UNIVERSITÀ DEGLI STUDI DI CATANIA

Vademecum per la sicurezza dei dati personali dell Università di Catania

D.Lgs. 196/2003 - Codice della Privacy

Introduzione

La privacy e l'applicazione del D.Lgs. 196/2003 sono divenuti temi che coinvolgono tutte le pubbliche amministrazioni, le quali devono provvedere ad informare i soggetti che operano nell'ambito dell'organizzazione sulle regole di comportamento da tenere a tutela dell'utenza interna ed esterna e dei suoi dati; pertanto, la presente guida riassume alcune delle regole comportamentali che si sono configurate come uno standard comune per diverse amministrazioni.
Questo documento intende fornire a tutti i soggetti che trattano dati personali in Ateneo le prime linee guida e un promemoria sui comportamenti essenziali da tenere nel luogo di lavoro per garantire la corretta gestione della sicurezza dell'informazione.

Il termine "sicurezza" si riferisce a tre aspetti distinti:
Riservatezza: Prevenzione contro l'accesso non autorizzato alle informazioni;
Integrità: Le informazioni non devono essere alterabili da incidenti o abusi;
Disponibilità: Il sistema deve essere protetto da interruzioni impreviste.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche opportuni meccanismi organizzativi; infatti, le sole misure tecniche, per quanto possano essere sofisticate, non saranno efficienti se non usate propriamente.
In particolare, le precauzioni di tipo tecnico possono proteggere le informazioni durante il loro transito attraverso i sistemi, o anche quando queste rimangono inutilizzate su un disco di un computer; nel momento in cui esse raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle norme.

Linee guida generali per la sicurezza

Utilizzate le chiavi
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 non banale per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania; pertanto alla fine della giornata chiudete a chiave il vostro ufficio e chiudete i documenti a chiave nei cassetti.

Accesso alle risorse informatiche
La sicurezza logica si realizza assicurando che tutti gli accessi ai diversi componenti del sistema informativo dell'Ateneo avvengano esclusivamente secondo modalità prestabilite. Per tale motivo, ogni qual volta si rende necessario l'utilizzo di una risorsa informatica, deve essere presente un meccanismo che costringa l'utente ad autenticarsi, ossia a dimostrare la propria identità, mediante ***credenziali di autenticazione*** che, tipicamente, sono costituite da un codice identificativo personale, ***userid***, ed una parola chiave, ***password*** (vedi: Linee guida per il corretto utilizzo delle password).

Conservate i supporti rimovibili (dischetti, cd, chiavi USB ecc) in un luogo sicuro
Per i supporti rimovibili si applicano gli stessi criteri che per i documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può

passare più facilmente inosservato. A meno che non siate sicuri che contengano solo dati non personali, riponeteli sotto chiave non appena avete finito di usarli.

Spegnete sempre il computer quando vi assentate dall'ufficio per un lungo periodo
Lasciare un computer acceso non crea problemi al suo funzionamento; tuttavia, un computer acceso è in linea di principio raggiungibile tramite la rete o anche direttamente sulla postazione di lavoro. Inoltre, più lungo è il periodo di assenza maggiore è la probabilità che un'interruzione dell'energia elettrica possa arrecare un danno.

Non lasciate lavori incompiuti sullo schermo
Chiudete sempre il programma quando vi allontanate dal posto di lavoro: potreste rimanere lontani più del previsto, e un documento presente sullo schermo è vulnerabile (quasi) quanto uno stampato o copiato su dischetto.

Maneggiate con cura le stampe di documenti riservati
Non lasciate accedere alle stampe persone non autorizzate; se la stampante non si trova sulla vostra scrivania recatevi quanto prima a ritirare le stampe. Distruggete personalmente le stampe quando non servono più.

Prestate attenzione all'utilizzo dei PC portatili
I PC portatili sono un facile bersaglio per i furti. Se avete necessità di gestire dati riservati su un portatile, fatevi installare un buon programma di cifratura del disco rigido, e utilizzate una procedura di backup periodico.

Non fate usare il vostro computer a personale esterno a meno di non essere sicuri della loro identità
Personale esterno può avere bisogno di installare un nuovo software/hardware nel vostro computer. Assicuratevi dell'identità della persona e delle autorizzazioni ad operare sul vostro PC.

Non utilizzate apparecchi non autorizzati
L'utilizzo di modem su postazioni di lavoro collegati alla rete di edificio offre una porta d'accesso dall'esterno non solo al vostro computer, ma a tutta la rete, ed è quindi vietata. Per l'utilizzo di altri apparecchi, consultatevi con l'incaricato dell'amministrazione del sistema.

Non installate programmi non autorizzati
Solo i programmi istituzionali o acquistati dall'Amministrazione con regolare licenza sono autorizzati. Se il vostro lavoro richiede l'utilizzo di programmi specifici, consultatevi con l'incaricato dell'amministrazione del sistema.

Applicate con cura le linee guida per la prevenzione da infezioni di virus
La prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus; tra l'altro, potreste incorrere in una perdita irreparabile di dati.

Effettuare periodicamente copie di sicurezza dei dati (backup)

Si possono verificare degli eventi (p.e. guasti, virus, cancellazioni accidentali) che compromettono il funzionamento del vostro PC e i dati in esso contenuti. Per cui, è opportuno effettuare, ad intervalli regolari e frequenti, delle copie di sicurezza dei dati locali. Questo può essere fatto copiando i dati su supporti removibili (magari mediante opportuni software) o, meglio ancora, trasferendo i dati su un *file server* che può gestire tutti i dati dell ufficio e semplificare le operazioni di backup, effettuate in maniera centralizzata dall incaricato dell amministrazione del sistema.

Mantenete aggiornato il PC

Periodicamente vengono individuati delle vulnerabilità (difetti, bug) del sistema operativo (p.e. windows) o dei software più comuni (p.e. Office), per cui, le case produttrici rilasciano degli aggiornamenti per proteggere il PC da attacchi via rete o da virus che utilizzano proprio questi bug per diffondersi. Quindi, è indispensabile avere aggiornato il proprio PC. A tale scopo esistono dei servizi automatici (Windows Update, Office Update) per verificare che il sistema sia aggiornato e, in caso contrario, permettono di aggiornarlo. Verificate la situazione con l incaricato dell amministrazione del sistema.

Linee guida per la prevenzione dei virus

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 trasmette un virus:
Attraverso programmi provenienti da fonti non ufficiali;
Attraverso le macro dei programmi di automazione d'ufficio.

Come *NON* si trasmette un virus:
Attraverso file di dati non in grado di contenere macro (p.e. file di testo);
Attraverso *mail* non contenenti allegati.

Quando il rischio da virus si fa serio:
Quando si installano programmi;
Quando si copiano dati da dischetti;
Quando si scaricano dati o programmi da Internet.

Quali effetti ha un virus?
Effetti sonori e messaggi sconosciuti appaiono sul video;
Nei menù appaiono funzioni extra finora non disponibili;
Lo spazio disco residuo si riduce inspiegabilmente;
Le prestazioni del computer degradano o diventa inutilizzabile;
I dati sono modificati o distrutti.

Come prevenire i virus

Usate soltanto programmi provenienti da fonti affidabili
Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione antivirus prima di essere installato. Non utilizzate programmi non autorizzati che sono spesso utilizzati per veicolare virus.

Assicuratevi di non far partire accidentalmente il vostro computer da dischetto
Infatti se il dischetto fosse infettato, il virus si trasferirebbe nella memoria RAM e potrebbe espandersi ad altri files.

Proteggete i vostri supporti rimovibili da scrittura quando possibile
È il più efficace mezzo di prevenzione. In questo modo eviterete le scritture accidentali, magari tentate da un virus che tenta di propagarsi. I virus non possono in ogni caso aggirare la protezione meccanica.

Assicuratevi che il vostro software antivirus sia aggiornato
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 identificativi sono rilasciati, di solito, con

maggiore frequenza rispetto alle nuove versioni dei motori di ricerca dei virus. Informatevi con l'incaricato dell'amministrazione del sistema per maggiori dettagli.

Non diffondete messaggi di provenienza dubbia

Se ricevete messaggi che avvisano di un nuovo virus pericolosissimo, ignoratelo, qualunque sia la provenienza: i messaggi di posta elettronica di questo tipo, in genere, sono "bufale" (hoax), l'equivalente di leggende metropolitane in rete.

Non partecipate a "catene di S. Antonio" e simili

Analogamente, tutti i messaggi che vi invitano a "diffondere una notizia quanto più possibile" sono *bufale*, aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche.

Linee guida per il corretto utilizzo delle password

Le password

Vi sono svariate categorie di password, ognuna con il proprio ruolo preciso:

a) **la password di accensione del PC** (password di BIOS) impedisce l'utilizzo improprio della propria postazione di lavoro, quando per un qualsiasi motivo non ci si trovi in Ufficio;
b) **la password di rete** impedisce che l'eventuale accesso non autorizzato ad un PC renda disponibili le risorse dell'Ufficio (stampanti, cartelle condivise);
c) **la password delle applicazioni informatiche centralizzate** permette di restringere l'accesso alle funzioni e ai dati al solo personale autorizzato;
d) **la password di protezione delle risorse (cartelle) condivise** impedisce l'accesso a tali risorse da parte di utenti non autorizzati i cui PC siano collegati sulla stessa rete locale ed impedisce la propagazione di virus informatici nella rete locale;
e) **la password della casella di posta elettronica istituzionale** impedisce che i messaggi di posta elettronica indirizzati ad un utente possano essere letti da utenti non autorizzati;
f) **la password del salvaschermo** impedisce che un'assenza momentanea permetta a una persona non autorizzata di visualizzare il lavoro in corso e/o di accedere ai documenti residenti sulla postazione di lavoro.

Imparate a utilizzare questi tipi di password, e mantenete distinta almeno quella di tipo *a)*, che può dover essere resa nota, almeno temporaneamente, ai tecnici incaricati dell'assistenza. Scegliete le password secondo le indicazioni successive.

Come scegliere una password

Il più semplice metodo per l'accesso illecito a un sistema 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.
Le migliori password sono quelle facili da ricordare ma, allo stesso tempo, difficili da indovinare. Questo genere di password può essere ottenuto, ad esempio, comprimendo frasi lunghe in pochi caratteri presenti nella frase, utilizzando anche segni di interpunzione, caratteri maiuscoli e minuscoli, simboli al posto dei caratteri.

La frase "Nel 1969 l'uomo è andato sulla luna" può, ad esempio, fornire tra le tante possibilità la seguente "N69UèAsL".
Accanto a questa tecnica, per ottenere password ancora più "forti", si possono sostituire le lettere risultanti dalla compressione della frase, con cifre o caratteri che assomiglino alle lettere; ad esempio, la frase "Questo può essere un modo per ricordare la password" diventa "Qp&1mpRP".
Un altro modo per ottenere password "forti" consiste nel combinare date o numeri che si ricordano facilmente con pezzi di parole che sono in qualche modo abituali e quindi semplici da ricordare; ad esempio, la combinazione "felice1983", che utilizzata direttamente potrebbe essere una password "debole" (combinazione del nome del figlio e della data di nascita), può diventare una password migliore in questo modo "FeLi83ce", o una password "forte" così "F&Li83cE".
N.B. Non utilizzare come password gli esempi riportati nel presente documento

Non fatevi spiare quando digitate le password
Anche se avete buone capacità di dattiloscrittura, quando digitate la vostra password potrebbe essere letta guardando i tasti che state battendo.

Custodite le password in un luogo sicuro
Non scrivete la vostra password su supporti che possano essere trovati facilmente e soprattutto in prossimità della vostra postazione di lavoro. L'unico affidabile dispositivo di registrazione è la vostra memoria. Se avete necessità di conservare traccia delle password per scritto, non lasciate in giro i fogli utilizzati.

Cosa Fare
1. Cambiare la password a) frequentemente (al massimo ogni sei mesi);
2. Usare password lunghe almeno 8 caratteri con un misto di lettere, numeri e segni di interpunzione.
3. Utilizzate password distinte per sistemi con diverso grado di sensibilità. In alcuni casi le password viaggiano in chiaro sulla rete e possono essere intercettate, per cui, oltre a cambiarle spesso, è importante che siano diverse da quelle usate da sistemi "sicuri".

Cosa NON fare
1. NON comunicate a nessuno la vostra password. Ricordate che lo scopo principale per cui usate una password è assicurare che nessun altro possa utilizzare le vostre risorse o possa farlo a Vostro nome.
2. NON scrivete la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer.
3. Quando immettete la password NON fate sbirciare a nessuno quello che state battendo sulla tastiera.
4. NON scegliete password che si possano trovare in un dizionario. Su alcuni sistemi è possibile "provare" tutte le password contenute in un dizionario per vedere quale sia quella giusta.
5. NON crediate che usare parole straniere renderà più difficile il lavoro di scoperta, infatti chi vuole scoprire una password è dotato di molti dizionari delle più svariate lingue.
6. NON usate il vostro nome utente. È la password più semplice da indovinare
7. NON usate password che possano in qualche modo essere legate a voi come, ad esempio, il vostro nome, quello di vostra moglie/marito, dei figli, del cane, date di nascita, numeri di telefono etc.