degli stessi. Ad oggi, hanno accesso i tecnici relativamente ai software di contabilità e gestione timbrature e paghe.

#### 5. I DATI DEL CENTRO.

I software e le procedure in uso al Centro, generano, gestiscono e memorizzano i dati in formato elettronico. Questi risiedono generalmente:

1. sulle singole postazioni del dipendente;
2. sulle cartelle personali in rete associate a ciascun dipendente, il cui accesso è esclusivo del dipendente e degli operatori del SIA;
3. su cartelle comuni presenti sui NAS. L'accesso è determinato dalle funzioni svolte dal personale assegnato alle distinte aree funzionali, impostato dal SIA secondo le direttive ricevute dalla direzione;
4. sui server che ospitano e gestiscono i vari servizi Cefpas.

Al fine di garantire l'integrità, disponibilità ed accessibilità dei dati, gli stessi sono soggetti a copie di sicurezza ad opera del SIA, che vengono memorizzate in un apposito PC dotato di n.2 hard disk ubicato al CED (dati di cui al punto 2 e 3). La copia di salvataggio, tenuto conto della quantità di dati, viene effettuata a cadenza quindicinale. Il backup dei dati di cui al punto 4 sono differenziati per servizio. Per il dettaglio si rimanda alla scheda n.1. I dati di cui al punto 1 non sono oggetto di copie di sicurezza.

A seguito di distruzione o danneggiamento degli stessi, gli operatori del SIA ripristinano la copia di sicurezza più recente.

Quadro riassuntivo e completo delle informazioni inerenti i dati presenti in Azienda.

TABELLA N.2 SINOTTICA DEI DATI DEL CENTRO						
	Gestione Presenze	Contabilità Aziendale	Procedura Paghe	Flussi informativi	Dati Corsisti	Dati Albi
Esistenza di Dati Sensibili	x	x	x		x	
Archivio Centralizzato	x	x	x		x	
Esistenza di copie locali				x		x
Ubicazione dei dati (Copia originale)	x	x	x	x	x	x
Esistenza di dati inviati all'esterno del Centro	x		x	x		

## 6. PROTEZIONE DEI LOCALI

Le specifiche sono riportate nella Scheda n.3

## 7. CRITERI E PROCEDURE PER GARANTIRE L'INTEGRITA' DEI DATI.

L'accesso alle procedure informatiche ed ai relativi dati sono protette da autenticazione tramite password di accesso. Per la maggior parte dei software è possibile consentire un accesso differenziato in base ai permessi concessi all'utente. Nei successivi paragrafi viene fornita una descrizione dettagliata delle misure di sicurezza adottate.

### 7.1 Trattamento dati con strumenti elettronici.

I dati utilizzati dal software "Banche Dati" ed il relativo database risiedono sull'unità NAS del Centro, il cui accesso avviene tramite user-name e password dell'utente di dominio .

La password di Amministratore è nota ai periti informatici del SIA e agli operatori esterni abilitati alla manutenzione (vedi capitolo 4.3 ).

L'accesso ai computer locali è sempre protetto da password. Il 100% dei PC utilizzati consente l'utilizzo di una doppia password (Amministratore ed User) in modo da garantire l'accesso agli addetti alle operazioni di manutenzione, inoltre è obbligatorio il cambio password da parte dei dipendenti ogni 90 gg per i dati sensibili che contengono i loro pc. Le passwords devono rispettare alcune regole particolari come la lunghezza maggiore di 7 caratteri alfanumerici, nessun riferimento ad elementi identificativi facilmente intuibili.

## 8. DATI E PROCEDURE INERENTI IL LORO TRATTAMENTO

Le tipologie di dati presenti in azienda possono essere raggruppate in:

- Dati corsisti: I dati dei partecipanti ai corsi sono presenti nel Centro nella duplice modalità di cartacea ed elettronica. I dati "in cartaceo" sono rappresentati dalle schede d'ingresso e vengono gestiti principalmente dalla "SAF" - Segreteria Attività Formative - e dal personale autorizzato, ovvero dal personale assegnato all'attività



corsuale. I dati "elettronici" pervengono al Centro tramite appositi form online e vengono gestiti tramite apposite banche dati.

- Dati Docenti/Referenti/Tutor: I dati dei docenti/referenti/tutor pervengono al Cefpas tramite appositi sistemi di registrazione online che li memorizza in banche dati dedicate.
- Dati dipendenti: I dati dei dipendenti risiedono nel Centro in formato elettronico sui vari sistemi di gestione.
- Collaboratori e fornitori: I dati di questa categoria risiedono nel Centro in formato elettronico sui vari sistemi di gestione.

### 8.1 Computer accessibili in Rete

Per i computer accessibili tramite rete, valgono considerazioni analoghe a quelle effettuate al precedente paragrafo 7.1. Per quanto riguarda il software installato su di essi, è sempre necessario, per poter accedere al sistema, identificarsi mediante un nome-utente ed una password.

### 8.2 Rete interna ed Accesso a Dati Particolari.

Gli utenti preposti al trattamento di dati particolari (sensibili e/o comunque riservati) dispongono di una propria "user-name" e password per la verifica dell'identità.

Le credenziali per l'accesso alla rete aziendale sono rilasciate dal SIA, invece le credenziali per l'accesso agli applicativi sono rilasciate dalle figure specificate nella Scheda n.4.

### 8.3 Rete accessibile dall'esterno

Il Sistema Informativo del Cefpas, tramite tecnologia di accesso remoto può interfacciarsi con l'esterno per le attività di manutenzione e/o aggiornamento degli applicativi.

## 9. COMPORTAMENTI E REGOLE A CUI BISOGNA ATTENERSI

### - Spegnere il computer se ci si assenta per un periodo di tempo lungo.

Lasciare un computer acceso non crea problemi al suo funzionamento e velocizza il successivo accesso. Tuttavia, un computer acceso è in linea di principio maggiormente attaccabile perché raggiungibile tramite la rete o direttamente sulla postazione di lavoro. Inoltre, più lungo è il periodo di assenza, maggiore è la probabilità che nel frattempo avvenga un'interruzione dell'energia elettrica che possa portare un danno all'elaboratore, alla sua configurazione o al documento stesso.

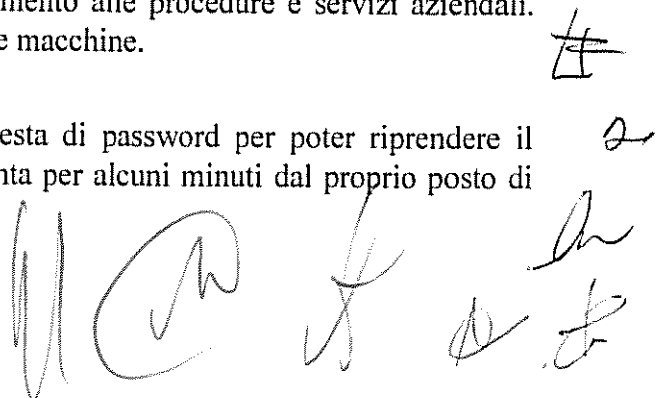
### - Manutenzione Hardware e Software

Ove possibile, tutti i PC sono stati dotati di una installazione di base che comprende vari software. Non è permesso modificare o rimuovere queste installazioni. Nel caso in cui sia necessaria la modifica di questo ambiente, tale intervento deve essere richiesto al SIA ed eseguito solo dopo autorizzazione. Analogamente non è permesso modificare o rimuovere le configurazioni hardware senza preventiva autorizzazione. Non è consentito lo spostamento di PC o parti di esso in altro luogo dove è stato collocato senza preventiva autorizzazione, al fine di evitare malfunzionamenti e mancanza di collegamento alle procedure e servizi aziendali. Non è consentita la disabilitazione dell'antivirus sulle macchine.

### - Impostare il salvaschermo

E' importante impostare il salvaschermo con richiesta di password per poter riprendere il controllo della postazione; in tal modo se ci si assenta per alcuni minuti dal proprio posto di lavoro, il PC diventi inutilizzabile.

### - Cambio delle password e loro scelta



Cambiare periodicamente le proprie password di accesso, anche nelle applicazioni dove non si è obbligati a farlo. Tutte le password devono essere scelte in modo tale da essere difficili da indovinare; evitare le solite date di nascita, numeri di telefono, nomi di familiari o del cane, etc.. E' sconsigliabile anche l'utilizzo di parole che sono contenute nei dizionari (italiano, inglese, etc.) in quanto con alcuni programmi è possibile "provare" tutte le password e, quelle contenute in dizionari, sono le prime ad essere tentate. In generale è preferibile una password non "debole", composta da una sigla non banale di almeno 8 caratteri, che comprenda lettere, numeri e simboli interpunzione. Non utilizzare la stessa password per sistemi o programmi differenti, o password già utilizzate in precedenza.

- **Account di accesso**

L'accesso ai Server o in generale al dominio, come quello di ogni programma critico, richiede di identificarsi a mezzo di un nome utente ed una password. Le operazioni vengono registrate (file di LOG) tenendo traccia dell'utente che le ha eseguite e quindi in base all'account utilizzato. Ogni utente deve avere l'accortezza di non permettere ad altri di utilizzare le proprie chiavi di accesso, anche per non rendersi responsabile di operazioni non eseguite personalmente. Nel caso si stia utilizzando una stazione di lavoro e si intenda passare a lavorare su una differente, l'utente è tenuto a chiudere le applicazioni e le sessioni di lavoro aperte sul suo computer ed autenticarsi sull'altro sempre con le proprie credenziali.

- **Uso di computer ed account per personale esterno.**

La consultazione dei sistemi da parte di personale esterno in generale non deve essere permessa. Nel caso che personale esterno debba installare del nuovo software o hardware (schede o apparecchiature) sulla postazione di lavoro di un utente, l'operazione deve essere permessa solo in presenza dello stesso utente.

- **Condivisioni**

Al fine di limitare la diffusione di virus, furti e danneggiamenti di documenti, problemi di funzionamento delle stazioni di lavoro, è fatto espressamente divieto di condividere il disco fisso del proprio computer o anche solo parte di esso. Nel caso vi siano delle esigenze di condividere documenti e/o dati, deve essere fatto presente agli addetti al SIA che provvederanno ad analizzare il problema e, qualora possibile e consentito dalle normative vigenti, verrà creata una apposita area di scambio con le opportune protezioni.

- **Utilizzo di Modem, Internet Key e dispositivi "Mobile" come telefonini o smartphone per accesso alla rete Internet**

Il loro utilizzo è vietato qualunque sia il loro impiego in quanto, con tali apparecchi, si crea un punto di accesso non controllato e aperto al mondo esterno, che può rendere maggiormente vulnerabile non solo le postazioni di lavoro su cui sono collegate, ma l'intera rete. Nel caso fossero necessarie connessioni con l'esterno, si devono richiedere le necessarie abilitazioni. L'installazione dei dispositivi, ove indispensabile, deve essere eseguita a cura del personale tecnico, ed esclusivamente previa autorizzazione ed espressa approvazione che certifichi l'impossibilità di raggiungere i medesimi obiettivi in modi maggiormente sicuri.

- **Utilizzo di access point wireless**

Il loro utilizzo è generalmente vietato e autorizzabile solo in presenza di un adeguato livello di crittografia (chiave WEP/WPA/WPA2). Con tali apparecchi, si può creare un punto di accesso non controllato e aperto al mondo esterno, che può rendere maggiormente vulnerabile non solo le postazioni di lavoro su cui sono collegate, ma l'intera rete. L'installazione, ove indispensabile, deve essere eseguita a cura del personale tecnico, ed esclusivamente a seguito

di autorizzazione che certifichi l'impossibilità di raggiungere i medesimi obiettivi in modi maggiormente sicuri.

- **Altre apparecchiature**

E' fatto divieto agli utenti di collegare, o permettere ad altri di farlo, qualsiasi tipo di apparecchiatura sulle porte seriali, parallele, USB, etc. di qualsiasi elaboratore o apparato di rete. E' permessa l'installazione solo dei kit per la firma digitale e di stampanti purché non siano collegate, in alcun modo, a linee telefoniche (ad es: stampanti multifunzioni, fax).

- **Virus informatici**

Su ogni personal computer è installato un programma antivirus che viene automaticamente aggiornato. E' tuttavia compito dell'utente accertarsi che venga eseguito correttamente, che non siano prodotti messaggi di mal funzionamento o di presenze di virus informatici, oltre ad accertarsi che avvengano realmente gli aggiornamenti e che il programma sia "attivo" per il controllo del sistema. Nel caso si vogliano modificare le configurazioni del software antivirus è necessario prima contattare il personale tecnico. Gli utenti sono invitati a lanciare periodicamente dei controlli su tutto il disco locale del proprio computer. Nel caso si riscontrino delle anomalie o dei virus, deve essere contattato il personale informatico per le opportune verifiche. Si ricordi che la prevenzione dalle infezioni da virus su un computer è molto più facile e comporta uno spreco di tempo molto minore rispetto alla correzione degli effetti di un virus.

- **Fonti di dati, uso di internet**

Gli utenti devono utilizzare i computer in dotazione per assolvere il proprio lavoro e devono pertanto utilizzarli per accedere ad informazioni inerenti le proprie mansioni. Non si devono quindi copiare o "scaricare" programmi, file musicali, video, immagini con contenuti pornografici, file protetti da diritto d'autore, licenze d'uso, etc. dalla rete internet o da altre fonti. Non si debbono visitare siti illegali (ad esempio depositi di software pirata) e non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

- **Posta elettronica, diffidare di dati, programmi, messaggi**

Gli utenti non devono aderire, con la posta elettronica, a "catene di Sant'Antonio" nelle loro varie forme e versioni. È necessario prestare attenzione ai messaggi ricevuti anche se sembrano provenire da persone conosciute. Non aprire gli allegati se non attesi, soprattutto se si tratta di programmi eseguibili e, in ogni caso, controllarli con antivirus aggiornati.

- **Dati e programmi provenienti dall'esterno:**

Come per la posta elettronica, è buona norma diffidare di tutti i dati e programmi che si ricevono, anche se la fonte appare affidabile o il contenuto molto interessante; si applicano quindi le stesse precauzioni.

- **Uso di computer e rete:**

Possono essere utilizzati solo computer da tavolo e portatili di proprietà dell'Azienda o altri pc con espressa autorizzazione del Dirigente; possono essere collegati alla rete locale solo i computer che sono stati opportunamente configurati dal personale informatico aziendale e, per tutto il tempo in cui sono connessi alla rete locale, devono essere utilizzati esclusivamente dai dipendenti. Ogni altro accesso alla rete deve essere preventivamente richiesto ed autorizzato.

- **Uso di altri computer**

Il personale NON deve permettere, a persone non dipendenti, il collegamento dei propri computer, anche se portatili, o altri apparati elettronici di qualsiasi natura, sia alle reti

fonia/dati che ai computer in dotazione presso questi uffici, nonostante ci sia un motivo apparentemente valido. In tale modo si cercano di limitare i rischi relativi a conflitti di configurazioni ed alle intercettazioni di comunicazione e dati.

- **Installazioni di nuovi programmi**

E' fatto divieto agli utenti di installare qualsiasi tipo di software, in particolar modo giochi e programmi che permettano condivisioni di file. Tutte le installazioni di programmi devono essere effettuate esclusivamente a cura o con l'ausilio del personale tecnico del SIA e comunque richieste ed autorizzate dall'Amministrazione, in quanto le licenze di utilizzo dei programmi devono essere conteggiate e, se necessario, acquistate.

I periti informatici del SIA possono procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza sia sui singoli personal computer sia sulle unità di rete. Per esigenze organizzative, produttive e di sicurezza gli stessi possono avvalersi di strumenti che consentono un controllo a distanza di tipo generalizzato, indiretto e anonimo, relativo all'intera struttura amministrativa, ad aree, settori o gruppi di utenti.

Qualora durante un controllo generalizzato, vengano rilevate anomalie nell'utilizzo degli strumenti informatici, l'Amministrazione del Centro procede preliminarmente all'invio di un avviso generalizzato relativo all'uso improprio riscontrato, con l'invito ad attenersi scrupolosamente al presente regolamento, e riservandosi la facoltà di svolgere successive azioni mirate alla verifica del corretto utilizzo.

