

SOMMARIO

SOMMARIO	1
Introduzione	2
Presentazione intervento.....	2
Corso incaricati e dipendenti	2
Ricognizione della sicurezza fisica	3
Inventario hardware e software.....	3
Schema di rete e dei collegamenti	3
Verifica delle misure di sicurezza	4
Test delle vulnerabilità locali	4
Test delle vulnerabilità remote	4
Individuazione dei trattamenti	4
Individuazione dei tipi di dati.....	5
Individuazione dei processi	5
Risk assessment & risk management.....	5
Designazione degli incaricati e dei responsabili	5
Redazione lettere di incarico	5
Redazione delle informative	6
Redazione del Documento Programmatico sulla Sicurezza	6
Modulistica per la gestione dei sistemi e della sicurezza	6
Presentazione dell'adeguamento effettuato	6
Previsione delle verifiche periodiche.....	6
Certificazione informatica del sistema (KERB).....	7
Certificazione indipendente sistema qualità di sicurezza delle informazioni secondo la norma internazionale ISO 27001	7

Introduzione

Prevediamo tre livelli di intervento: misure minime di sicurezza e privacy, certificazione del sistema informatico, certificazione del sistema di gestione delle informazioni. E' da intendersi che ogni livello necessita del precedente, ma che si può entrare da un cliente al secondo livello e prendere quanto di buono fatto da altri.

Di colore **rosso** le attività del primo livello, di colore **blu** le attività del secondo livello di intervento, in **verde** quelle del terzo livello, in **nero** le attività comuni a tutti i livelli (o comunque che si dovrebbero sempre svolgere).

Presentazione intervento

Vengono presentati i consulenti ed i tecnici che interverranno e le modalità dell'intervento.

Sono succintamente spiegate le attività da svolgere e le modalità di esecuzione delle varie analisi. Viene nominato un gruppo di lavoro comprendente un responsabile dei sistemi, un rappresentante della dirigenza ed il consulente.

Sono concordate le date delle successive visite.

Corso incaricati e dipendenti

Mediante la presentazione di slides vengono trattati gli argomenti relativi a privacy e sicurezza.

In particolare si dovrà parlare di:

- ④ cosa significa "privacy"
- ④ cosa significa "sicurezza"
- ④ la normativa attuale in materia di privacy
- ④ le figure e le definizioni previste dal codice
- ④ il trattamento di dati personali
- ④ responsabilità civili e penale nel trattamento di dati personali
- ④ i rischi relativi al trattamento di dati personali
- ④ le misure di sicurezza minime e necessarie
- ④ istruzioni agli incaricati

Viene redatto un registro con le firme dei partecipanti da allegare al DPS per dimostrare l'effettuazione della formazione obbligatoria. E' consegnato ai partecipanti un opuscolo contenente un sunto di quanto spiegato e norme basilari di comportamento.

Ricognizione della sicurezza fisica

Viene disegnata una pianta degli uffici con segnate le postazioni di lavoro, i server e gli apparati di comunicazione e di rete, nonché le finestre e gli accessi dall'esterno. Sono indicati anche eventuali impianti o apparati antincendio e anti-intrusione. E' redatta una descrizione degli uffici.

Viene verificata la robustezza degli infissi e serrature e l'eventuale possibilità di effrazione. Sono descritti impianti anti-intrusione, allarme, antincendio, di alimentazione ausiliaria, di condizionamento per la sala server.

Sono verificate l'efficienza di tali impianti e l'esistenza di certificazioni di rispondenza ai requisiti di legge da parte degli installatori (D.L. 626/94).

Vengono redatte se non esistenti procedure che descrivano l'operatività di tali apparati in condizioni normali ed in condizioni di emergenza.

Vengono valutate le banche dati e le politiche di accesso ai dati ivi conservati. Viene valutato il metodo di conservazione delle copie di backup.

Inventario hardware e software

Viene descritto il sistema informativo, a partire dall'infrastruttura di rete, server, apparati di comunicazione. Vengono elencati computer, modem, fax, fotocopiatrici, telefoni, cellulari, apparati bluetooth con le caratteristiche salienti. Vengono identificati masterizzatori, sistemi di backup, porte ed apparati USB od altri sistemi di memorizzazione portatili. Vengono altresì elencati notebook, palmari, impianti wifi connessioni esterne e collegamenti Internet.

Viene elencato il software installato su server e postazioni utente, controllando l'esistenza delle relative licenze d'uso. Vengono raccolti i dati di eventuali garanzie in essere, contratti di assistenza e assicurazioni stipulate. In questo contesto vengono analizzati in contratti di assistenza stipulati.

Schema di rete e dei collegamenti

Viene disegnato lo schema di rete, indicando server, postazioni, apparati di rete e di comunicazione. Viene riportata l'indicazione delle rete e sottoreti, indirizzi IP pubblici e privati, gateway, server DNS, DHCP, Dominio, firewall, proxy, mail server, ecc. Viene indicato il fornitore di connettività, eventuali siti web, Intranet, Extranet, connessioni remote, sia per remote banking che per altri servizi, server di accesso remoto, VPN e quant'altro.

Verifica delle misure di sicurezza

Viene verificata l'attivazione delle misure di sicurezza minime richieste dalla normativa.

Si verificano le policy relative a:

- ④ gestione delle credenziali di autenticazione ed autorizzazione
- ④ utilizzo dei sistemi
- ④ accesso alle aree
- ④ trasmissione dei dati personali
- ④ utilizzo dei supporti magnetici

Si verifica il piano di disaster recovery.

Test delle vulnerabilità locali

Viene effettuato un test mediante analizzatori software, al fine di individuare i servizi attivi, le condivisioni aperte, le versioni dei sistemi operativi e dei software applicativi e server, le patch mancanti, le vulnerabilità conosciute.

I risultati sono archiviati su supporto magnetico ed allegati alla documentazione.

Test delle vulnerabilità remote

Viene effettuato un test da remoto verso l'eventuale IP pubblico mediante analizzatori software.

Vengono analizzati gli apparati attraversati dai pacchetti per raggiungere il border router al fine di individuare eventuali punti critici. Attività di penetration test, DoS, od altre attività potenzialmente pericolose dovranno essere preventivamente autorizzate dopo che siano stati spiegati in maniera chiara e precisa intenti, modalità e rischi dei test che si intendono eseguire.

Ai report dovranno essere aggiunti i listati degli output degli strumenti di analisi di rete utilizzati.

Si effettueranno inoltre verifiche dei risultati ottenibili mediante uso specifico dei motori di ricerca.

Individuazione dei trattamenti

Mediante interviste vengono identificati i trattamenti effettuati. A titolo di esempio, gestione della contabilità, gestione di paghe e personale, ecc.

Sono individuati eventuali trattamenti in outsourcing.

In questa fase si individuano anche eventuali trattamenti effettuati senza strumenti elettronici.

Individuazione dei tipi di dati

Vengono elencati per ogni trattamento, anche mediante descrizione dei tracciati record, i dati gestiti (nome, cognome, ecc) indicando se si tratta di dati comuni, sensibili, giudiziari.

Individuazione dei processi

Per ogni trattamento vengono individuate e descritte, anche mediante l'uso di diagrammi, le operazioni alle quali sono sottoposti i dati personali gestiti dai vari trattamenti. Si può fare riferimento alla documentazione esistente per eventuali certificazioni di qualità già possedute.

Risk assessment & risk management

Per ciascun processo viene effettuata una analisi che tenuto conto della natura dei dati trattati e delle specifiche modalità di trattamento individua tutte le possibili minacce che possono affliggere i dati oggetto del processo e tutte le risorse di trattamento incluse quelle umane. La valutazione dei rischi viene fatta correlando minacce e vulnerabilità specifiche individuate per ciascun bene da proteggere, valutandone la probabilità di accadimento e la gravità del danno derivato. Per ciascun rischio rilevato vengono infine definite appropriate contromisure.

Designazione degli incaricati e dei responsabili

Vengono identificati gli operatori coinvolti nei processi individuati e ne viene fatta la designazione come incaricati del trattamento. Vengono, se necessario, designati i responsabili del trattamento. Sono individuati, per gli eventuali trattamenti in outsourcing, i responsabili od i titolari ai quali viene fatta comunicazione di dati personali. Viene redatto l'organigramma relativo alla gestione della privacy.

Redazione lettere di incarico

Una volta designati gli operatori che effettuano il trattamento si provvede a redarre le lettere di incarico. Possono essere sia nominali che indirizzate ad un gruppo omogeneo (p.e. Impiegati dell'ufficio personale). Per ogni trattamento si deve provvedere a specificare compiti e mansioni dell'incaricato, secondo quanto richiesto dall'art.30 del C.Pr. Se la manutenzione dei sistemi è affidata all'esterno, saranno nominati il gestore dei sistemi (personale interno) ed il responsabile della manutenzione (personale esterno). Saranno redatte le lettere ed i contratti per responsabili esterni in caso di trattamento in outsourcing, per i titolari di autonomo trattamento per la comunicazione di dati personali (p.e. commercialista, ecc.), le lettere di assunzione di responsabilità per eventuali terzi ammessi nei locali per funzioni di servizio (p.e. impresa di pulizie)

Redazione delle informative

Per ciascun trattamento saranno redatte appropriate informative che dovranno contenere tutte le informazioni specificate dall'art. 13 C.Pr. tenendo conto delle indicazioni fornite dal Garante (p.e. annunci di lavoro).

Redazione del Documento Programmatico sulla Sicurezza

Tutte le informazioni raccolte, le descrizioni dei trattamenti, i risultati delle valutazioni e dell'analisi di rischio, le misure di sicurezza, ecc. vengono riportate nel Documento Programmatico sulla Sicurezza, redatto secondo quanto disposto al punto 19 del disciplinare tecnico allegato B del C.Pr. A compendio del DPS può venire redatto un regolamento aziendale per l'utilizzo dei sistemi informatici e per la corretta gestione dei dati personali.

Modulistica per la gestione dei sistemi e della sicurezza

Vengono approntati i moduli necessari per mantenere la documentazione sullo stato dei sistemi, lo storico delle operazioni effettuate, le minacce riscontrate, gli adempimenti richiesti, ecc.

- ④ registro informative e consensi
- ④ registro firme di presenza
- ④ corsi di formazione
- ④ registro delle manutenzioni dei sistemi
- ④ registro delle assegnazioni e modifica password
- ④ registro e report incidenti di sicurezza
- ④ registro degli audit periodici

Presentazione dell'adeguamento effettuato

Al termine dell'intervento di adeguamento sarà buona norma concludere le attività con una riunione finale nella quale saranno presentati i documenti redatti e verrà consegnato un documento scritto riepilogativo contenente il rapporto finale ed eventuali indicazioni per una migliore gestione dei sistemi.

Previsione delle verifiche periodiche

Con la periodicità individuata nel DPS, saranno necessarie delle verifiche sul sistema in base ad una checklist preventivamente progettata.

Tali visite consentiranno di:

- ④ sorvegliare il corretto funzionamento dei sistemi critici e di apportare eventuali piccole correzioni su:
 - aggiornamenti di sicurezza dei sistemi operativi e dei software

- operatività dell'antivirus
- corretta esecuzione dei backup
- eventuale test di intrusione in presenza di servizi pubblici
- ④ registrare cambiamenti del sistema e conseguentemente modificare il DPS

Certificazione informatica del sistema (KERB)

Lo standard di sicurezza di base richiesto dalla normativa sulla privacy spesso non è sufficiente alle necessità dell'azienda. La nostra esperienza nel settore, ci ha consentito di definire un livello intermedio tra le misure minime richieste dalla normativa e la certificazione di sicurezza ISO 27001 che garantisce elevatissimi livelli di sicurezza; questo standard è comunque propedeutico alla certificazione ISO27001.

Il livello di certificazione di sicurezza da noi proposto si chiama KERB ed è da vedersi come l'evoluzione naturale di un sistema adeguato alla privacy.

I passi tipici di un progetto di questo tipo sono:

- ④ assessment iniziale dello stato della sicurezza delle informazioni del Cliente
- ④ individuazione degli obiettivi di sicurezza più adatti e del percorso di miglioramento successivo
- ④ impostazione del sistema di gestione, con supporto alla redazione dei necessari documenti
- ④ individuazione delle azioni di riorganizzazione necessarie per adeguare la struttura aziendale del Cliente a quanto richiesto dal sistema
- ④ formazione agli addetti al sistema (conoscenza della norma, conoscenza del sistema, tecniche di audit interno)
- ④ audit di certificazione
- ④ verifiche periodiche di sorveglianza e correzione dei sistemi di sicurezza critici

Certificazione indipendente sistema qualità di sicurezza delle informazioni secondo la norma internazionale ISO 27001

Lo Standard ISO 27001:2005 è una norma internazionale che fornisce i requisiti di un Sistema di Gestione della Sicurezza nelle tecnologie dell'informazione (Information Security Management System - ISMS). Lo standard è stato creato e pubblicato nell'ottobre 2005 a fini certificativi, in modo da costituire, assieme alla sua linea guida ISO/IEC 17799:2005, un sistema completo per garantire la gestione della sicurezza nella tecnologia dell'informazione.

Dal momento che l'informazione è un bene di fondamentale valore per qualunque organizzazione, e che ormai la maggior parte delle informazioni sono custodite su supporti informatici, ogni organizzazione deve essere in grado di garantire la sicurezza dei propri dati, in un contesto dove i rischi informatici causati dalle violazioni dei sistemi di sicurezza sono in continuo aumento.

L'obiettivo del nuovo standard ISO 27001:2005 è proprio quello di proteggere i dati e le informazioni da minacce di ogni tipo, al fine di assicurarne l'integrità, la riservatezza e la disponibilità, e fornire i requisiti per adottare un adeguato sistema di gestione della sicurezza delle informazioni (ISMS) finalizzato ad una corretta gestione dei dati sensibili dell'azienda.

La norma è applicabile a imprese operanti nella gran parte dei settori commerciali e industriali, come finanza e assicurazioni, telecomunicazioni, servizi, trasporti, settori governativi.

L'impostazione dello standard ISO/IEC 27001 è coerente con quella del Sistema di Gestione per la Qualità ISO 9001:2000, basandosi sull'approccio per processi, strutturato in politica per la sicurezza, identificazione, analisi dei rischi, valutazione e trattamento dei rischi, riesame e rivalutazione dei rischi, utilizzo di procedure e di strumenti come audit interni, non conformità, azioni correttive e preventive, sorveglianza, nell'ottica del miglioramento continuo. E' da vedersi come l'evoluzione naturale di un sistema adeguato alla privacy.

I passi tipici di un progetto di questo tipo sono:

- ④ assessment iniziale dello stato della sicurezza delle informazioni del Cliente
- ④ individuazione degli obiettivi di sicurezza più adatti e del percorso di miglioramento successivo
- ④ impostazione del sistema di gestione, con supporto alla redazione dei necessari documenti
- ④ analisi dei rischi, delle vulnerabilità, delle minacce, delle contromisure
- ④ individuazione delle azioni di riorganizzazione necessarie per adeguare la struttura aziendale del Cliente a quanto richiesto dal sistema
- ④ formazione agli addetti al sistema (conoscenza della norma, conoscenza del sistema, tecniche di audit interno)
- ④ simulazione di audit di certificazione

E' anche possibile, in questa fase, rendere il sistema ISO27001 organico ed integrato con la certificazione di qualità ISO9001, sia se quest'ultima già esiste nell'organizzazione, sia se il sistema viene costruito ex novo.

In questo caso i passaggi complessivi sono i seguenti:

- ④ individuazione e definizione delle aree aziendali interessate dal sistema di gestione integrato
- ④ analisi e documentazione dei processi aziendali in essere nelle aree interessate
- ④ assessment iniziale dello stato della sicurezza delle informazioni del Cliente
- ④ individuazione degli obiettivi di qualità e del percorso di miglioramento successivo
- ④ individuazione degli obiettivi di sicurezza più adatti e del percorso di miglioramento successivo
- ④ analisi di rischio
- ④ impostazione del sistema di gestione integrato, con supporto alla redazione dei necessari documenti (manuale integrato, politica della sicurezza, procedure, istruzioni operative, dichiarazione di applicabilità ecc.)

- ④ individuazione delle azioni di riorganizzazione necessarie per adeguare la struttura aziendale del Cliente a quanto richiesto dal sistema
- ④ formazione agli addetti al sistema (conoscenza della norma, conoscenza del sistema, tecniche di audit interno)
- ④ simulazione di audit di certificazione

Livelli	Attività
<u>livello 0</u>	Presentazione intervento
Attività comuni	Corso incaricati e dipendenti
	Risk assesment & risk management
	Presentazione dell'adeguamento effettuato
	Previsione delle verifiche periodiche
	Certificazione informatica del sistema (KERB)
<u>Livello 1</u>	Ricognizione della sicurezza fisica
Attività minime per la privacy	Inventario hardware e Software
	Schema di rete e dei collegamenti
	Individuazione dei trattamenti
	Individuazione dei tipi dati
	Individuazione dei processi
	Designazione degli incaricati e dei responsabili
	Redazione lettere di incarico
	Redazione delle Informative
	Redazione DPS
<u>Livello 2</u>	Verifica delle misure di sicurezza
Attività idonee – certificazione sistema informatico	Test delle vulnerabilità locali
	Test delle vulnerabilità locali
	Modulistica per la gestione dei sistemi e della sicurezza
<u>Livello 3</u>	Certificazione indipendente sistema qualità di sicurezza delle informazioni secondo la norma internazionale ISO 27001
Certificazione del sistema di gestione delle informazioni	