Introduzione

*D*al 1 Gennaio 2004 è in vigore, in Italia, il "Codice in materia di protezione dei dati personali" (Decreto legislativo n. 196 del 30/6/2003) che riforma interamente la disciplina sulla privacy. Il Codice abroga e sostituisce tutte le precedenti leggi, decreti e regolamenti in materia, riunendo in un unico organico contesto l'intera normativa sulla privacy.
Tutte le aziende sono tenute a rispettare la nuova normativa, la cui corretta applicazione consente, non solo di adempiere agli obblighi di legge, ma anche di migliorare l'organizzazione aziendale, i processi di lavoro e la qualità dei risultati. Il Codice richiede l'adozione di diverse misure di sicurezza per garantire che i dati trattati siano custoditi e controllati secondo alcune misure minime di sicurezza: a titolo di esempio possiamo citare il fatto che ogni persona che accede alla banca dati (dall'anagrafica dei clienti ad archivi contenenti dati sensibili) deve essere preventivamente incaricata e riconosciuta dal sistema attraverso un identificativo associato ad una password che deve essere lunga almeno otto caratteri, modificata all'atto del primo collegamento e non deve essere agevolmente riconducibile al proprietario. Altre misure minime prevedono l'aggiornamento costante del software con le ultime "patch" rilasciate dal produttore e il backup settimanale dei dati. Oltre alle misure minime il Codice prevede altre misure di sicurezza più ampie "idonee" a garantire ulteriormente la protezione dei dati e dei sistemi.
In generale il Codice prescrive di fatto la realizzazione di un vero e proprio sistema di sicurezza che protegga i dati custoditi all'interno dell'azienda.

Le misure di sicurezza adottate devono essere riportate in un Documento Programmatico annuale sulla Sicurezza (DPS) la cui redazione o aggiornamento deve essere riportata nella relazione accompagnatoria al bilancio aziendale. Il DPS deve essere redatto entro il 31 Marzo di ogni anno. La mancata adozione delle misure minime di sicurezza rende penalmente perseguibili gli inadempienti (ovvero chiunque essendovi tenuto omette di adottarle), salvo l'adozione di un ravvedimento operoso. La mancata adozione delle misure minime o di quelle idonee può portare il soggetto cui si riferiscono i dati e che è stato danneggiato a chiedere un risarcimento dei danni.

Il nuovo Codice sulla Privacy

Adempimenti

Chiunque tratta dati personali è tenuto a rispettare gli obblighi prescritti dal "Codice in materia di protezione dei dati personali"[1]. Aziende, imprese, ditte, studi professionali, banche, assicurazioni, organizzazioni ed *esercenti le professioni sanitarie*, ed ogni altra categoria, privata e pubblica, indipendentemente dalle loro dimensioni, sono tenute ad operare nel rispetto di precise regole che riguardano la sicurezza dei dati e dei sistemi al fine di ridurre al minimo le fonti di rischio e garantire correttezza, integrità ed aggiornamento delle informazioni.

Tra gli interventi richiesti per la sicurezza dei dati e dei sistemi, a secondo dei casi è necessario organizzare e disciplinare l'uso di:

- sistemi di autenticazione informatica;
- credenziali di autenticazione (password, codici identificativi, carte a microprocessore, certificati digitali, rilevatori di caratteristiche biometriche);
- sistema di autorizzazione informatica;
- protezione dei dati e sistemi dalle intrusioni di estranei, virus, internet worm, programmi maligni;
- aggiornamenti delle vulnerabilità individuate con *patch, hot fix, service pack*;
- protezione da intrusioni nei sistemi informatici;
- back up dei dati e organizzazione del ripristino;
- redazione di un aggiornato documento programmatico sulla sicurezza;
- tecniche di cifratura.

E' necessario anche che i sistemi di rilevazione biometria, di videosorveglianza, di localizzatori di persone, di lavoro a distanza, siano organizzati in conformità al Codice.

Diritto alla protezione dei dati personali

Il Codice, all'art.1, introduce un nuovo e fondamentale diritto: *"chiunque ha diritto alla protezione dei dati personali che lo riguardano"*. I dati che devono essere protetti riguardano sia le persone fisiche (tutti noi), sia le persone giuridiche (i dati riferiti ad aziende, imprese, ditte, ecc.). La protezione dei dati personali è garantita da idonee e preventive misure di sicurezza obbligatorie per chi tratta i dati personali.

Misure di sicurezza, sanzioni penali e amministrative per il responsabile dell'azienda

Le misure di sicurezza richieste dal Codice sono articolate in due gruppi:

- quelle "minime", la cui mancata adozione comporta sanzioni penali per il responsabile legale dell'azienda e/o se designato per il responsabile del trattamento (solitamente l'amministratore delegato o una figura di alto livello), ma anche per chiunque, essendovi tenuto, omette di adottarle;

[1] Emanato con decreto legislativo del 30 giugno 2003 n.196,

- quelle più ampie, o “idonee”, decise in autonomia dal titolare in relazione alle proprie specificità che, se non adottate, in caso di danno dovuto a trattamenti di dati non protetti adeguatamente concorreranno all’individuazione delle responsabilità e del conseguente risarcimento economico.

Sono previste, inoltre, misure per titolari particolari quali i fornitori di un servizio di comunicazione elettronica accessibile al pubblico o gli organismi e *gli esercenti le professioni sanitarie.*

Misure di sicurezza minime

Le misure minime di sicurezza richieste dalla legge sono tecniche, informatiche, organizzative, logistiche e procedurali e sono tutte orientate a ridurre i rischi che incombono sui dati personali trattati per ridurne al minimo i rischi di perdita o distruzione anche accidentale. Poiché tutti i dati sensibili del Laboratorio vengono trattati elettronicamente, le misure da adottare per la protezione dei trattamenti elettronici dei dati sono sinteticamente elencate di seguito.

Credenziali, autenticazione, autorizzazione

Alla base delle nuove misure minime sono poste le modalità per l’accesso ai dati che devono avvenire solo da parte delle persone autorizzate ed esplicitamente incaricate; ad esse dovranno essere assegnate o associate “credenziali di autenticazione”, cioè parole chiave, codici identificativi, carte a microprocessore, dispositivi che riconoscono le caratteristiche biometriche. Tali credenziali dovranno consentire “l’autenticazione informatica” delle persone incaricate del trattamento di dati. Inoltre, quando più persone incaricate accedono ai dati, è necessario associare ad ogni soggetto uno specifico profilo per l’accesso. Il profilo identifica dei trattamenti di dati che possono essere svolti e costituisce “l’ambito del trattamento consentito”; l’intero processo è definito “sistema di autorizzazione” per l’accesso ai trattamenti consentiti e preventivamente individuati.

La legge definisce anche i criteri con cui le credenziali devono essere scelte; ad esempio la parola chiave usata in un sistema di autenticazione deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non deve contenere riferimenti agevolmente riconducibili all’incaricato e deve essere modificata da quest’ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave dovrà essere modificata almeno ogni tre mesi.

Protezione da programmi maligni, prevenzione dalle vulnerabilità, salvataggio dei dati

Alcune misure previste dal codice sono rivolte a tutelare la sicurezza di tutte le tipologie di dati personali dalle nuove emergenti criticità:

- i dati personali devono essere protetti contro il rischio di intrusione e dell'azione di virus, internet worm, programmi maligni, ecc., mediante l'attivazione di idonei strumenti manuali ed elettronici, (ad esempio antivirus, firewall, ed altri adeguati sistemi) da tenere aggiornati;
- gli strumenti elettronici – nel caso di trattamenti di dati sensibili e giudiziari[2] - devono essere aggiornati periodicamente con programmi che consentono di eliminare le vulnerabilità individuate e correggere i difetti del software individuati (*patch, hot fix, service pack*);
- i dati devono essere salvati su copie di riserva almeno settimanalmente nel rispetto di apposite disposizioni tecniche e organizzative.

Backup, supporti rimovibili, ripristino

Se si trattano i cosiddetti dati sensibili o giudiziari questi dati dovranno essere protetti da ulteriori misure di sicurezza, quali:

- strumenti elettronici che evitano gli accessi abusivi (intrusioni);
- procedure per la generazione e la custodia di copie di sicurezza dei dati (back up);
- istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti;
- disposizioni per riutilizzare o distruggere i supporti rimovibili sui quali sono registrati tali dati;
- strumenti per il ripristino della disponibilità dei dati e dei sistemi entro tempi certi e compatibili con i diritti degli interessati, non superiori a sette giorni.

[2] Per una definizione di dato sensibile o giudiziario si veda il glossario riportato in allegato

Documento programmatico annuo sulla sicurezza

Rilevante l'importanza assunta dal Documento Programmatico annuo per la Sicurezza (DPS), che deve essere compilato o aggiornato entro il 31 marzo di ogni anno e contenere, tra l'altro:
- l'analisi dei rischi che incombono sui dati
- le misure da adottare per garantire l'integrità e la disponibilità dei dati
- la previsione di idonei interventi formativi degli incaricati del trattamento per renderli edotti dei rischi che incombono sui dati
- la descrizione dei criteri da seguire per garantire l'adozione delle misure minime di sicurezza in caso di outsourcing dei trattamenti.

Inoltre, solo per i dati personali idonei a rivelare lo stato di salute e la vita sessuale trattati da organismi sanitari e gli esercenti di professioni sanitarie, devono essere indicati i criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato, ad esempio attraverso la disgiunzione dei dati anagrafici da quelli riferiti alla salute.
Infine, ed è forse l'aspetto più innovativo che eleva il documento all'attenzione dei vertici aziendali rendendoli consapevoli delle scelte necessarie per garantire la sicurezza, vi è l'obbligo per il titolare di riferire nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Misure di sicurezza idonee e responsabilità civile del titolare del trattamento

Le misure di sicurezza "minime" sono solo una parte degli accorgimenti obbligatori in materia di sicurezza (art. 33 del Codice). Infatti, come già previsto dalla legge n. 675/1996, esiste un obbligo più generale di ridurre al minimo determinati rischi, per cui occorre custodire e controllare i dati personali oggetto di trattamento per contenere le probabilità che i dati siano distrutti, dispersi anche accidentalmente, conoscibili fuori dei casi consentiti o altrimenti trattati in modo illecito.
Ciò va fatto adottando misure idonee anche in base al progresso tecnico, alla natura dei dati ed alla caratteristiche del trattamento.
L'inosservanza di questo obbligo rende il trattamento illecito anche se non si determina un danno per gli interessati; viola inoltre i loro diritti, compreso il diritto fondamentale alla protezione dei dati personali che può essere esercitato nei confronti del titolare del trattamento (artt. 1 e 7, comma 3, del Codice), ed espone a responsabilità civile per danno anche non patrimoniale qualora, davanti al giudice ordinario, non si dimostri di aver adottato tutte le misure idonee ad evitarlo (artt. 15 e 152 del Codice).

Tali misure di sicurezza "idonee" sono individuate dal Titolare sulla base di una analisi specifica delle proprie caratteristiche tecnologiche, organizzative e di processo, tenuto conto delle "innovazioni tecnologiche" e delle soluzioni di sicurezza offerte dal mercato.

Altre importanti scadenze

L'adozione delle misure minime di sicurezza e di quelle più ampie per gli strumenti elettronici deve essere dichiarata nella "notificazione[3]".

Disposizioni

Termini	Adempimenti
31 dicembre 2005	Termine per l'adozione di tutte le "misure minime" non previste dalla precedente normativa.
31 marzo 2006	Termine per l'adozione di tutte le "misure minime" non previste dalla precedente normativa per quei soli titolari che possono dimostrare obiettive ragioni tecniche che non consentono in tutto o in parte l'immediata applicazione delle misure minime e che, allo scopo, hanno compilato un documento a data certa (da conservare presso la propria struttura) con la descrizione delle ragioni del rinvio ed hanno comunque adottato ogni possibile misura per evitare un incremento dei rischi di cui all'art.31 del dlgs.196/2003.
31 marzo di ogni anno	Termine ultimo annuale per la compilazione del DPS (Documento Programmatico sulla Sicurezza)

Trattamento dei dati sensibili nella struttura del Laboratorio Analisi Valdès

Il Laboratorio Analisi Valdès è un soggetto privato che si identifica nella persona dell'Amministratore Unico Dott.ssa Giovanna Paola Carboni che sarà il Titolare del trattamento .
Il Laboratorio si inquadra nella categoria commerciale di fornitore di servizi.
I dati trattati dal Laboratorio interessano la categoria dei clienti o utenti ed in particolare vengono trattati dati genetici, dati idonei a rivelare lo stato di salute della persona e dati idonei a rivelare la vita sessuale.

Il trattamento dei dati viene effettuato all'interno della struttura di riferimento che è il Laboratorio Analisi Valdès sito in Via Gianturco 9/11 09125 Cagliari (Italia).
All'interno di questa macro-struttura si possono individuare quattro sezioni dentro le quali vengono trattati in maniera diversa i dati:

- Segreteria accettazione
- Laboratori analisi
- Segreteria sanitaria
- Direzione
- Amministrazione

Nell'istruzione operativa 75IO24 "Adeguamento alla legge sulla Privacy" sono ulteriormente descritte le attività messe in atto dalla struttura per adeguarsi al DLGS 196/03.

[3] La notificazione è una dichiarazione con la quale un soggetto pubblico o privato rende nota al Garante per la protezione dei dati personali l'esistenza di un'attività di raccolta e di utilizzazione dei dati personali, svolta quale autonomo titolare del trattamento.

Distribuzione dei compiti e delle responsabilità

Sono state distribuite le lettere di incarico al trattamento dei dati sensibili, a tutti gli operatori, relativamente alle mansioni svolte nel Laboratorio (vedi lettere ed organigramma); nella seguente tabella vengono definiti i macrosettori di attività:

Struttura	**Trattamenti effettuati nella struttura**	**Compiti e responsabilità della struttura**
Segreteria accettazione	Trattamento dei dati anagrafici del cliente, diagnosi accertate e presunte.	Acquisizione e caricamento dei dati sul Sistema Informatico. Gestione consenso. Custodia del referto finale cartaceo riportante i dati sensibili del cliente. Consegna del referto finale cartaceo riportante i dati sensibili al cliente.
Laboratori analisi	Trattamento dei dati riferiti a dati sensibili degli utenti (dati genetici, vita sessuale, malattia).	Elaborazione e consultazione dei dati sensibili.
Segreteria sanitaria	Trattamento dei dati anagrafici del cliente. Trattamento dei dati riferiti a dati sensibili degli utenti (dati genetici, vita sessuale, malattia).	Inserimento dati sensibili nel referto, comunicazioni ad interessati e gestione tecnica operativa della base dati (salvataggi, ripristini).
Direzione	Trattamento dei dati anagrafici del cliente. Trattamento dei dati riferiti a dati sensibili degli utenti (dati genetici, vita sessuale, malattia).	Controllo e validazione dati elaborati dai laboratori analisi, controllo e validazione dati inseriti nei referti dalla segreteria sanitaria.
Amministrazione	Trattamento delle banche dati fornitori e situazione contabile clienti.	Elaborazione e custodia dati amministrativi cliente, relativi ad analisi effettuate nel laboratorio. Inserimento dati anagrafici ed amministrativi di fornitori, collaboratori e loro custodia.

Regole per la gestione delle password (o credenziali di autenticazione)

Tutti gli incaricati del trattamento dei dati accedono al sistema informativo (LAB 100) per mezzo di una password personale.
Le password sono strettamente personali e non possono essere riassegnate ad altri utenti.

La password è un elemento fondamentale per la sicurezza delle informazioni. L'affidabilità delle password è il meccanismo più importante per proteggere i dati; un corretto utilizzo della password è a garanzia dell'utente.

La password è composta da 8 caratteri alfanumerici. Detta password non contiene, né conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore e deve essere autonomamente modificata dall'incaricato al primo accesso al sistema e dallo stesso consegnata in una busta chiusa al custode delle password, il quale provvede a metterla nella cassaforte in un plico sigillato.

Ogni tre mesi ciascun incaricato provvede a sostituire la propria password e a consegnare al custode delle password una busta chiusa sulla quale è indicato il proprio nome e la data di modifica ed al cui interno è contenuta la nuova password; il custode delle password provvederà a sostituire la precedente busta con quest'ultima.

Le password verranno automaticamente disattivate dopo tre mesi di non utilizzo.
Le password di amministratore di tutti i PC che lo prevedono sono assegnate dall'amministratore di sistema, esse sono conservate in busta chiusa nella cassaforte. In caso di necessità l'amministratore di sistema è autorizzato a intervenire sui personal computer.

In caso di manutenzione straordinaria possono essere comunicate, qualora necessario, dall'amministratore di sistema al tecnico/sistemista addetto alla manutenzione le credenziali di autenticazione di servizio. Al termine delle operazioni di manutenzione l'amministratore di sistema deve ripristinare nuove credenziali di autenticazione che devono essere custodite in cassaforte.
Le disposizioni di seguito elencate sono vincolanti per tutti i posti lavoro tramite i quali si può accedere alla rete e alle banche dati contenenti dati personali e/o sensibili.
Per la definizione/gestione della password devono essere rispettate le seguenti regole:
- la password deve essere costituita da una sequenza di minimo otto caratteri alfanumerici e non deve essere facilmente individuabile;
- deve contenere almeno un carattere alfabetico ed uno numerico;
- non deve contenere più di due caratteri identici consecutivi;
- non deve contenere il nome come parte della password;
- la nuova password non deve essere simile alla password precedente;
- la password deve essere cambiata almeno ogni tre mesi
- la password termina dopo tre mesi di inattività;
- la password è segreta e non deve essere comunicata ad altri;
- la password va custodita con diligenza e riservatezza;
- l'utente deve sostituire la password, nel caso ne accertasse la perdita o ne verificasse una rivelazione surrettizia.

Misure per la gestione di strumenti elettronico /informatico

Per gli elaboratori che ospitano archivi (o hanno accesso tramite la rete) con dati personali sono adottate le seguenti misure:
• l'accesso agli incaricati ed agli addetti alla manutenzione è possibile solo in seguito ad autorizzazione scritta;
• gli hard disk non sono condivisi in rete se non temporaneamente per operazioni di copia;
• tutte le operazioni di manutenzione che sono effettuate on-site avvengono con la supervisione dell'incaricato del trattamento o di un suo delegato;
• le copie di backup realizzate giornalmente su cassette HD sono conservate in cassaforte ignifuga posta nella direzione
• divieto di utilizzare floppy disk come mezzo per il backup;
• divieto per gli utilizzatori di strumenti elettronici di lasciare incustodito, o accessibile, lo strumento elettronico stesso. A tale riguardo, sul programma LAB100, per evitare errori e dimenticanze, è adottata una uscita automatica dal programma dopo 3 minuti di non utilizzo, con ridigitazione della password segreta per la prosecuzione del lavoro.
• divieto di memorizzazione di archivi con dati sensibili di carattere personale dell'utente sulla propria postazione di lavoro non inerenti alla funzione svolta;
• divieto di installazione di software di qualsiasi tipo sui personal computer che contengono archivi con dati sensibili senza apposita autorizzazione scritta da parte del responsabile del trattamento dati;
• divieto di installazione sui personal computer di accessi remoti di qualsiasi tipo mediante modem e linee telefoniche (tranne quelli autorizzati dal responsabile del trattamento.

Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento.

La stampa di documenti contenenti dati sensibili è effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato.

Il fax si trova in locale ad accesso controllato (segreteria interna) e l'utilizzo è consentito unicamente agli incaricati del trattamento.

La manutenzione degli elaboratori, che può eventualmente prevedere il trasferimento fisico presso un laboratorio riparazioni, è autorizzata solo a condizione che il fornitore del servizio dichiari per iscritto di avere redatto il documento programmatico sulla sicurezza e di aver adottato le misure minime di sicurezza previste dal disciplinare.

Regole di comportamento per minimizzare i rischi da virus

Per minimizzare il rischio da virus informatici, gli utilizzatori dei PC adottano le seguenti regole:
• divieto di lavorare con diritti di amministratore o superutente sui sistemi operativi che supportano la multiutenza;
• limitare lo scambio fra computer di supporti rimovibili (floppy, cd, zip) contenenti file con estensione EXE, COM, OVR, OVL, SYS, DOC, XLS;
• controllare (scansionare con un antivirus aggiornato) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti;
• evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza, ovvero divieto di "scaricare" dalla rete internet ogni sorta di file, eseguibile e non. La decisione di "scaricare" può essere presa solo dal responsabile del trattamento;
• disattivare gli Activex e il download dei file per gli utenti del browser Internet Explorer;
• disattivare la creazione di nuove finestre ed il loro ridimensionamento e impostare il livello di protezione su "chiedi conferma" (il browser avvisa quando uno script cerca di eseguire qualche azione);
• attivare la protezione massima per gli utenti del programma di posta Outlook Express al fine di proteggersi dal codice html di certi messaggi e-mail (buona norma è visualizzare e trasmettere messaggi in formato testo poiché alcune pagine web, per il solo fatto di essere visualizzate possono infettare il computer);
• non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus. Usare prudenza anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e della rubrica di un computer infettato per inviare nuovi messaggi "infetti");
• non cliccare mai un link presente in un messaggio di posta elettronica da provenienza sconosciuta, (in quanto potrebbe essere falso e portare a un sito-truffa);
• non utilizzare le chat;
• consultare con periodicità settimanale la sezione sicurezza del fornitore del sistema operativo e applicare le patch di sicurezza consigliate;
• non attivare le condivisioni dell'HD in scrittura.
• seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto);
• avvisare l'Amministratore di sistema nel caso in cui il virus sia stato scoperto solo dopo aver subito svariati malfunzionamenti della rete o di qualche PC, ovvero in ritardo (in questo caso è possibile che l'infezione abbia raggiunto parti vitali del sistema);
• conservare i dischi di ripristino del proprio PC (creati con l'installazione del sistema operativo, o forniti direttamente dal costruttore del PC);
• conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge;
• conservare la copia originale del sistema operativo e la copia di backup consentita per legge;
• conservare i driver delle periferiche (stampanti, schede di rete, monitor, ecc., fornite dal costruttore).

Nel caso di sistemi danneggiati seriamente da virus l'Amministratore procede a reinstallare il sistema operativo, i programmi applicativi ed i dati; seguendo la procedura indicata:

1. formattare l'Hard Disk, definire le partizioni e reinstallate il Sistema Operativo (molti produttori di personal computer forniscono uno o più cd di ripristino che facilitano l'operazione);
2. installare il software antivirus, verificate e installare immediatamente gli eventuali ultimi aggiornamenti;
3. reinstallare i programmi applicativi a partire dai supporti originali;
4. effettuare il RESTORE dei soli dati a partire da una copia di backup recente. NESSUN PROGRAMMA ESEGUIBILE DEVE ESSERE RIPRISTINATO DALLA COPIA DI BACKUP: potrebbe essere infetto;
5. effettuare una scansione per rilevare la presenza di virus nelle copie dei dati;
6. ricordare all'utente di prestare particolare attenzione al manifestarsi di nuovi malfunzionamenti nel riprendere il lavoro di routine.

Criteri e modalità di ripristino della disponibilità dei dati

Tutti gli incaricati del trattamento dei dati devono avvisare tempestivamente il responsabile della sicurezza informatica o l'amministratore di sistema o il responsabile del trattamento dei dati, nel caso in cui constatino le seguenti anomalie:
• discrepanze nell'uso delle password;
• modifica e sparizione di dati;
• cattive prestazioni del sistema (così come percepite dagli utenti);
• irregolarità nell'andamento del traffico;
• irregolarità nei tempi di utilizzo del sistema;
• quote particolarmente elevate di tentativi di connessione falliti.

In caso di incidente sono considerate le seguenti priorità:
1. evitare danni diretti alle persone;
2. proteggere l'informazione sensibile o proprietaria;
3. evitare danni economici;
4. limitare i danni all'immagine del Laboratorio

Un incidente può essere definito come un evento che produce effetti negativi sulle operazioni del sistema e che si configura come frode, danno, abuso, compromissione dell'informazione, perdita di beni.

Garantita l'incolumità fisica alle persone si procedere a:
1. isolare l'area contenente il sistema oggetto dell'incidente;
2. isolare il sistema compromesso dalla rete;
3. spegnere correttamente il sistema oggetto dell'incidente. Una volta spento il sistema oggetto dell'incidente non deve più essere riacceso;
4. documentare tutte le operazioni.

Se l'incidente è dovuto ad imperizia del personale o ad eventi accidentali, ovvero quando non vi è frode, danno, abuso e non è configurabile nessun tipo di reato, il ripristino può essere effettuato, a cura dell'amministratore di sistema, direttamente sugli hard disk originali a partire dalle ultime copie di backup ritenute valide.
Altrimenti il titolare del trattamento, il responsabile del trattamento e l'amministratore di sistema coinvolgeranno esperti e/o autorità competenti.

La successiva fase di indagine e di ripristino del sistema sarà condotta da personale esperto di incident response, tenendo presente quanto sotto indicato:
1. eseguire una copia bit to bit degli hard disk del sistema compromesso;
2. se l'incidente riguarda i dati il restore dei dati può avvenire sulla copia di cui al punto 1 precedente a partire dalle ultime copie di backup ritenute valide;
3. se l'incidente riguarda il sistema operativo o esiste la possibilità che sia stato installato software di tipo MMC il ripristino deve essere effettuato reinstallando il sistema operativo su nuovo supporto.
È indispensabile che per una eventuale indagine venga assicurata l'integrità e la sicurezza dello stato del sistema in oggetto e quindi non venga introdotta alcuna alterazione ai dati residenti nel sistema medesimo; un ripristino affrettato del sistema potrebbe alterare le prove dell'incidente.

Allegato: Glossario Privacy

AFFIDAMENTO DATI IN OUTSOURCING
affidamento della gestione dei dati a ditte o a persone esterne all'Ente per lo svolgimento di lavorazioni particolari.

BANCA DI DATI
qualsiasi complesso organizzato di dati ripartito in una o più unità dislocate in una o più posizioni.

BLOCCO
la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

CREDENZIALI DI AUTENTICAZIONE
dati e dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati utilizzati per l'autenticazione informatica.

DATI IDENTIFICATIVI
dati personali che permettono l'identificazione diretta dell'interessato

DATI ANONIMI
i dati che in origine, o a seguito del trattamento, non possono essere associati ad un interessato identificato o identificabile. Costituiscono la classe di dati a minore rischio, per la quale non sono previste particolari misure di sicurezza.

DATI PERSONALI
qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati od identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione ivi compreso un numero di identificazione personale. Costituiscono la classe di dati a rischio intermedio.

DATI SENSIBILI/GIUDIZIARI/SANITARI
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. Costituiscono la classe di dati ad alto rischio.

DIFFUSIONE
il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

GARANTE
l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

INCARICATI
le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile del trattamento. (Art. 4, Comma I, Lett. h D. L.vo 196/2003).

INTERESSATO
la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

MISURE MINIME DI SICUREZZA
il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'art. 31 (D. L.vo n. 196/2003).

PAROLA CHIAVE
componente di una credenziale associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

PROFILO DI AUTORIZZAZIONE
l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti

RESPONSABILE DEL SISTEMA INFORMATIVO
il referente istituito dal D. L.vo 39/93 cui compete la pianificazione degli interventi di automazione, l'adozione delle cautele e delle misure di sicurezza.

RESPONSABILE PER IL TRATTAMENTO DEI DATI
la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.
È designato dal titolare e deve garantire il rispetto delle norme in materia di trattamento dati e di sicurezza, i suoi compiti devono essere elencati per iscritto. La nomina del responsabile è facoltativa e non esonera da responsabilità il titolare.

SISTEMA DI AUTORIZZAZIONE
insieme di strumenti e procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo del richiedente.

TITOLARE
la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza (nell'istituzione scolastica, la titolarità è esercitata dal dirigente scolastico).

TRATTAMENTO
qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati.

UTENTE
qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico

Chiunque voglia approfondire le informazioni contenute in questo opuscolo potrà rivolgersi alla Dott.ssa Maria Giulia Salgo che metterà a disposizione il DPS del Laboratorio Analisi Valdès.