MINISTERO DELL'UNIVERSITA' E DELLA RICERCA - UFFICIO SCOLASTICO REGIONALE PER LA PUGLIA
ISTITUTO COMPRENSIVO STATALE con sezione musicale
SCUOLA DELL'INFANZIA, PRIMARIA E SECONDARIA DI 1° GRADO
"MUSTI-DIMICCOLI" - Barletta


Documento Programmatico Sulla Sicurezza

Art. 19, Allegato B, D.l. 30 giugno 2003 n. 196

INDICE

1. PREMESSE METODOLOGICHE
   - 1.1 MODALITA' DI COSTRUZIONE DI UN _PIANO SICUREZZA" PER IL TRATTAMENTO DEI DATI PERSONALI
   - 1.2 CICLO DELLA SICUREZZA
   - 1.3 L'ARCHITETTURA DI SICUREZZA
   - 1.4 L'ARCHITETTURA DI SICUREZZA E LA RIDUZIONE DEI RISCHI
2. FINALITA' DEL PRESENTE DOCUMENTO PROGRAMMATICO SULLA SICUREZZA
3. CAMPO DI APPLICAZIONE
4. RIFERIMENTI NORMATIVI
5. LE FIGURE PREVISTE DALLA NORMATIVA NEL SETTORE DELLA SICUREZZA PER LA PRIVACY
   - 5.1 IL TITOLARE DEL TRATTAMENTO
   - 5.2 IL RESPONSABILE DEL TRATTAMENTO
   - 5.3 COMPITI DEL TITOLARE E DEL RESPONSABILE DEL TRATTAMENTO
   - 5.4 L'AMMINISTRATORE DI SISTEMA
   - 5.5 IL CUSTODE DELLE PASSWORD
   - 5.6 GLI INCARICATI DEL TRATTAMENTO
6. NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI
7. NOMINA DEGLI AMMINIS TRATORI DI SISTEMA
8. NOMINA DEL CUSTODE DELLE PASSWORD
9. NOMINA DEGLI INCARICATI DEL TRATTAMENTO
10. DATI AFFIDATI AD ENTI ESTERNI PER IL TRA TTAMENTO IN OUT-SOURCING
    - 10.1 TRATTAMENTO DEI DATI IN OUT-SOURCING
    - 10.2 CRITERI PER LA SCELTA DEGLI ENTI TERZI CUI AFFIDARE IL TRATTAMENTO DEI DATI IN OUT-SOURCING
    - 10.3 NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI IN OUT-SOURCING
11. INVENTARI E METODOLOGIE OPERATIVE DI TRA TTAMENTO DEI DATI
    - 11.1 INDIVIDUAZIONE DELLE BANCHE DI 0DATI OGGETTO DEL TRATTAMENTO
    - 11.2 INVENTARIO DELLE SEDI IN CUI VENGONO TRATTATI I DATI
    - 11.3 INVENTARIO DEGLI UFFICI IN CUI VENGONO TR ATTATI I DATI
    - 11.4 INVENTARIO DEI SISTEMI DI ELABORAZIONE
12. MISURE DI SICUREZZA CONTRO IL RISCHIO DI DISTRUZIONE O PERDITA DI DATI
    - 12.1 CRITERI E PROCEDURE PER GARANTIRE L'INTEGRITÀ DEI DATI
    - 12.2 PROTEZIONE DA VIRUS INFORMATICI
    - 12.3 INFEZIONI E CONTAGIO DA VIRUS INFORMATICI
    - 12.4 CUSTODIA E CONSERVAZIONE DEI SUPPORTI UTILIZZATI PER IL BACK-UP DEI DATI
    - 12.5 UTILIZZO E RIUTILIZZO DEI SUPPORTI MAGNETICI
    - 12.6 PIANO DI FORMAZIONE DEGLI INCARICATI
13. MISURE DI SICUREZZA CONTRO IL RISCHIO DI ACCESSO NON AUTORIZZATO
    - 13.1 NORME GENERALI DI PREVENZIONE
    - 13.2 PROCED URE PER CONTROLLARE L'ACCESSO AI LOCALI IN CUI VENGONO TRATTATI I DATI
    - 13.3 PROCEDURE DI ASSEGNAZ IONE DEGLI USER-ID
    - 13.4 PROCEDURE DI ASSEGNAZ IONE DELLE PASSWORD
    - 13.5 IDENTIFICAZIONE DEGLI ELABORATORI CONNESSI IN RETE PUBBLICA
    - 13.6 CRITERI E PR OCEDURE PER GARANTIRE LA SICUREZZA DELLE TRASMISSIONI DEI DATI
14. MISURE DI SICUREZZA CONTRO IL RISCHIO DI TRATTAMENTO NON CONSENTITO
    - 14.1 PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI
    - 14.2 VERIFICHE PERIODICHE DELLE CONDIZIONI PER IL MANTENIMENTO DELLE AUTORIZZAZIONI
    - 14.3 DEFINIZIONE DEI CRITERI DI ASSEGNAZIONE DEI PERMESSI DI ACCESSO AI DATI
    - 14.4 VERIFICHE PERIODICHE DELLE CONDIZIONI PER IL MANTENIMENTO DEI PERMESSI DI ACCESSO AI DATI
    - 14.5 PIANO DI FORMAZIONE DEL PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI
15. MANUTENZIONE APPARECCHIATURE E DEI SISTEMI DI TRATTAMENTO DEI DATI
    - 15.1 MANUTENZIONE DEI SISTEMI DI ELABORAZIONE DEI DATI
    - 15.2 MANUTENZIONE DEI SISTEMI OPERATIVI
    - 15.3 MANUTENZIONE DELLE APPLICAZIONI SOFTWARE
16. MISURE DI SICUREZZA PER IL TRATTAMENTO DEI DATI EFFETTUATO CON STRUMENTI NON AUTOMATIZZATI.
    - 16.1 NOMINA E ISTRUZIONI AGLI INCARICATI
    - 16.2 COPIE DEGLI ATTI E DEI DOCUMENTI
17. ALLEGATI
18. REVISIONI

1. PREMESSE METODOLOGICHE

1.1 MODALITA' DI COSTRUZIONE DI UN "PIANO SICUREZZA" PER IL TRATTAMENTO DEI DATI PERSONALI

Un modo pratico per procedere alla costruzione del "piano sicurezza" potrebbe essere il seguente:

- Inventario delle banche dati
- Individuazione dei responsabili e degli incaricati
- Definizione dei trattamenti
- Definizione delle misure di sicurezza
- Gestione della documentazione richiesta dalla legge.

A meno che non si tratti di una piccola azienda, in generale i sistemi informativi sono normalmente complessi e spesso collegati con i sistemi di altre strutture economiche (imprese consociate, business partner, banche, enti statali, ecc..); pertanto è sempre opportuno adottare una metodologia precisa per fare l'inventario delle banche dati che contengono informazioni soggette alla legge ed i relativi trattamenti.

Il percorso logico da seguire nell'analisi potrebbe partire:

- dalle applicazioni,

per analizzare in seguito

- le banche dati
- i dati privati
- gli archivi fisici
- i collegamenti con altre applicazioni/sistemi,
- gli archivi tecnici (copie di back-up, copie per i test),
- i log applicativi e di sistema,
- gli archivi di sicurezza per il piano di disaster recovery ed, in fine,
- gli archivi storici.

Le Applicazioni - L'inventario di tutte le applicazioni esistenti nella struttura è fondamentale per verificare se si trattano dati privati, rilevarne il trattamento e le finalità. In questo contesto è importante innanzitutto definire che cosa si intende per applicazione; per esempio sotto il titolo di applicazione del personale potrebbero ricadere tutti i programmi applicativi per la gestione delle retribuzioni, le carriere, gli skill, ecc.

Le Banche Dati - Una volta completato l'inventario delle applicazioni si può verificare il contenuto delle relative banche dati e definire se vi siano dati che abbiano le caratteristiche richieste nelle previsioni legislative.
E' in questa fase che si dovrebbe anche individuare se esistono e quali sono i cosiddetti dati *sensibili*.
Infatti per questa particolare tipologia di dati viene richiesta una attenzione specifica ed un trattamento differenziato.
Si ritiene preferibile prendere in esame solo le banche dati primarie e di trattare gli altri archivi come archivi derivati, ma facenti parte di un unico trattamento.

Altri Archivi - Occorre considerare anche eventuali nastri depositati fuori dai locali della struttura nei cosiddetti archivi di sicurezza o storici o dati in elaborazione a società di servizi.

Collegamenti - Sicuramente un punto critico per molte organizzazioni; dipende dalla complessità del sistema informativo e dal suo grado di distribuzione. In un centro ben organizzato tutti i collegamenti tra applicazioni dovrebbero essere descritti nei documenti tecnici. Ciò è meno vero per gli ambienti distribuiti, soprattutto se il protocollo di rete non è di tipo gerarchico, ma paritetico. Le LAN sono reti che appartengono a questa categoria. I responsabili delle varie applicazioni dovrebbero essere la fonte delle informazioni necessarie per questo inventario.
Non bisogna inoltre escludere la ricerca ad altre categorie di archivi che sicuramente contengono dati privati, anche se non sono direttamente riconducibili alle singole applicazioni. Si fa riferimento a tutti quegli archivi che vengono creati dai sistemi operativi o fanno parte dei processi di gestione dei centri di calcolo. Ricadono sotto questa categoria per esempio i

log, che contengono le informazioni delle attività fatte durante la giornata da chiunque operi sui calcolatori.
Normalmente questi log, se esistenti, contengono il codice della persona che ha operato e le indicazioni di che cosa ha fatto, ora e minuto.

1.2 CICLO DELLA SICUREZZA

Il ciclo sicurezza può essere definito nelle seguenti fasi/operazioni:

- Analisi dei rischi
- Contromisure possibili
- Definizione della politica aziendale sulla sicurezza
- Realizzazione delle misure decise
- Amministrazione
- Auditing e controlli

Analisi dei rischi: In questa fase si dovrebbe procedere all'inventario dei dati da proteggere e alla valutazione dei rischi a cui sono soggetti. Particolare attenzione va posta ai rischi dovuti alle carenze organizzative ed alla scarsa cultura sugli aspetti della sicurezza informatica. Oggi i rischi per l'integrità dei dati si sono moltiplicati. Si parla sempre più spesso di intercettazioni, di pirati informatici, di virus ecc.. Volendo classificare i rischi abbiamo i rischi secondo l'origine, le cause e le modalità.

Rischi secondo l'origine:

- **Interni** - connessi alla attività dei dipendenti della azienda. Secondo le statistiche sono i più probabili.
- **Esterni** - connessi alla attività di qualunque altra persona.
- **Ambientali** - relativi a eventi di grande portata, quali: incendi, terremoti, allagamenti, ecc..

Rischi secondo le cause:

- **Carenze organizzative** - responsabilità non correttamente assegnate, sottovalutazione dei rischi, ecc..
- **Colpa** - se causati da ignoranza, incuria o leggerezza. Statisticamente è la causa più diffusa.
- **Dolo** - In rapida crescita. Infatti con l'avvento di Internet è cresciuto enormemente il numero delle persone che possiedono le apparecchiature e le necessarie conoscenze tecniche per arrecare danno.

Rischi secondo le modalità:

- **Intercettazioni** - principalmente lungo la rete di trasmissione.
- **Ingegneria sociale** - per divertimento, si prende gioco della vittima. Sono le modalità più diffuse e pericolose
- **Backdoor** - Quando i programmatori lasciano dei punti di ingresso non noti nel software.
- **Cavalli di Troia** - lo dice lo stesso nome - software predisposto per operare in modo non noto all'utente.
- **Denial of service** - comandi che pregiudicano la efficienza delle reti e dei server.
- **Virus** - software che ha la capacità di autopropagarsi
- **Personificazione** - quando ci si presenta sotto mentite spoglie.

Ovviamente la lista potrebbe essere più lunga e completa. Si consideri che con l'avvento della informatica distribuita e di Internet, il possibile Hacker può essere chiunque e in qualunque parte del mondo ed è praticamente impossibile individuarlo.

Le Contromisure - Di fronte ad una casistica di minacce cosi variegata ed eterogenea e per molti versi imprevedibile, le difese parziali ed improvvisate sono destinate ad essere poco efficaci. Infatti anche per la sicurezza informatica, come per molti sistemi di sicurezza, si può dire che è l'anello più debole che determina il grado di resistenza della catena.

Definizione della politica aziendale sulla sicurezza: E' la fase più importante. E' fondamentale che il management aziendale o delle strutture economiche in genere prenda atto dei rischi e definisca una adeguata risposta in termine di politica aziendale (regole, organizzazione, responsabilità, ecc.) e relativi budget di spesa. Il bilanciamento costi benefici e l'accettazione dei rischi residui sono parte non rinunciabile di questa fase. Il risultato concreto è la pubblicazione dello

standard aziendale di sicurezza.

Realizzazione: Occorre tradurre quanto definito nella fase precedente in atti concreti. Questa fase, in organizzazioni complesse, può richiedere tempi e molto impegno. Se i sistemi informativi nella fase di progetto non sono stati disegnati tenendo nel dovuto conto i requisiti della sicurezza, questa fase può avere costi molto elevati e talvolta non bilanciati con i benefici che si vogliono ottenere.

Amministrazione: Sicurezza vuol dire regole, vincoli, controlli, liste di accesso, permessi ecc..; ciò comporta una certa dose di inevitabile burocrazia e di lavoro amministrativo. Senza l'attività di amministrazione, dopo qualche tempo, il sistema di sicurezza si degrada e fallisce i suoi obiettivi

Auditing e controlli: Costruire un sistema di sicurezza senza, in qualche modo, verificarne l'efficacia, serve a poco. I sistemi informatici sono normalmente molto complessi (sistemi operativi, applicazioni, banche dati, reti, ecc.) e solo con test accurati si può avere una ragionevole certezza di aver costruito un sistema privo di scoperture o manchevolezze. Ovviamente non possiamo limitarci ai test iniziali, ma questi vanno ripetuti con frequenze opportune (1 o 2 volte l'anno).
Con ciò il ciclo è concluso. Ovviamente, poiché difficilmente i sistemi informativi e l'ambiente in cui operano sono statici, il ciclo della sicurezza non termina mai. E' altamente raccomandabile che almeno una volta l'anno si riparta con una revisione dei rischi e, se necessario, anche con le altre fasi.

1.3 L'ARCHITETTURA DI SICUREZZA

L'architettura di sicurezza è l'insieme di regole, funzioni, strumenti, oggetti e controlli, coerentemente disegnati e resi funzionanti, che garantiscono in ogni struttura organizzativa, ambiente informatico, sistema informativo, singolo elaboratore, ecc. il rispetto degli standard di sicurezza definiti dall'azienda.

Normalmente abbiamo architetture di sicurezza differenziate per:

- *Ambiente tradizionale* (Centro di calcolo con mainframe e rete privata)
- *Ambiente distribuito/Server* (LAN con server dipartimentali)
- *Ambiente Internet/Intranet* (Web)
- *Ambiente distribuito/Client* (Workstation, browser).

Gli elementi essenziali di una architettura sono:

- Funzioni di sicurezza
- Meccanismi di sicurezza
- Oggetti di sicurezza
- Processi di gestione

Funzioni di sicurezza : Identificazione e autenticazione degli utenti, controllo accessi ai dati ed alle applicazioni, crittografia, non rigetto, firma elettronica, ecc. sono esempi di funzioni che vanno valutate e decise. Naturalmente si focalizzerà prioritariamente l'attenzione alle funzioni previste dall'Allegato B.

Meccanismi di sicurezza : Sono i prodotti Hardware e Software che realizzano le funzioni di sicurezza previste nell'architettura.

Oggetti di sicurezza : E' importante che vengano con molta precisione individuati quegli oggetti informatici che sono funzionali ai meccanismi di sicurezza. Fanno parte di questa categoria le password, le chiavi di crittografia, le liste di accesso, ecc.. Una protezione non appropriata di questi oggetti potrebbe vanificare l'efficacia dell'intero sistema.

Processi di gestione : E' l'insieme dei processi e delle regole per la gestione delle funzioni, dei meccanismi e degli oggetti di sicurezza che fanno parte della architettura. Vi dovrebbero far parte anche processi di allarme e controllo.

Un'architettura di sicurezza così strutturata e gestita dovrebbe senz'altro rispondere a quanto previsto dall'articolo 31, D.l. 30 giugno 2003, n. 196 e soprattutto essere *preventiva e tecnologicamente sempre aggiornata.*
In modo esplicito l'art. 31 richiede che i dati personali oggetto di trattamento siano **custoditi** ... **controllati** ... in modo da ridurre **al minimo** i rischi di **distruzione**, **perdita** anche accidentale, ... di **accesso non autorizzato**, ... di **trattamento non**

consentito, ... di trattamento **non conforme** alla finalità della raccolta.

Funzioni di sicurezza - Di seguito verranno esaminate le *funzioni di sicurezza* che rispondono ai singoli requisiti. **Custodia** - Presuppone che siano definiti dei processi (norme e responsabilità) nell'area sia della sicurezza fisica che logica.
Sicurezza fisica - Locali dei centri di calcolo isolati e dotati di accessi controllati. E' importante che solo gli addetti ai lavori (incaricati del trattamento) vi possano accedere e che altre persone (visitatori, addetti ai lavori ausiliari, ecc.) vi accedano solo con apposita autorizzazione.
E' buona norma dotare gli ingressi di apparecchiature per la identificazione delle persone (es. lettori di badge) e tutte le aperture di allarmi per cautelarsi da intrusioni durante il periodo in cui il centro resta non presidiato.
Per i server dipartimentali o comunque distribuiti le soluzioni possono essere molte, più o meno efficaci: uso di armadietti chiusi a chiave, locali appositamente predisposti, lucchetti, ecc.. Occorre ricordare che nei Personal Computer è molto facile asportare i dischi fissi.
Poiché sono sempre possibili delle intercettazioni anche le *apparecchiature di rete* dovrebbero essere custodite opportunamente.

Un discorso a parte meritano le *nastroteche*. Nastri etichettati e gestiti con la tecnica del carico e scarico e inventari periodici di controllo (almeno una volta all'anno).
Poiché la legge parla di rischi di perdita anche accidentale, se i nastri sono unici, sarà bene dotarsi di opportuni impianti antincendio che non provochino ulteriori danni ai nastri in caso di utilizzo di dette apparecchiature.
Quanto detto per i nastri vale anche per i dischi rimovibili.

Sicurezza logica - I metodi per proteggere le informazioni dal punto di vista logico sono molti e svariati e fortemente dipendenti dalla tipologia dei sistemi operativi utilizzati (piattaforme Software). Comunque alcune caratteristiche sono comuni a tutte le piattaforme.

Citiamo solo alcune che sono applicabili sia ai sistemi host che ai server distribuiti ed in qualche misura anche alle singole workstation.

- *Integrità del sistema operativo:* è il primo elemento chiave. Non tutti i sistemi operativi da questo punto di vista sono uguali; inoltre vanno installati e mantenuti a regola d'arte. La classificazione del TCSEC Americano aiuta a fare un primo confronto. Per avere comunque maggiori certezze è necessario far fare da personale specializzato gli opportuni test (penetration test) per individuare le scoperture ed avere le indicazioni per rimediarvi.
Deve essere sempre tenuto presente che una scopertura sul sistema operativo indebolisce tutte le altre protezioni di sicurezza.

- *Sistema chiuso o aperto:* Per stare più tranquilli ed avere minori rischi è sicuramente consigliabile disegnare il sistema di sicurezza secondo la regola che è tutto proibito meno le cose autorizzate (sistema chiuso), piuttosto che secondo lo schema opposto: è tutto permesso meno le cose proibite (sistema aperto). La prima soluzione è più costosa e richiede una accurata amministrazione.

- *Accessi discrezionali od obbligatori:* si parla di accesso discrezionale quando si demanda ad una persona (normalmente proprietario della applicazione) l'autorità di decidere a chi dare l'accesso ai dati e a chi no. Si ha l'accesso obbligatorio quando l'accesso ai dati è strutturale e controllato dal sistema di sicurezza.
Penso che per i dati sensibili sia preferibile adottare la soluzione degli accessi obbligatori.

- *Classificazione delle informazioni:* Sul piano pratico converrebbe adottare un sistema di classificazione che veda, per esempio, i dati "sensibili" classificati ad un livello più alto dei dati "personali". L'adozione di un opportuno sistema di classificazione, oltre ad accrescere la protezione dei dati, dovrebbe permettere di adottare un sistema di protezione selettivo.

Un esempio potrebbe essere:

- Informazioni "sensibili": altamente riservate
- Informazioni "private": riservate
- Altre informazioni aziendali riservate: riservate
- Altre informazioni aziendali: non classificate

un sistema di classificazione, perché sia efficace, deve comprendere anche le informazioni cartacee.

- *Metodi di accesso*: Il più usato è quello basato su parole chiave o password. Per accrescerne l'efficacia occorre che ci siano regole precise di gestione delle password. Occorre definirne la lunghezza minima, la durata, e le regole grammaticali per evitare le password facilmente indovinabili. Ogni password dovrebbe essere abbinata ad un individuo; è l'unico modo per poter risalire alle responsabilità di eventuali azioni contrarie a quanto previsto dalla legge.

- *Antivirus*: Nell'architettura di sicurezza dei Personal Computer dovrebbe essere sempre previsto non solo un Antivirus, ma anche e soprattutto un rigoroso processo di controllo dei dischetti che entrano in azienda e, se collegati ad Internet, del software che viene scaricato dalla rete.

La lista di metodologie di protezione potrebbe continuare, ma ritengo che quelle richiamate siano sufficienti per disegnare una architettura di sicurezza minima. Ovviamente se le banche dati dovessero essere inserite in un sistema particolarmente esposto, come per esempio un Web di Internet, occorrerà provvedere ad un disegno specifico e prevedere la installazione di Firewall e di protocolli di mutuo riconoscimento basati su chiavi crittografiche.

I controlli - La legge li richiede in modo esplicito; inoltre, dimostrare di averli in funzione, sarà sicuramente utile per il Responsabile, se dovesse essere necessario.

Controlli periodici - Possiamo dividere i controlli in:

- *Auditing*: personale specializzato, spesso esterno all'azienda, verifica l'aderenza dei comportamenti e delle soluzioni tecniche agli standard di sicurezza (in questo caso anche alle disposizioni di legge). L'Auditing richiede, come prerequisito, che l'azienda si sia data per iscritto le regole e abbia definito ruoli e responsabilità.

- *Revisioni interne* : differiscono dalle metodologie precedenti solo per il fatto che sono eseguite dallo stesso personale interno dell'azienda e richiedono preparazione ed impegno meno gravoso. Spesso precedono le revisioni ufficiali vere e proprie.

- *Test* : tecnici dotati di opportuni tools e metodologie provano a violare i sistemi informativi, ad accedere ai dati ed alle applicazioni pur non avendo alcuna autorizzazione iniziale

Controlli continui - Possiamo dividere i controlli in:

- *Analisi dei log*: per prima cosa occorre che il meccanismo che registra i log (liste di attività) sia attivato sia sui sistemi operativi che sui software di sicurezza e che i log siano protetti e mantenuti per un periodo sufficiente. L'attività di analisi per la ricerca di eventi anomali e la successiva determinazione delle cause andrebbe fatta giornalmente. Accumulare log per periodi più lunghi, data la mole di dati da verificare, renderebbe vana ogni attività di verifica. L'uso di tools automatici di supporto snellisce molto questa attività e la rende meno gravosa.

Inoltre i log sono di per sé banche dati con informazioni private e pertanto da gestire opportunamente.

- *Routine di controllo*: sotto questa terminologia si intendono tutti quei software che effettuano operazioni di verifica continua sui sistemi per garantire che gli standard di sicurezza siano rispettati e che ne segnalano le deviazioni. Ritengo che si possano personalizzare queste routine facendo in modo che verifichino, laddove è possibile, che il trattamento delle banche dati personali resti conforme a quanto notificato al Garante.

1.4 L'ARCHITETTURA DI SICUREZZA E LA RIDUZIONE DEI RISCHI

In modo esplicito l'art. 31, D.l. 30 giugno 2003, n. 196, richiede che i dati personali oggetto di trattamento siano **custoditi** ... **controllati** ... in modo da ridurre **al minimo** i rischi di **distruzione**, **perdita** anche accidentale, ... di **accesso non autorizzato**, ... di **trattamento non consentito**, ... di trattamento **non conforme** alla finalità della raccolta.

Possiamo annoverare i rischi principalmente nella seguente casistica:

- Rischi di distruzione o perdita anche accidentale
- Rischi di accesso non autorizzato
- Rischio di trattamento non consentito o non conforme

Rischi di distruzione o perdita anche accidentale - Un dato memorizzato in un archivio elettronico può essere distrutto o perso per svariate cause:

- *comandi applicativi errati* : ciò è dovuto essenzialmente ad applicazioni non ben testate. Si riduce il rischio sia seguendo rigorose procedure di test che separando il mondo cosiddetto di sviluppo e test da quello di produzione.

- *comandi operativi errati*: Un operatore può sempre sbagliare e provocare distruzioni irreparabili. Volendo ridurre tale rischio è necessario ridurre al minimo le necessità di comandi manuali, demandando tali comandi ad applicazioni specializzate (schedulatori, sistemi di automazione).

- *software pericoloso*: metto in questa categoria, oltre ai virus, tutta quella serie di routine, per altro molto diffuse nei centri elaborazioni, che possono accedere ai dati superando le barriere dei sistemi di sicurezza e al di fuori del controllo dei programmi applicativi. L'uso di tali programmi dovrebbe essere vietato (salvo uno ristretto utilizzo in casi particolari) ed inoltre con opportuni controlli andrebbero ricercati e cancellati dalle librerie.

- *malfunzionamenti dell'Hardware*: anche l'hardware più costoso e tecnologicamente più evoluto è soggetto a malfunzionamenti. La difesa più efficace consiste nel duplicare gli archivi con frequenze prestabilite.

- *eventi disastrosi*: Mi riferisco ad incendi, allagamenti, esplosioni o atti dolosi, ecc. che distruggano i supporti magnetici su cui i dati sono registrati.

Si ritiene che la legge imponga l'adozione di misure di back-up obbligatorie (art. 34 lett. f, D.l. 30 giugno 2003, n. 196) per tutte le banche dati private. In altre parole le applicazioni che gestiscono i dati privati andrebbero inserite tra quelle vitali per l'azienda e trattate secondo le procedure di disaster/recovery.

Rischi di accesso non autorizzato - Se vogliamo tenere sotto controllo il rischio di accesso non autorizzato dobbiamo disporre di una funzione di controllo accessi che copra l'intero sistema informativo e non solo le specifiche applicazioni. Infatti dobbiamo cautelarci da ogni manomissione di dati, sia da parte del personale degli uffici che per compito deve trattare i dati privati, sia del personale tecnico del centro elaborazioni che svolge operazioni di trattamento sugli archivi interi. Particolare cura deve essere posta agli accessi da parte di applicazioni o da comandi di sistema operativo.
In altre parole i dati privati devono avere una protezione totale e le logiche con cui vengono date le autorizzazioni devono essere sotto il controllo diretto del *Responsabile del trattamento*.

Rischio di trattamento non consentito o non conforme - Per poter ridurre questa tipologia di rischio bisogna fare in modo che il trattamento definito per ogni banca dati e notificato al Garante rimanga tale e non possa essere modificato da nessuno senza la espressa volontà del Titolare o del Responsabile a ciò delegato. Per ottenere ciò, più che sulle soluzioni tecniche, bisogna agire sulla organizzazione e l'assegnazione delle responsabilità.

Gli articoli citati, come del resto molti altri, pongono precisi limiti e divieti, a seconda dei casi, alla diffusione e comunicazione dei dati privati e/o sensibili. Ricordiamoci che è considerata comunicazione la semplice possibilità di consultazione dei dati. E' anche previsto che il Garante possa vietare la diffusione di alcuni dati e che è vietata la comunicazione e la diffusione dei dati di cui è stata ordinata la cancellazione.

Tutto questo vuol dire che l'accesso in lettura dei dati deve essere strettamente controllato e che i software di trasmissione devono essere gestiti molto accuratamente.

Una particolare comunicazione/trasmissione è il trasferimento dei dati all'estero. Sulle reti si dovranno installare dei filtri, gateway o firewall per evitare trasmissioni verso località non desiderate.

2. FINALITA' DEL PRESENTE DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Il presente Documento Programmatico Sulla Sicurezza (DPSS) riporta i percorsi di analisi e le conseguenti misure minime di sicurezza identificate e da adottare in via preventiva, conformemente a quanto previsto dall'Allegato B del D.l. 30 giugno 2003, n. 196.

Costituisce pure un valido strumento per la adozione delle misure idonee previste dall'art.31, D.l. 30 giugno 2003, n. 196.
L'analisi e il risultato del presente Documento Programmatico sulla Sicurezza portano a pianificare e a programmare le misure necessarie per ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, intendendosi per misure di sicurezza il complesso degli accorgimenti tecnici, informatici, organizzativi, logistici e procedurali di sicurezza.

3. CAMPO DI APPLICAZIONE

Il ***Documento Programmatico Sulla Sicurezza*** (DPSS) è il documento di programma che definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali. Dette definizioni conseguono dall'analisi dei rischi, dalla distribuzione dei compiti e delle responsabilità nell'ambito della struttura analizzata.

In particolare nel ***Documento Programmatico Sulla Sicurezza*** (DPSS) vengono definiti:

- i criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ai medesimi locali;
- i criteri e le procedure per assicurare l'integrità dei dati;
- i criteri e le procedure per la sicurezza della trasmissione dei dati, ivi compresi quelli per le redazioni di accesso per Via telematica;
- l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni.

Il ***Documento Programmatico Sulla Sicurezza*** (DPSS) riguarda tutti i dati personali:

- Sensibili
- Giudiziari
- Comuni

Il ***Documento Programmatico Sulla Sicurezza*** (DPSS) si applica al trattamento di tutti i dati personali per mezzo di:

- Strumenti elettronici di elaborazione
- Altri strumenti di elaborazione (ad esempio: Cartacei, Audio, Visivi e Audiovisivi, ecc..)

Il ***Documento Programmatico Sulla Sicurezza*** (DPSS) deve essere conosciuto ed applicato da tutte le figure che operano nella struttura.

4. RIFERIMENTI NORMATIVI

- D.l. 30 giugno 2003, n. 196
- D.l. 30 giugno 2003, n. 196, Allegato B

5. LE FIGURE PREVISTE DALLA NORMATIVA NEL SETTORE DELLA SICUREZZA PER LA PRIVACY

5.1 IL TITOLARE DEL TRATTAMENTO

Il D.l. 30 giugno 2003, n. 196, all'art. 28 definisce **titolare** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo *cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali*, ivi compreso il profilo della sicurezza.

5.2 IL RESPONSABILE DEL TRATTAMENTO

Il D.l. 30 giugno 2003, n. 196, all'art. 29 definisce ***Responsabile del trattamento*** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo *preposti facoltativamente dal titolare al trattamento di dati personali*.

Può quindi essere prevista, in relazione all'attività del ***Titolare del Trattamento***, la nomina di uno o più ***Responsabili del Trattamento*** con compiti diversi a seconda delle funzioni svolte, sia all'interno che all'esterno, sia da persone fisiche, sia da persone giuridiche.

L'art 29 dispone che il responsabile, se designato, deve essere nominato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Il responsabile procede al trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni predette e delle proprie istruzioni.

Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti. I compiti affidati al responsabile devono essere analiticamente specificati per iscritto.

5.3 COMPITI DEL TITOLARE E DEL RESPONSABILE DEL TRATTAMENTO

*Al **Titolare del Trattamento*** quindi competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza ed il Responsabile del Trattamento è il soggetto preposti dal titolare al trattamento di dati personali.

In merito alla sicurezza dei dati l'art 33 e 31 del D.l. 30 giugno 2003, n. 196, dispongono che **il Titolare ed il Responsabile** dovranno curare che i dati personali oggetto di trattamento siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Quanto alle misure minime di sicurezza dovranno adottare quelle previste dal disciplinare tecnico dell'Allegato B.
Nel caso in cui il ***trattamento dei dati*** venisse fatto ***con strumenti elettronici o comunque automatizzati***, in conformità all'art 28 e 29 cureranno l'adozione delle seguenti misure minime (art. 34 del D.l. 30 giugno 2003, n. 196):

a) autenticazione informatica;

b) adozione di procedure di gestione delle credenziali di autenticazione;

c) utilizzazione di un sistema di autorizzazione;

d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

g) tenuta di un aggiornato documento programmatico sulla sicurezza;

Qualora il trattamento effettuato da organismi sanitari abbia ad oggetto dati sensibili, cureranno l'adozione di tecniche di cifratura o di codici identificativi.

Nel caso in cui il ***trattamento dei dati personali*** viene effettuato ***con strumenti elettronici o comunque automatizzati da un fornitore di un servizio di comunicazione elettronica accessibile al pubblico***, in conformità all'art 32 del D.l. 30 giugno 2003, n. 196, il Titolare ed il Responsabile dovranno:

- adottare ai sensi dell'articolo 31 idonee misure tecniche e organizzative adeguate al rischio esistente, per salvaguardare la sicurezza dei suoi servizi, l'integrità dei dati relativi al traffico, dei dati relativi all'ubicazione e delle comunicazioni elettroniche rispetto ad ogni forma di utilizzazione o cognizione non consentita.
- nel caso in cui la sicurezza del servizio o dei dati personali richiede anche l'adozione di misure che riguardano la rete, il fornitore del servizio di comunicazione elettronica accessibile al pubblico dovrà adottare tali misure congiuntamente con il fornitore della rete pubblica di comunicazioni.
- se sussiste un particolare rischio di violazione della sicurezza della rete, dovrà informare gli utenti e/o gli abbonati indicando, quando il rischio è al di fuori dell'ambito di applicazione delle misure che il fornitore stesso è tenuto ad adottare ai sensi dei commi 1 e 2, tutti i possibili rimedi e i relativi costi presumibili. Analoga informativa dovrà essere resa al Garante e all'Autorità per le garanzie nelle comunicazioni.

In ogni caso il Titolare del trattamento direttamente, o se delegato il responsabile, nel caso di trattamento effettuato con strumenti elettronici o automatizzati, in conformità al disposto degli artt. 1 e ss. Dell'Allegato B dovrà:

- se il trattamento di dati personali con strumenti elettronici è consentito agli incaricati, dotare gli stessi di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave. Ad ogni incaricato verranno assegnate o associate individualmente una o più credenziali per l'autenticazione.
- Impartire istruzioni agli incaricati in relazione all'adozione delle necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato. In particolare dovranno costituire una procedura per la quale:
- la parola chiave, quando è prevista dal sistema di autenticazione, dovrà 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 dovrà contenere riferimenti agevolmente riconducibili all'incaricato; dovrà 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. Inoltre il codice per l'identificazione, laddove utilizzato, non potrà essere assegnato ad altri incaricati, neppure in tempi diversi.
- le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
- lo strumento elettronico durante una sessione di trattamento non dovrà essere lasciato incustodito o comunque accessibile da parte di terzi non autorizzati.
- se l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

Perché si vuole che il contenuto del presente ***"Documento Programmatico Sulla Sicurezza"*** (DPSS) sia sempre attuale nel tempo e si astragga dall'organizzazione attuale e possa questo essere applicato in ogni momento anche in presenza di variazioni organizzative nel presente documento si sottintende la presenza del ***Responsabile del trattamento per la***

sicurezza dei dati e si ritiene che allo stesso siano stati affidati compiti molto vasti.

Naturalmente nel caso di variazioni inerenti la nomina del ***Responsabile del Trattamento*** o dei poteri a questi delegati non vi sia o venga meno la figura del ***Responsabile del Trattamento*** o non siano più ricompresi alcuni compiti nel presente scritto previsti in capo allo stesso assegnando oneri inferiori è da intendersi che i compiti o i maggiori compiti spettino al ***Titolare del Trattamento*** che non li ha delegati, è onere del ***Titolare del Trattamento*** individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più ***Responsabili del Trattamento*** e tra questi, uno o più ***Responsabile del trattamento per la sicurezza dei dati*** (RSTD) che assicurino e garantiscano che vengano adottate le misure di sicurezza ai sensi dell'art.31 del D.l. 30 giugno 2003, n. 196.

Qualora il ***Titolare del Trattamento*** ritenga di non nominare alcun ***Responsabile del Trattamento*** e alcun ***Responsabile del trattamento per la sicurezza dei dati***, o revochi o cessi la delega in precedenza conferita o pur nominando un ***"Responsabile" a questi vengano affidati compiti propri che non riguardino tutti i dati trattati sia da un punto di vista geografico sia da un punto di vista organizzativo o funzionale*** il ***Titolare del Trattamento*** ne assumerà tutte le responsabilità e funzioni.

Il ***Titolare del Trattamento*** affida al ***Responsabile del trattamento per la sicurezza dei dati*** il compito di adottare misure tese a ridurre al minimo il rischio di distruzione dei dati, accesso non autorizzato o trattamento non consentito, previe idonee istruzioni fornite per iscritto.

Il ***Titolare del Trattamento*** può affidare ai singoli ***Responsabili del Trattamento*** l'onere di individuare, nominare ed indicare per iscritto uno o più ***Incaricati del trattamento*** .

Sono compiti del ***Responsabile del trattamento per la sicurezza dei dati*** oltre a quant'altro la normativa o la delega del Titolare gli imponga quelli di:

- Individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, gli ***Amministratori di Sistema***.
- Individuare, nominare e incaricare per iscritto, un ***Custode delle password*** qualora vi siano più incaricati del trattamento che sia effettuato con mezzi informatici.
- Individuare, nominare e incaricare per iscritto, gli ***Incaricati del trattamento dei dati personali*** precisando diritti, procedure, regole e limiti in merito.
- Attribuire, con l'ausilio degli ***Amministratori di Sistema*** , ad ogni ***Utente*** (USER) o incaricato un ***Codice identificativo personale*** (USER-ID) per l'utilizzazione dell'elaboratore, che deve essere individuale e non riutilizzabile.
- Autorizzare i singoli incaricati del trattamento e della manutenzione, e gli strumenti da utilizzare.
- Redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione come meglio specificato al successivo paragrafo 13, nonché l'elenco delle tipologie dei trattamenti effettuati.
- Verificare, con l'ausilio degli amministratori di sistema, con cadenza almeno semestrale, l'efficacia dei programmi di protezione ed antivirus, nonché definire le modalità di acceso ai locali e le misure indicate al successivo paragrafo 13.
- Garantire che tutte le misure di sicurezza riguardanti i dati personali trattati siano applicate all'interno dell'azienda ed eventualmente al di fuori dell'azienda, qualora siano cedute a soggetti terzi quali ***Responsabili del Trattamento*** , tutte o parte delle attività di trattamento.
- Informare il titolare nella eventualità che si siano rilevati dei rischi.

5.4 L'AMMINISTRATORE DI SISTEMA

L'amministratore di sistema è il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione *(Art. 29* del D.l. 30 giugno 2003, n. 196*)*.

Nel caso di **trattamenti effettuati con gli elaboratori elettronici**, semprecchè non si tratti di dati personali di cui è consentita la diffusione, devono essere rispettate le seguenti misure previste dagli artt. 1 e ss. Dell'Allegato B, in materia di codice identificativo personale e di antivirus:

a) ciascun utente o incaricato del trattamento per l'utilizzazione dell'elaboratore deve avere un codice identificativo personale; uno stesso codice (fatta eccezione per gli amministratori di sistema relativamente ai sistemi operativi

che prevedono un unico livello di accesso per tale funzione), non può, neppure in tempi diversi, essere assegnato a persone diverse;

b) i codici identificativi personali devono essere assegnati e gestiti in modo che ne sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore o di mancato utilizzo dei medesimi per un periodo superiore ai sei mesi;
c) gli elaboratori devono essere protetti contro il rischio di intrusione ad opera di programmi di cui all'articolo 615 *quinquies* del codice penale, mediante idonei programmi, la cui efficacia ed aggiornamento sono verificati con cadenza almeno annuale.

Per il trattamento dei dati personali l'accesso per effettuare le operazioni di trattamento è determinato sulla base di autorizzazioni assegnate, singolarmente o per gruppi di lavoro, agli incaricati del trattamento o della manutenzione. Le autorizzazioni all'accesso sono rilasciate e revocate dal ***Titolare*** e, se designato, dal ***Responsabile***.

Periodicamente, e comunque almeno una volta l'anno, è verificata la sussistenza delle condizioni per la loro conservazione. L'amministratore di sistema però dovrà verificare se l'utente o l'incaricato sia stato autorizzato all'accesso. Sono oggetto di autorizzazione anche gli strumenti che possono essere utilizzati per il trattamento. Se riferita agli strumenti, l'autorizzazione deve individuare i singoli elaboratori attraverso i quali è possibile accedere per effettuare operazioni di trattamento.

La validità delle richieste di accesso ai dati personali deve essere verificata prima di consentire l'accesso stesso. Non è consentita l'utilizzazione di un medesimo codice identificativo personale per accedere contemporaneamente alla stessa applicazione da diverse stazioni di lavoro.

E' quindi compito degli ***Amministratori di Sistema*** :

- Prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di back-up secondo i criteri stabiliti dal ***Responsabile del trattamento per la sicurezza dei dati*** , conformemente a quanto più analiticamente individuato al successivo **paragrafo 12**
- Assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro.
- Fare in modo che sia prevista l'assegnazione di ***Codici identificativi personali*** (USER-ID) per l'utilizzo dell'elaboratore, secondo i criteri in precedenza esposti e che sia prevista la disattivazione dei ***Codici identificativi personali*** (USER-ID), in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei ***Codici identificativi personali*** (USER-ID) per oltre 6 mesi.
- Proteggere gli elaboratori dal rischio di intrusione (violazione del sistema da parte di "hackers") e dal rischio di virus mediante idonei programmi.

5.5 CUSTODE DELLE PAROLE CHIAVE (PASSWORD) O I PREPOSTI AD ESSE

Il ***Custode delle Parole Chiave (PassWord)***" è la persona (individuata per iscritto dal ***Titolare*** o ***Responsabile***) preposta alla custodia delle parole chiave o che abbia accesso ad informazioni che concernono le medesime. Il "***Custode delle Parole Chiave (PassWord)***" deve essere nominato nel caso in cui, effettuando il trattamento dei dati personali con strumenti elettronici o comunque automatizzati, vi sia più di un incaricato del trattamento e siano in uso più parole chiave.

E' compito del ***Custode delle password*** gestire e custodire "***Password"*** per l'accesso ai dati da parte degli incaricati.
Il ***Custode delle password*** deve predisporre, per ogni ***Incaricato del trattamento,*** una busta sulla quale è indicato lo "***USER-ID"*** utilizzato: all'interno della busta deve essere indicata la "***Password"*** usata per accedere alla "***Banca di Dat***i"; ove tecnicamente possibile in relazione alle caratteristiche dell'elaboratore deve essere consentita l'autonoma sostituzione ed in questo caso occorre descrivere la procedura per detta modifica ed informare gli incaricati che nel caso di sostituzione gli stessi devono prima della sua sostituzione devono consegnare la Nuova Password al "***Custode delle Parole Chiave (PassWord)***".

Le buste con le "***Password"*** debbono essere conservate in luogo chiuso e protetto.
Dette operazioni devono essere adottate, anteriormente all'inizio del trattamento da parte degli incaricati.
Nel caso in cui siano nominato un amministratore di sistema le funzioni connesse all' "*USER ID*" ed all'assegnazione iniziale della Password saranno assunte dallo stesso ed al ***Custode delle password*** competeranno le sole funzioni di custodia.

La password dovrà essere composta da almeno otto caratteri, oppure nel caso in cui lo strumento elettronico non lo consenta

da un numero di caratteri pari al massimo consentito; non dovrà contenere riferimenti facilmente riconducibili all'incaricato. (art. 5, Allegato B).
La password dovrà essere sostituita almeno ogni sei mesi; nel caso di trattamento avente ad oggetto dati sensibili almeno ogni tre mesi (art. 5, Allegato B).

5.6 GLI INCARICATI DEL TRATTAMENTO

Sono Incaricati del trattamento le persone incaricate per iscritto di compiere le operazioni del trattamento dal titolare o dal responsabile, e che operano sotto la loro diretta autorità *(Art. 30* del D.l. 30 giugno 2003, n. 196*).*
L'art *30* del D.l. 30 giugno 2003, n. 196, al suo primo comma dispone che gli incaricati del trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi alle istruzioni del titolare o del responsabile.

6. NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI

La nomina di ciascun ***Responsabile del trattamento per la sicurezza dei dati*** deve essere effettuata con una lettera di incarico in cui sono specificate le responsabilità che gli sono affidate e deve essere controfirmata dall'interessato per accettazione.

Copia della lettera di nomina accettata deve essere conservata a cura del ***Titolare del Trattamento*** in luogo sicuro.
Fra i vari ***Responsabili del Trattamento*** può esserne individuato uno o più che assicurino e garantiscano che vengano adottate le misure di sicurezza di cui all'art.31 del D.l. 30 giugno 2003, n. 196, denominati ***Responsabile del trattamento per la sicurezza dei dati.***

Il ***Titolare del Trattamento*** deve informare ciascun ***Responsabile del Trattamento*** delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dall'Allegato B.
A ciascun ***Responsabile del Trattamento*** il ***Titolare del Trattamento*** deve consegnare una copia di tutte le norme che riguardano la Sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina del ***Responsabile del Trattamento*** è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.
La nomina del ***Responsabile del Trattamento*** può essere revocata in qualsiasi momento dal ***Titolare del Trattamento*** dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.

7. NOMINA DEGLI AMMINISTRATORI DI SISTEMA

L' ***"Amministratore di Sistema"*** è la persona fisica o giuridica che sovrintende alle risorse del sistema operativo di un elaboratore o di un sistema di ***Banche di dati.***

Anche se non espressamente previsto dalla norma, è opportuno che il ***Responsabile del trattamento per la sicurezza dei dati*** nomini uno o più ***Amministratori di Sistema***, specificando gli elaboratori o le banche dati che è chiamato a sovrintendere, informandolo delle responsabilità che gli sono state affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dall'Allegato B.

La lettera di incarico deve essere controfirmata dall'interessato per presa visione e copia della stessa deve essere conservata a cura del ***Responsabile del trattamento per la sicurezza dei dati*** in luogo sicuro.
Agli ***Amministratori di Sistema*** il ***Responsabile del Trattamento*** deve consegnare una copia di tutte le norme che riguardano la Sicurezza del trattamento dei dati in vigore al momento della nomina.

La figura dell' ***"Amministratore di Sistema"*** può coincidere con quella del ***Responsabile del trattamento per la sicurezza dei dati***.

8. NOMINA DEL CUSTODE DELLE PASSWORD

Il ***Responsabile del trattamento per la sicurezza dei dati*** nomina uno o più "***Custodi delle Password"*** a cui è conferito il compito di custodire le "Parole chiave" o "***Password"*** per l'accesso ai dati archiviati nei sistemi di elaborazione dei dati.
La nomina di ciascun ***Custode delle password*** deve essere effettuata con una lettera di incarico.

La nomina del ***Custode delle password*** deve essere controfirmata dall'interessato per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del ***Responsabile del trattamento per la sicurezza dei dati*** in luogo sicuro.
Il ***Responsabile del trattamento per la sicurezza dei dati*** deve informare ciascun ***Custode delle password*** della responsabilità che gli è stata affidata in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dall'Allegato B.

A ciascun ***Custode delle password*** il ***Responsabile del trattamento per la sicurezza dei dati*** deve consegnare una copia di tutte le norme che riguardano la Sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina del ***Custode delle password*** è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.
La nomina del ***Custode delle password*** può essere revocata in qualsiasi momento dal ***Responsabile del trattamento per la sicurezza dei dati*** dei dati senza preavviso, ed essere affidata ad altro soggetto.

9. NOMINA DEGLI INCARICATI DEL TRATTAMENTO

Ai ***Responsabili del Trattamento*** può essere affidato il compito di nominare, con comunicazione scritta, uno o più ***Incaricati del trattamento*** dei dati.

La nomina di ciascun ***Incaricato del trattamento*** dei dati deve essere effettuata con una lettera di incarico in cui sono specificati i compiti che gli sono affidati.
Gli ***Incaricati del trattamento*** devono ricevere idonee ed analitiche istruzioni scritte, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.

Agli incaricati deve essere assegnata una parola chiave e un codice identificativo personale.
La nomina degli ***Incaricati del trattamento*** deve essere controfirmata dall'interessato per presa visione e copia della stessa deve essere conservata a cura del ***Responsabile del trattamento per la sicurezza dei dati*** in luogo sicuro.

Agli ***Incaricati del trattamento*** il ***Responsabile del trattamento per la sicurezza dei dati*** deve consegnare una copia di tutte le norme che riguardano la Sicurezza del Trattamento dei Dati in vigore al momento della nomina.
La nomina degli ***Incaricati del trattamento*** è a tempo indeterminato, e decade per revoca, per sue dimissioni, o con il venir meno dei compiti che giustificavano il trattamento dei dati personali.

10. DATI AFFIDATI AD ENTI ESTERNI PER IL TRATTAMENTO IN OUT-SOURCING

10.1 TRATTAMENTO DEI DATI IN OUTSOURCING

Il ***Titolare del Trattamento*** può decidere di affidare il trattamento dei dati in tutto o in parte a soggetti terzi, in Out-Sourcing, nominandoli responsabili del trattamento.
In questo caso debbono essere specificati i soggetti interessati e i luoghi dove fisicamente avviene il trattamento dei dati stessi.

Nel caso in cui questi non vengano espressamente nominati***, "Responsabili del trattamento in out-sourcing"*** ai sensi dell'art.29 del Codice Unico devono intendersi autonomi titolari del trattamento e quindi soggetti ai corrispettivi obblighi, e pertanto rispondono direttamente ed in via esclusiva per le eventuali violazioni alla legge.
Il ***Titolare del Trattamento*** o uno dei ***Responsabili del Trattamento***, cui è affidato tale specifico incarico, deve redigere e aggiornare ad ogni variazione l'elenco dei soggetti che effettuano il trattamento dei dati in qualità di ***Responsabile del Trattamento***, con particolare attenzione a quei soggetti terzi in out-sourcing, ed indicare per ognuno di essi il tipo di trattamento effettuato.

Per l'inventario dei soggetti terzi, in Out-Sourcing, deve essere utilizzato apposito modulo e, che deve essere conservato a cura del ***Responsabile del Trattamento*** in luogo sicuro.

10.2 CRITERI PER LA SCELTA DEGLI ENTI TERZI A CUI AFFIDARE IL TRATTAMENTO DEI DATI IN OUT-SOURCING

Il ***Titolare del Trattamento*** può nominare "***Responsabile del trattamento in out-sourcing"*** quei soggetti terzi che abbiano i requisiti individuati dall'art.29 del Codice Unico (esperienza, capacità ed affidabilità).

Il "***Responsabile del trattamento dei dati in out-sourcing"*** deve rilasciare una dichiarazione scritta al ***Titolare del Trattamento*** da cui risulti che sono state adottate le misure idonee di sicurezza per il trattamento dei dati secondo quanto disposto dall'Allegato B.

10.3 NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI IN OUT-SOURCING

Per ogni trattamento affidato ad un soggetto esterno nominato "***Responsabile del trattamento in out-sourcing***", il ***Titolare del Trattamento*** deve assicurarsi che siano rispettate le norme di sicurezza di un livello non inferiore a quanto stabilito per il trattamento interno.

Il ***Titolare del Trattamento*** deve informare il "***Responsabile del trattamento dei dati in out-sourcing"*** dei compiti che gli sono affidati in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dall'Allegato B.
Il "***Responsabile del trattamento dei dati in out-sourcing"*** deve accettare la nomina, secondo il modello predisposto.

La nomina del "***Responsabile del trattamento dei dati in out-sourcing"*** deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del ***Titolare del Trattamento*** in luogo sicuro.

11. INVENTARI E METODOLOGIE OPERATIVE DI TRATTAMENTO DEI DATI

11.1 INDIVIDUAZIONE DELLE BANCHE DI DATI OGGETTO DEL TRATTAMENTO

Al "***Responsabile del trattamento della sicurezza dei dati"*** è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle tipologie di trattamenti effettuati.
Ogni "***Banca di dati"*** o archivio deve essere classificato in relazione alle informazioni in essa contenute indicando se si tratta di:

- Dati Personali Comuni
- Dati Personali Sensibili
- Dati Personali Giudiziari

Per l'individuazione degli archivi dei dati oggetto del trattamento deve essere utilizzato il modulo ALL_AA che deve essere conservato a cura del "***Responsabile del trattamento della sicurezza dei dati"*** in luogo sicuro.

11.2 INVENTARIO DELLE SEDI IN CUI VENGONO TRATTATI I DATI

Al "***Responsabile del trattamento della sicurezza dei dati"*** è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle sedi in cui viene effettuato il trattamento dei dati. Per redigere l'inventario delle sedi in cui vengono trattati i dati deve essere utilizzato il modulo ALL_AB che deve essere conservato a cura del "***Responsabile del trattamento della sicurezza dei dati"*** in luogo sicuro.

11.3 INVENTARIO DEGLI UFFICI IN CUI VENGONO TRATTATI I DATI

Al "***Responsabile del trattamento della sicurezza dei dati"*** è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco degli uffici in cui viene effettuato il trattamento dei dati. In particolare, per ogni ufficio deve essere indicata la sede e se l'accesso è controllato. Per l'inventario degli uffici deve essere utilizzato il modulo ALL_AC che deve essere conservato a cura del "***Responsabile del trattamento della sicurezza dei dati"*** in luogo sicuro.

11.4 INVENTARIO DEI SISTEMI DI ELABORAZIONE

Al "***Responsabile del trattamento della sicurezza dei dati"*** è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione con cui viene effettuato il trattamento dei dati.
Per ogni sistema debbono essere descritte le caratteristiche e se si tratta di sistema di elaborazione:

- Non accessibile da altri elaboratori (stand-alone)
- In rete non accessibile al pubblico
- In rete accessibile al pubblico

Per ogni sistema deve essere specificato il nome dell'incaricato o degli incaricati che lo utilizzano nonché del ***Custode delle password*** .

Per l'inventario dei sistemi di elaborazione deve essere utilizzato il modulo ALL_AD che deve essere conservato a cura del "***Responsabile del trattamento della sicurezza dei dati"*** in luogo sicuro.

12. MISURE DI SICUREZZA CONTRO IL RISCHIO DI DISTRUZIONE O PERDITA DI DATI

12.1 CRITERI E PROCEDURE PER GARANTIRE L'INTEGRITÀ DEI DATI

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, il "***Responsabile del trattamento della sicurezza dei dati"***, stabilisce, con il supporto tecnico ***dell'Amministratore del sistema*** la periodicità con cui debbono essere effettuate le copie di sicurezza delle ***Banche di dati*** trattati.

I criteri debbono essere definiti dal ***Responsabile del trattamento della sicurezza dei dati*** in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

In particolare per ogni ***Banca di dati*** debbono essere definite le seguenti specifiche:

- Il "Tipo di supporto" da utilizzare per le "Copie di Back-Up".
- Il numero di "Copie di Back-Up" effettuate ogni volta
- Se i supporti utilizzati per le "Copie di Back-Up" sono riutilizzati e in questo caso con quale periodicità.
- Se per effettuare le "Copie di Back-Up" si utilizzano procedure automatizzate e programmate.
- Le modalità di controllo delle "Copie di Back-Up".
- La durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati.
- ***L'Incaricato del trattamento*** a cui è stato assegnato il compito di effettuare le "Copie di Back-Up".
- Le istruzioni e i comandi necessari per effettuare le "Copie di Back-Up".

Per redigere il "***Documento con le istruzioni di copia"*** deve essere utilizzato per ogni "***Banca di dati"*** il modulo ALL_AM che deve essere conservato a cura del "***Responsabile del trattamento della sicurezza dei dati"*** in luogo sicuro e deve essere trasmesso in copia controllata a:

- ***Amministratore di sistema*** di competenza
- ***Incaricati del trattamento*** di competenza

12.2 PROTEZIONE DA VIRUS INFORMATICI

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita di dati a causa di Virus Informatici, il "***Responsabile del trattamento della sicurezza dei dati***", stabilisce, con il supporto tecnico dell' "***Amministratore del sistema"*** quali protezioni software adottare in relazione all'evoluzione tecnologica dei sistemi disponibili sul mercato.

Il "***Responsabile del trattamento della sicurezza dei dati***", stabilisce inoltre la periodicità, almeno ogni anno (in caso di dati sensibili o giudiziari almeno semestralmente), con cui debbono essere effettuati gli aggiornamenti dei sistemi Antivirus utilizzati per ottenere un accettabile standard di sicurezza delle ***Banche di dati*** trattate.

I criteri debbono essere definiti dal "***Responsabile del trattamento della sicurezza dei dati"*** in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

In particolare per ogni sistema debbono essere definite le seguenti specifiche:

- Il tipo di programma utilizzato.
- La periodicità di aggiornamento

Per ogni sistema deve essere predisposto il modulo "Rilevazione di Virus Informatico" ALL_AP sul quale debbono essere annotati eventuali virus rilevati, e se possibile la fonte da cui sono pervenuti, al fine di isolare o comunque trattare con precauzione i possibili portatori di infezioni informatiche.
I moduli compilati ed aggiornati dagli ***Incaricati del trattamento*** debbono essere conservati a cura del "***Responsabile del trattamento della sicurezza dei dati"*** in luogo sicuro e debbono essere trasmessi in copia controllata all***' "Amministratore di sistema"*** di competenza.

12.3 INFEZIONI E CONTAGIO DA VIRUS INFORMATICI

Nel caso in cui su uno o più sistemi si dovesse verificare perdita di informazioni o danni a causa di infezione o contagio da

Virus Informatici ***l'Amministratore del sistema*** deve provvedere a:

- Isolare il sistema.
- Verificare se ci sono altri sistemi infettati con lo stesso Virus Informatico.
- Identificare l'Antivirus adatto e bonificare il sistema infetto.
- Installare l'Antivirus adatto su tutti gli altri sistemi che ne sono sprovvisti.

L'Amministratore del sistema deve inoltre compilare il modulo di "Report dei Contagi da Virus Informatici" ALL_AQ.
I moduli compilati devono essere conservati a cura del "***Responsabile del trattamento della sicurezza dei dati"*** in luogo sicuro.

12.4 CUSTODIA E CONSERVAZIONE DEI SUPPORTI UTILIZZATI PER IL BACK-UP DEI DATI

Il "***Responsabile del trattamento della sicurezza dei dati"*** , è responsabile della Custodia e della conservazione dei supporti utilizzati per il Back-Up dei dati.

Per ogni "***Banca di dati"*** nel modulo ALL_AM deve essere indicato il luogo di conservazione dei supporti utilizzati per il Back-Up dei dati.

Il luogo di conservazione deve essere individuato in modo che sia protetto da:

- Agenti chimici
- Fonti di calore
- Campi magnetici
- Intrusioni e atti vandalici
- Incendio
- Allagamento
- Furto

L'accesso ai supporti utilizzati per il Back-Up dei dati è limitato per ogni "***Banca di dati"*** al:

- "***Responsabile del trattamento della sicurezza dei dati"*** .
- Eventuale **Responsabile del Trattamento** di competenza.
- ***Incaricato del trattamento*** di competenza.
- "***Amministratore di sistema"*** di competenza.

12.5 UTILIZZO E RIUTILIZZO DEI SUPPORTI MAGNETICI

Se il "***Responsabile del trattamento della sicurezza dei dati"*** decide che i supporti magnetici utilizzati per le copie di Back-Up delle ***Banche di dati*** trattate non sono più utilizzabili per gli scopi per i quali erano stati destinati, deve provvedere a farne cancellare il contenuto annullando e rendendo illeggibili le informazioni in esso contenute.

E' compito del "***Responsabile del trattamento della sicurezza dei dati"*** assicurarsi che in nessun caso vengano lasciate copie di Back-Up delle ***Banche di dati*** trattate, non più utilizzate, senza che ne venga cancellato il contenuto ed annullate e rese illeggibili le informazioni in esso registrate.

12.6 PIANO DI FORMAZIONE DEGLI INCARICATI

Al "***Responsabile del trattamento della sicurezza dei dati"*** è affidato il compito di verificare ogni anno, entro il 31 dicembre, le necessità di formazione del personale incaricato di effettuare periodicamente le operazioni di Back-Up delle ***Banche di dati*** trattate.

Per ogni ***Incaricato del trattamento***, il "***Responsabile del trattamento della sicurezza dei dati"*** definisce, sulla base dell'esperienza e delle sue conoscenze, ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica se è necessaria della formazione tecnica, utilizzando il modulo ALL_AN che deve essere trasmesso in copia controllata al ***Titolare del Trattamento***.

13. MISURE DI SICUREZZA CONTRO IL RISCHIO DI ACCESSO NON AUTORIZZATO

13.1 NORME GENERALI DI PREVENZIONE

In considerazione di quanto disposto dall'Allegato B, è fatto divieto a chiunque di:

- Effettuare copie su supporti magnetici o trasmissioni non autorizzate dal ***Responsabile del trattamento per la sicurezza dei dati*** di dati oggetto del trattamento.
- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal ***Responsabile del trattamento per la sicurezza dei dati*** , di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
- Sottrarre, cancellare, distruggere senza l'autorizzazione del ***Responsabile del trattamento per la sicurezza dei dati***, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
- Consegnare a persone non autorizzate dal ***Responsabile del trattamento per la sicurezza dei dati***, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

13.2 PROCEDURE PER CONTROLLARE L'ACCESSO AI LOCALI IN CUI VENGONO TRATTATI I DATI

Al ***Responsabile del trattamento per la sicurezza dei dati*** è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco degli uffici in cui viene effettuato il trattamento dei dati, nominando un apposito "***Incaricato",*** con il compito di controllare direttamente i sistemi, le apparecchiature, o i registri di accesso ai locali allo scopo di impedire intrusioni o danneggiamenti.

Il ***Responsabile del trattamento per la sicurezza dei dati*** deve definire le modalità di accesso agli uffici in cui sono presenti sistemi o apparecchiature di accesso ai dati trattati.

Il ***Responsabile del trattamento per la sicurezza dei dati*** deve informare con una comunicazione scritta l'***"incaricato dell'ufficio"*** dei compiti che gli sono stati affidati utilizzando il modello predisposto.

13.3 PROCEDURE DI ASSEGNAZIONE DEGLI USER-ID

Il ***Responsabile del trattamento per la sicurezza dei dati*** deve definire in accordo con gl***i Amministratori del sistema*** le modalità di assegnazione dei nomi identificativi per consentire a ciascun ***Incaricato del trattamento*** di accedere ai sistemi di trattamento delle ***Banche di dat****i.*

Non sono ammessi nomi identificativi di gruppo, con la sola eccezione dei codici identificativi assegnati per l'amministrazione di sistema, relativamente ad eventuali sistemi operativi che prevedono un unico livello di accesso.
In ogni caso, un codice identificativo assegnato ad un ***Incaricato del trattamento*** deve essere annullato se ***l'Incaricato del trattamento*** ha dato le dimissioni.

13.4 PROCEDURE DI ASSEGNAZIONE DELLE PASSWORD

Il ***Responsabile del trattamento per la sicurezza dei dati*** deve definire in accordo con gli ***Amministratori del sistema*** le modalità di assegnazione delle password.

La definizione dei criteri di assegnazione delle password è descritta nel modulo ALL_AS. In relazione al tipo di ***_Banca di dati"*** trattata, ***l'Amministratore del sistema*** può decidere che ogni utente ***Incaricato del trattamento*** possa modificare autonomamente la propria ***"Password"*** di accesso. In tal caso l'incaricato consegnerà una busta al Custode della password" contenente la nuova password o se il dato viene memorizzato in particolari archivi dell'elaboratore, in questo caso la modifica equivale alla comunicazione al ***Custode delle password.***

13.5 IDENTIFICAZIONE DEGLI ELABORATORI CONNESSI IN RETE PUBBLICA

Al ***Responsabile del trattamento per la sicurezza dei dati*** è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione connessi in rete pubblica.

Per ogni sistema deve essere specificato *l'**Incaricato del trattamento***, ***l'Amministratore del sistema*** e il ***Custode delle password***.

Per l'inventario dei sistemi di elaborazione deve essere utilizzato il modulo ALL_AO che deve essere conservato a cura del ***Responsabile del trattamento per la sicurezza dei dati*** in luogo sicuro e deve essere trasmesso in copia controllata all***'*** ***"Amministratore di sistema"*** di competenza.

13.6 CRITERI E PROCEDURE PER GARANTIRE LA SICUREZZA DELLE TRASMISSIONI DEI DATI

Al fine di garantire la sicurezza delle trasmissioni dei dati tra le sedi dislocate nel territorio, attraverso l'utilizzo di apparecchi di trasmissione dati, quali "Modem" e "Router", il ***Responsabile del trattamento per la sicurezza dei dati*** (RDST), stabilisce, con il supporto tecnico dell'***Amministratore del sistema*** , le misure tecniche da adottare in rapporto al rischio di intercettazione o di intrusione o di hacker su ogni sistema collegato in rete pubblica.

I criteri debbono essere definiti dal ***Responsabile del trattamento per la sicurezza dei dati*** in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

In particolare per ogni sistema interessato debbono essere definite le seguenti specifiche:

- le misure applicate per evitare intrusioni.
- le misure applicate per evitare contagi da "Virus Informatici".

utilizzando per ogni sistema interessato il modulo ALL_AO che deve essere conservato a cura del ***Responsabile del trattamento per la sicurezza dei dati*** in luogo sicuro e deve essere trasmesso in copia controllata all***'*** ***"Amministratore di sistema"*** di competenza.

14. MISURE DI SICUREZZA CONTRO IL RISCHIO DI TRATTAMENTO NON CONSENTITO

14.1 PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI

Al ***Responsabile del trattamento per la sicurezza dei dati*** è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco degli ***Incaricati del trattamento*** autorizzati al trattamento dei dati personali.
In particolare, in caso di trattamento automatizzato di dati, per ogni ***Incaricato del trattamento*** deve essere indicato lo USER-ID assegnato e la password con un numero di caratteri non inferiori a otto.

In caso di dimissioni di un ***Incaricato del trattamento*** o di revoca delle autorizzazioni al trattamento dei dati, il ***Responsabile del trattamento per la sicurezza dei dati*** , deve darne immediata comunicazione al "***Custode delle Password"*** e all' "***Amministratore di sistema"*** di competenza che provvederanno a disattivare la possibilità di accesso al sistema per il soggetto in questione.

Per redigere l'elenco degli ***Incaricati del trattamento*** deve essere utilizzato il modulo ALL_AI che deve essere conservato a cura del ***Responsabile del trattamento per la sicurezza dei dati*** in luogo sicuro e deve essere trasmesso in copia controllata a:

- "***Amministratore di sistema"*** di competenza
- ***Custode delle password*** di competenza

14.2 VERIFICHE PERIODICHE DELLE CONDIZIONI PER IL MANTENIMENTO DELLE AUTORIZZAZIONI

Al ***Responsabile del trattamento per la sicurezza dei dati*** è affidato il compito di verificare ogni anno, entro il 31 dicembre, le autorizzazioni di accesso ai dati oggetto del trattamento e di aggiornare l'elenco degli utenti autorizzati utilizzando il modulo ALL_AI che deve essere conservato a cura del ***Responsabile del trattamento per la sicurezza dei dati*** in luogo sicuro e deve essere trasmesso in copia controllata a:

- "***Amministratore di sistema"*** di competenza
- ***Custode delle password*** di competenza

14.3 DEFINIZIONE DEI CRITERI DI ASSEGNAZIONE DEI PERMESSI DI ACCESSO AI DATI

Al ***Responsabile del trattamento per la sicurezza dei dati*** è affidato il compito di redigere e di aggiornare ad ogni variazione la tabella dei "Permessi di accesso" che indica per ogni "***Banca di dati"*** i tipi di permesso di accesso per ogni ***Incaricato del trattamento*** autorizzato.
In particolare per ogni ***Incaricato del trattamento*** e per ogni "***Banca di dati"*** debbono essere indicati i privilegi assegnati tra i seguenti:

- Inserimento di dati
- Lettura e stampa di dati
- Variazione di dati
- Cancellazione di dati

La tabella dei "Permessi di accesso" deve essere redatta utilizzando il modulo ALL_AL che deve essere conservato a cura del ***Responsabile del trattamento per la sicurezza dei dati*** in luogo sicuro e deve essere trasmesso in copia controllata a:

- "***Amministratore di sistema"*** di competenza
- ***Custode delle password*** di competenza

14.4 VERIFICHE PERIODICHE DELLE CONDIZIONI PER IL MANTENERE I PERMESSI DI ACCESSO AI DATI

Al "***Responsabile del trattamento per la sicurezza dei dati "*** è affidato il compito di verificare ogni anno, entro il 31 dicembre, le necessità di accesso ai dati oggetto del trattamento e di aggiornare l'elenco degli utenti autorizzati utilizzando il modulo ALL_AL che deve essere in luogo sicuro e deve essere trasmesso in copia controllata a:

- "***Amministratore di sistema"*** di competenza
- ***Custode delle password*** di competenza

14.5 PIANO DI FORMAZIONE DEL PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI

Al ***Responsabile del trattamento per la sicurezza dei dati*** è affidato il compito di verificare ogni anno, entro il 31 dicembre, le necessità di formazione del personale ***Incaricato del trattamento*** dei dati con lo scopo di fornire ogni informazione necessaria a migliorare la sicurezza di trattamento dei dati.

Per ogni utente il ***Responsabile del trattamento per la sicurezza dei dati*** definisce, sulla base dell'esperienza e delle sue conoscenze, ed in funzione anche di eventuali variazioni della normativa, le necessità di formazione utilizzando il modulo ALL_AL che deve essere trasmesso in copia controllata al ***Titolare del Trattamento*** .

15. MANUTENZIONE APPARECCHIATURE E DEI SISTEMI DI TRATTAMENTO DEI DATI

15.1 MANUTENZIONE DEI SISTEMI DI ELABORAZIONE DEI DATI

Al ***Responsabile del trattamento per la sicurezza dei dati*** è affidato il compito di verificare ogni anno, avvalendosi dell' "***Amministratore di Sistema***", la situazione delle apparecchiature hardware installate con cui vengono trattati i dati, delle apparecchiature periferiche, ed in particolare dei dispositivi di collegamento con le reti pubbliche.

La verifica ha lo scopo di controllare l'affidabilità del sistema, per quanto riguarda:

- La sicurezza dei dati trattati.
- Il rischio di distruzione o di perdita.
- Il rischio di accesso non autorizzato o non consentito.

Tenendo conto anche dell'evoluzione tecnologica.

Il ***Responsabile del trattamento per la sicurezza dei dati*** deve compilare il modulo di "evidenziazione dei rischi hardware" conformemente al modulo ALL_AS.

Nel caso in cui esistano rischi evidenti il ***Responsabile del trattamento per la sicurezza dei dati*** deve informarne il ***Titolare del trattamento*** perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

15.2 MANUTENZIONE DEI SISTEMI OPERATIVI

Al ***Responsabile del Trattamento*** è affidato il compito di verificare ogni semestre, la situazione dei Sistemi Operativi installati sulle apparecchiature con cui vengono trattati i dati.

La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi, per quanto riguarda:

- La sicurezza dei dati trattati.
- Il rischio di distruzione o di perdita.
- Il rischio di accesso non autorizzato o non consentito.

Tenendo conto in particolare di:

- Disponibilità di nuove versioni migliorative dei Sistemi Operativi utilizzati.
- Segnalazioni di Patch ,Fix o System-Pack per la rimozione di errori o malfunzionamenti.
- Segnalazioni di Patch, Fix o System-Pack per l'introduzione di maggiori sicurezze

Contro i rischi di intrusione o di danneggiamento dei dati.

Il ***Responsabile del trattamento per la sicurezza dei dati*** deve compilare il modulo di evidenziazione dei rischi sui Sistemi Operativi" conformemente al modulo ALL_AT.

Nel caso in cui esistano rischi evidenti il ***Responsabile del trattamento per la sicurezza dei dati*** deve informarne il ***Titolare del Trattamento*** perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

15.3 MANUTENZIONE DELLE APPLICAZIONI SOFTWARE

Al ***Responsabile del trattamento per la sicurezza dei dati*** è affidato il compito di verificare ogni anno (semestralmente nel caso di dati sensibili o giudiziari), la situazione delle applicazioni installate sulle apparecchiature con cui vengono trattati i dati.

La verifica ha lo scopo di controllare l'affidabilità del software applicativo, per quanto riguarda:

- La sicurezza dei dati trattati.
- Il rischio di distruzione o di perdita.
- Il rischio di accesso non autorizzato o non consentito.

Tenendo conto in particolare della disponibilità di nuove versioni migliorative delle applicazioni installate che consentano maggiore sicurezza contro i rischi di intrusione o di danneggiamento dei dati.

Il ***Responsabile del trattamento per la sicurezza dei dati*** deve compilare il modulo di "evidenziazione dei rischi nelle applicazioni" conformemente al modulo ALL_AU.

Nel caso in cui esistano rischi evidenti il "***Responsabile del trattamento per la sicurezza dei dati"*** deve informarne il ***Titolare del Trattamento*** perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

16. MISURE DI SICUREZZA PER IL TRATTAMENTO DEI DATI EFFETTUATO CON STRUMENTI NON AUTOMATIZZATI.

16.1 NOMINA E ISTRUZIONI AGLI INCARICATI

Per ogni archivio i "***Responsabili del trattamento per la sicurezza dei dati***" debbono definire l'elenco degli incaricati autorizzati ad accedervi e impartire istruzioni tese a garantire un controllo costante nell'accesso negli archivi. Annualmente dovrà essere verificato l'ambito del trattamento consentito ai singoli incaricati.

Gli incaricati che trattano atti e documenti contenenti dati personali sono tenuti a conservarli in modo che non vi possano accedere persone non autorizzate e restituirli al termine delle operazioni.

Qualora i documenti contengano dati sensibili o giudiziari gli incaricati sono tenuti a conservarli fino alla restituzione in contenitori muniti di serratura (questa disposizione non è più contenuta nel nuovo Codice Unico, ma è comunque consigliabile come standard operativo).

L'accesso agli archivi contenenti documenti ove sono presenti dati sensibili o giudiziari è consentito, dopo l'orario di chiusura, previo controllo o identificazione e registrazione dei soggetti

16.2 COPIE DEGLI ATTI E DEI DOCUMENTI

Quanto indicato nel punto precedente, si applica anche a qualunque tipo di copia effettuata sui documenti contenenti dati personali.

17. ALLEGATI

ALL_AA Elenco degli archivi dei dati oggetto del trattamento
ALL_AB Elenco delle sedi in cui vengono trattati i dati
ALL_AC Elenco dei locali in cui vengono trattati i dati
ALL_AD Elenco dei sistemi di elaborazione per il trattamento dei dati
ALL_AE Elenco dei responsabili del trattamento dei dati personali
ALL_AF Elenco degli amministratori di sistema
ALL_AG Elenco dei custodi delle password
ALL_AH Elenco degli incaricati al controllo degli accessi ai locali
ALL_AI Elenco del personale autorizzato al trattamento dei dati
ALL_AL Elenco dei permessi di accesso ai dati
ALL_AM Criteri e procedure per garantire l'integrità dei dati
ALL_AN Piani di formazione degli incaricati
ALL_AO Inventario dei sistemi di elaborazione connessi in rete pubblica
ALL_AP Report dei virus Informatici rilevati
ALL_AQ Report dei contagi da Virus Informatici
ALL_AR Criteri di assegnazione delle password
ALL_AS Report annuale dei rischi hardware
ALL_AT Report annuale dei rischi sui Sistemi Operativi
ALL_AU Report annuale dei rischi nelle applicazioni
ALL_AV Scheda dei controlli degli archivi magnetici
ALL_AW Scheda dei controlli del sistema di allarme
ALL_AX Scheda controllo USER ID
ALL_AY Scheda controllo buste password
ALL_AZ Scheda controllo archiviazione documenti
ALL_BA Scheda controllo operato dagli incaricati
ALL_BB Elenco USER ID
ALL_BC Elenco buste contenti le password
ALL_BD Elenco dei locali dove vengono conservate le buste delle password
ALL_BE Elenco dei responsabili alla manutenzione di sistema
ALL_BF Scheda soggetti ammessi dopo l'orario di chiusura
ALL_BG Piano operativo sicurezza
ALL_BH Schema organico Privacy

Nomina del Responsabile del Trattamento dei dati personali ATA
Nomina del Responsabile Trattamento Dati Collaboratori Sostituti del Dirigente
Nomina del Responsabile Trattamento Dati Organi Collegiali d'Istituto
Nomina del Responsabile del Trattamento dei dati personali Docenti
Nomina del Responsabile Sicurezza Informatica
Nomina del Responsabile Sicurezza
Lettera di incarico Trattamento dati ATA
Lettera di incarico Trattamento dati Corpo Docenti
Lettera di incarico di Custode delle password
Lettera di incarico di Copie di sicurezza

REVISIONI

Indice delle revisioni

Rev.	Data	Descrizione	Redatto	Verificato	Approvato