

Informazioni sul documento programmatico sulla sicurezza DPS

Simone Zabberoni

Sicurezzainrete – qualche dettaglio introduttivo

http://www.sicurezzainrete.com/documento_programmatico_sulla_sicurezza.htm

Le principali scadenze determinate dal Garante sono:

- 31 marzo 2006 termine per l'obbligo di redigere un documento programmatico (D.P.S.) e l'obbligo di adozione delle misure minime di sicurezza come stabilito nel decreto legge del 1999.
- 31 marzo 2006 termine ultimo per adottare misure minime di sicurezza nella propria azienda
- 30 giugno 2006 il termine per coloro che non possono, per certificati motivi, approntare il DPS entro la fine di Marzo.

Il Documento Programmatico sulla Sicurezza deve essere adottato da chiunque effettua un trattamento di dati sensibili o giudiziari dove con il termine trattamento si intende qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, 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, anche se non registrati in una banca di dati

Decreto Legislativo 30 giugno 2003, n. 196

"Codice in materia di protezione dei dati personali"

pubblicato nella Gazzetta Ufficiale n. 174 del 29 luglio 2003 - Supplemento Ordinario n. 123

<http://www.parlamento.it/leggi/deleghe/03196dl.htm>

Estratto dell' Art. 4 (Definizioni)

1. Ai fini del presente codice si intende per:

- a) "trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, 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, anche se non registrati in una banca di dati;
- b) "dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- c) "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;

d) "dati sensibili", 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;

e) "dati giudiziari", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

Art. 31 (Obblighi di sicurezza)

1. I dati personali oggetto di trattamento sono 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.

Art. 34 (Trattamenti con strumenti elettronici), Misure minime di sicurezza

Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

- autenticazione informatica;
- adozione di procedure di gestione delle credenziali di autenticazione;
- utilizzazione di un sistema di autorizzazione;
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- tenuta di un aggiornato documento programmatico sulla sicurezza;
- adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Punti necessari all'interno di un DPS

Tipologie di dati trattati

I dati trattati dal Titolare si possono suddividere come segue:

- Dati comuni relativi agli utenti
- Dati comuni relativi a fornitori
- Dati comuni relativi ad altri soggetti
- Dati (inclusi suoni ed immagini) idonei a rilevare la posizione di persone ed oggetti
- Dati relativi allo svolgimento di attività economiche ed alle informazioni commerciali
- Dati di natura giudiziaria relativi a utenti e/o parenti degli utenti stessi
- Dati relativi al personale, nonché ai candidati per diventarlo, di natura anche sensibile
- Dati di natura anche sensibile relativi a utenti (quali handicap, situazioni giudiziarie)

In coda al documento c'è una tabella riassuntiva dei dati.

Caratteristiche di aree, locali e strumenti con cui si effettuano i trattamenti e tipologie di trattamento

- Schedari ed altri supporti cartacei
- Elaboratori non in rete
- Elaboratori in rete privata
 - Si dispone di una rete, realizzata mediante collegamenti interni via cavo, costituita da:
 - numero x server (indicare dove si trovano i servers!)
 - numero x postazioni client, dislocati nei vari uffici
 - numero x stampanti di rete o meno, dislocate nei vari uffici
- Elaboratori in rete pubblica
 - Per elaboratori in rete pubblica si intendono quelli che sono raggiungibili da Internet, ovvero erogano servizi non solo per gli utenti della sede. Si dispone di una rete pubblica costituita da:
 - numero x server (indicare dove si trovano i servers!)
 - numero x altri dispositivi (modem, router, dispositivi di backup ecc) (indicare dove si trovano i dispositivi!)
- Impianti di videosorveglianza ed altri idonei a rilevare immagini, suoni e posizione di persone ed oggetti

La mappa dei trattamenti effettuati

Bisogna creare una tabella riassuntiva in cui andiamo ad indicare i tipi di dati trattati e li mettiamo in relazione ai server che li trattano

I tipi di dato sono già stati indicati poco sopra

Usiamo un elenco di strumenti elettronici utilizzati per il trattamento:

- A Server di posta elettronica
- B File server
- C Server Gestionale / Contabilità
- D Server proxy
- E Videosorveglianza

La seguente tabella è indicativa, i singoli trattamenti e dati possono essere “incrociati” o meno in base alle diverse situazioni.

Tipi di dati

1 - Dati comuni relativi agli utenti	X	X	X	X	
2 - Dati comuni relativi a fornitori	X	X	X	X	
3 - Dati comuni relativi ad altri soggetti	X	X	X	X	
4 - Dati (inclusi suoni ed immagini) idonei a rilevare la posizione di persone ed oggetti		X	X		X
5 - Dati relativi allo svolgimento di attività economiche ed alle informazioni commerciali	X	X	X	X	
6 - Dati di natura giudiziaria relativi a utenti e/o parenti degli utenti stessi	X	X			
7 - Dati relativi al personale, nonché ai candidati per diventarlo, di natura anche sensibile	X				
8 - Dati di natura anche sensibile relativi a utenti (quali handicap, situazioni giudiziarie)	X	X			X

Strumenti A B C D E

Mansionario privacy ed interventi formativi degli incaricati

In base ai punti indicati dal DLGs bisogna definire per i singoli servizi aziendali (es: Amministrazione, Utenti, Personale, Commerciale) quali dati vengono trattati ed i responsabili per ogni servizio

Analisi dei rischi che incombono sui dati

Comportamento degli operatori

Rischio	Descrizione	Gravità	Contromisure
Furto di credenziali	Possibilità di utilizzare le password di un altro utente (password ottenuta in vari modi, quali ritrovamento di password su fogli di carta, spiare l'utente mentre la digita, indovinare la password)	Dipendente dal livello di privilegi dell'utente cui vengono rubate le credenziali	Formazione degli utenti relativa al password management
Carenza di consapevolezza, disattenzione, incuria	Utilizzo errato degli strumenti, selezione di password facili da indovinare, scrittura della password in fogli/post it	Dipendente dal livello di privilegi dell'utente	Formazione degli utenti relativa al password management. Formazione degli utenti relativa all'utilizzo del software
Comportamenti sleali e/o fraudolenti	Utilizzo dei propri privilegi di accesso ai sistemi a scopo di lucro personale	Dipendente dal livello di privilegi dell'utente. Dipendente dalla possibilità o meno di utilizzare i sistemi aziendali a proprio lucro (es.: modifica del proprio compenso)	Limitazione dei privilegi agli utenti standard.
Errore operativo	Cancellazione dati, inserimento di dati inconsistenti	Dipendente dal livello di privilegi dell'utente. Dipendente dai controlli del software.	Backup giornaliero dei dati. Controllo da parte del software della coerenza dei dati inseriti/elaborati. Limitazione ai privilegi degli utenti

Eventi relativi agli strumenti

Rischio	Descrizione	Gravità	Contromisure
Virus / worms / spyware	Programmi automatizzati di utilizzo delle vulnerabilità conosciute e di auto-propagazione per i più diversi scopi Programmi che raccolgono informazioni dei pc infetti e li spediscono su internet	Dipendente dal virus, da quasi nullo (virus che avvia il browser internet su siti per adulti) a molto grave (blocco di sistema, backdoor, invio dati su internet)	Sistemi antivirus con costante aggiornamento e management centralizzato
Spamming, Denial of Service (impedimento di servizio)	Impedimento di erogare servizi causato inondando i sistemi con messaggi commerciali e non	Dipendente dalla criticità di erogare il servizio, da nullo (sistemi non vulnerabili in quanto non su internet) a molto alto (es.: impossibilità di inviare/ricevere posta)	Sistemi di firewalling Sistemi di antispam (eliminazione preventiva dei messaggi marcati come spam)

Malfunzionamento degli strumenti	Guasto hardware (linee, alimentazioni, schede di rete, hard disk)	Variabile in funzione del guasto. Si va dalla non disponibilità del servizio (guasto di un alimentatore o di una scheda di rete o di una linea di comunicazione) alla non disponibilità dei dati (guasto di un hard disk)	Hardware ridondati (Dual Power supply, sistemi basati su Raid, schede di rete in bonding)
Intrusioni esterne	Ingressi non autorizzati dall'esterno ai servizi internet e/o alla rete interna	Generalmente alta, in dipendenza del bersaglio dell'intruso (dall' utilizzo delle macchine ospiti per contenere filmati e musica al furto di informazioni riservate)	Sistemi di firewall. Aggiornamento costante dei software utilizzati. Politiche valide di password management
Intercettazione informazioni	Registrazione di informazioni in transito sulle linee di comunicazione	In dipendenza dei dati in transito	Cifratura di tutte le connessioni che transitino su mezzi pubblici (Internet). Eventuale cifratura delle connessioni che transitano sulla rete interna che rechino dati sensibili

Eventi relativi al contesto

Rischio	Descrizione	Gravità	Contromisure
Accesso non autorizzato a locali/aree contenenti apparati e/o dati riservati	Possibilità di visualizzare dati / documenti riservati	Alta	Controllo accessi alle aree riservate (se possibile con registrazione degli accessi stessi) Strong authentication
Furto di apparati contenenti dati	Furto di cassette di backup, schedari, dischi rigidi	Alta	Controllo accessi alle aree riservate (se possibile con registrazione degli accessi stessi) Chiusura degli apparati in appositi armadi dotati di serrature
Eventi distruttivi naturali o dolosi	Incendi, inondazioni, folgorazioni, terremoti, sommosse	Dipendente dallo stato delle contromisure	Politica di disaster recovery Sistemi anti-incendio Posizionamento degli apparati non ai piani bassi degli edifici Costruzioni antisismiche
Guasti agli impianti	Cadute/picchi di tensione, guasto alla climatizzazione	Dipendente dalla qualità dell'hardware utilizzato (hardware di fascia alta resistono meglio ai rischi indicati)	UPS per prevenire cadute/picchi di tensione Manutenzione e controllo costante degli impianti di condizionamento

Misure atte a garantire l'integrità e la disponibilità dei dati

La protezione di aree e locali

Indicare per ogni sede la disponibilità di

- dispositivi antincendio
- gruppo di continuità dell'alimentazione elettrica
- impianto di condizionamento

e in quali locali sono disponibili questi strumenti.

Indicare inoltre le misure di sicurezza per l'accesso ai locali:

- vigilanza
- chiavi di accesso
- chiavi di accesso alle zone critiche
- badge

Le misure logiche di sicurezza

E' obbligatorio che esista un sistema di autenticazione informatica, che mediante credenziali (username e password) permetterà di gestire anche i privilegi dell'utente sui vari servizi.

Per realizzare le credenziali di autenticazione si utilizzano i seguenti metodi:

- ad ogni incaricato viene assegnato un account **individualmente**, per cui non è ammesso che due o più incaricati possano accedere agli strumenti elettronici utilizzando il medesimo account
- la propria password non deve essere comunicata a nessuno
- nel caso in cui l'incaricato perda la qualità che gli consentiva di accedere allo strumento allora l'account sarà immediatamente disabilitato
- entro sei mesi di mancato utilizzo l'account andrà disabilitato
- le password devono essere composte da almeno otto caratteri (eventualmente includendo caratteri e numeri)
- al primo accesso al sistema verrà richiesto all'utente di cambiare la propria password
- ogni X mesi verrà richiesto all'utente di cambiare la propria password

Agli incaricati vengono impartite precise istruzioni in merito ai seguenti punti:

- obbligo di non lasciare incustodito e accessibile il computer, neppure in caso di breve assenza
- obbligo di elaborare in modo appropriato la password:
 - non devono contenere riferimenti riconducibili all'interessato (nomi, cognomi, soprannomi, date di nascita) né consistere in nomi noti

Account di amministrazione locali

Per quanto riguarda le password di amministrazione dei server, bisogna indicare

- su quali server sono impostate quali password
- da chi sono conosciute
- chi le può gestire

Antivirus

Deve essere disponibile un antivirus su ogni postazione e su ogni server.

Bisogna indicare

- il tipo di prodotto
- cosa va a proteggere
 - files locali
 - mail
 - traffico internet
- modalità di aggiornamento

Firewall

Deve esistere un firewall che protegga la rete e bisogna indicarne il funzionamento.

Andiamo ad ipotizzare di avere 3 sottoreti :

- **Esterna:** dedicata all'accesso ad internet e ad eventuali servizi che necessitano la totale disponibilità su internet (attualmente non ve ne sono)
- **DMZ:** dedicata ai servers che pubblicano servizi sia per la rete interna che su internet e a clients che necessitano particolari abilitazioni
- **Interna:** dedicata ai client e ai server dati o di infrastruttura che non necessitino di pubblicare servizi su internet

Il firewall permette il traffico nei seguenti sensi (elenco puramente esemplificativo):

Esterna -> Interna	Traffico non abilitato
Esterna -> DMZ	Traffico abilitato solo per i servizi che vogliamo pubblicare
Interna -> DMZ	Traffico abilitato
Interna -> Esterna	Traffico abilitato solo per i servizi che dobbiamo raggiungere su internet
DMZ -> Esterna	Traffico abilitato solo per i servizi che dobbiamo raggiungere su internet
DMZ -> Interna	Traffico Abilitato

Bisogna inoltre indicare se il firewall gestisce o protegge eventuali collegamenti VPN con altre sedi o altri partners

Criteria e modalità di ripristino dei dati

Bisogna indicare come si fronteggiano le ipotesi in cui i dati siano colpiti da eventi che possano danneggiarli, o addirittura distruggerli.

- RAID sui server
 - Su quali server sono disponibili i dischi in raid ?
 - Che modalità di raid è in uso ?

- Backup
 - A che ora vengono effettuati i backup ?
 - Che cosa viene backupato
 - Come avviene la rotazione delle cassette (o altri supporti) di backup ?
 - Dove vengono conservate le cassette (es.: cassaforte ignifuga) ?
 - Viene effettuato un test di restore periodico ?

- Crash recovery
 - Come si agisce in caso di guasto di un server ?
 - Reinstallazione su un hardware differente
 - Spostamento dischi su un hardware uguale

- Disaster recovery
 - Nel caso il cd venga reso inutilizzabile (inondazione/incendio), quali sono le politiche di riattivazione delle attività informatiche e del recupero dati ?

TABELLA DEI SINGOLI TRATTAMENTI

Per ogni server andiamo a definire una tabella riassuntiva di questo tipo

Gestionale	
ID trattamento	C
Descrizione	Server Gestionale
Natura dei dati trattati	Dati economici Anagrafiche clienti
Referente del titolare	Mario Rossi
Altre strutture (anche esterne) e funzioni che concorrono al trattamento	Azienda 1 (fornitore del sw gestionale) Azienda 2 (manutentore del sistema operativo)
Banca dati	Oracle / FoxPro / DB2 ecc...
Ubicazione fisica	CED
Strumenti utilizzati per il trattamento e tipologia di dispositivi di accesso	Server IBM Modello xyz 2 Dischi SCSI in Raid 1 -> Sistema Operativo 3 Dischi SCSI in Raid 5 -> Dati
Connessione	Rete Lan interna

MISURE DI SICUREZZA

<i>Antivirus</i>	Protezione applicativa dei server da virus, worm e simili
<i>Firewall + cluster</i>	Protezione logica da attacchi originati da internet
<i>Backup</i>	Disponibilità dei dati aggiornati al giorno precedente in caso di fault hardware
<i>Raid</i>	(Relativamente ad ogni server) Resistenza ai guasti di almeno un disco mantenendo attivi i servizi e l'integrità dei dati
<i>Ups</i>	Prevenzione dei picchi di corrente e della possibilità di eseguire un corretto shutdown degli apparati in caso di blocchi della corrente
<i>Condizionamento</i>	Prevenzione del surriscaldamento delle apparecchiature
<i>Anti incendio</i>	Possibilità di intervenire in modo manuale o automatizzato in caso di incendi
<i>Dual Power Supply</i>	Doppia alimentazione sui server per poter mantenere attivi i servizi in caso di guasto di un alimentatore o scollegamento erroneo di una presa di corrente

TIPI DI DATI TRATTATI

DATI SENSIBILI

Idonei a rivelare le origini razziali o etniche

Idonei a rivelare le convinzioni religiose; adesioni ad organizzazioni a carattere religioso

Idonei a rivelare le convinzioni filosofiche o di altro genere e le adesioni ad organizzazioni a carattere filosofico

Idonei a rivelare le opinioni politiche

Idonei a rivelare la adesione a partiti od organizzazioni a carattere politico

Idonei a rivelare la adesione a sindacati o organizzazioni a carattere sindacale

Idonei a rivelare lo stato di salute

Idonei a rivelare la vita sessuale

DATI GIUDIZIARI

Dati relativi a comportamenti illeciti o fraudolenti

Dati relativi a provvedimenti o procedimenti giudiziari

Dati relativi a provvedimenti o procedimenti sanzionatori, disciplinari, amministrativi o contabili

DATI DIVERSI DA QUELLI SENSIBILI E GIUDIZIARI

Nominativo, indirizzo o altri elementi di identificazione personale

nome, cognome, età, sesso, luogo e data di nascita

indirizzo privato, indirizzo di lavoro, numero di telefono, di telefax o di posta elettronica

posizione rispetto agli obblighi militari

dati fisici (altezza, peso, ecc.)

dati idonei a rivelare l'origine nazionale

Codice fiscale ed altri numeri di identificazione personale

carte sanitarie

numero carta di identità, passaporto, patente di guida, numero di posizione previdenziale o assistenziale

targa automobilistica

Dati relativi alla famiglia e a situazioni personali

stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare

Istruzione e cultura

curriculum di studi e accademico

pubblicazioni: articoli, monografie, relazioni, materiale audio-visivo, ecc.

titoli di studio

Lavoro

occupazione attuale e precedente

informazioni sul reclutamento, sul tirocinio o sulla formazione professionale

informazioni sulla sospensione o interruzione del rapporto di lavoro o sul passaggio ad altra occupazione

curriculum vitae o lavorativo, competenze professionali

dati relativi alle pregresse esperienze professionali

retribuzioni, assegni, integrazioni salariali e trattenute, beni aziendali in possesso del dipendente

dati sulla gestione e sulla valutazione delle attività lavorative

cariche pubbliche rivestite

dati relativi ad eventuali controversie con precedenti datori di lavoro

Beni, proprietà, possessi

proprietà, possessi e locazioni; beni e servizi forniti o ottenuti

Attività economiche, commerciali, finanziarie e assicurative

dati contabili, ordini, buoni di spedizione, fatture, articoli, prodotti, servizi, contratti, accordi, transazioni

identificativi finanziari, redditi, beni patrimoniali, investimenti

passività, solvibilità, prestiti, mutui, ipoteche

crediti, indennità, benefici, concessioni, donazioni, sussidi, contributi

dati assicurativi, dati previdenziali

dati relativi al comportamento debitorio

dati relativi all'affidabilità o puntualità nei pagamenti

dati relativi alla solvibilità economica

dati relativi all'adempimento di obbligazioni

dati relativi allo svolgimento di attività economiche e altre informazioni commerciali (es. fatturato, bilanci, aspetti economici, finanziari, organizzativi, produttivi, industriali, commerciali, imprenditoriali)

dati relativi a comportamenti illeciti o fraudolenti

dati relativi ad altri provvedimenti o procedimenti giudiziari

dati relativi ad altri provvedimenti o procedimenti sanzionatori, disciplinari, amministrativi o contabili