ASL SALERNO
AZIENDA SANITARIA LOCALE SALERNO

Privacy – Analisi dei Rischi

Data: Marzo 2011

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DATI PERSONALI E SENSIBILI

Azienda Sanitaria Locale Salerno

Redatto in conformità alla norma

DLGS 196/2003

Privacy – Analisi dei Rischi

Data: Marzo 2011

Copia n°

Allegati n°

	REDAZIONE	VERIFICA	APPROVAZIONE
	Responsabile del trattamento	Titolare del trattamento	Titolare del trattamento
Data			
Firma			

REVISIONI			
Riferimenti	Descrizione aggiornamento	Verifica	Approvazione

Privacy – Analisi dei Rischi

Data: Marzo 2011

ANALISI DEI RISCHI

Privacy – Analisi dei Rischi

Data: Marzo 2011

0. Premessa

La presente analisi risponde alla prescrizione introdotta dal Disciplinare Tecnico in materia di misure minime di sicurezza (Allegato B del D. Lgs. 196/2003) che impone alle Aziende e ad altri Soggetti Giuridici titolari di trattamenti di dati personali di predisporre ed aggiornare "entro il 31 marzo di ogni anno, un documento programmatico sulla sicurezza dei dati contenente idonee informazioni riguardo l'analisi dei rischi che incombono sui dati".

Lo scopo è quello di individuare i principali eventi potenzialmente dannosi per la sicurezza dei dati, valutarne le possibili conseguenze e la gravita e porli in correlazione con le idonee misure da adottare.

A livello internazionale è stato stabilito che la corretta gestione della sicurezza presuppone una metodologia di processo o ciclo continuo, in cui la "analisi dei rischi" innesca l'intero processo di gestione della sicurezza.

Le fasi concatenate in cui il ciclo è suddiviso sono:

- analisi dei rischi
- politiche di sicurezza
- piano di attuazione
- amministrazione della sicurezza
- audit test

per tornare poi nuovamente all'analisi dei rischi, ed innescare così il ciclo continuo.

La corretta gestione dei dati personali viene, con la nuova normativa di riferimento, considerata fondamentale per garantire la riservatezza di coloro cui appartengono i dati trattati, pertanto la sicurezza delle informazioni non è più un fatto esclusivamente legato alla difesa del patrimonio conoscitivo

dell'azienda e/o Soggetto Giuridico. In questo scenario, la valutazione dell'adeguatezza delle misure di sicurezza adottate è fondamentale per garantire la conformità alla normativa, ma soprattutto la tutela dei diritti dell'interessato.

Questo elemento innovativo trova nell'Azienda Sanitaria Locale Salerno una realtà già fortemente orientata alla difesa della privacy dei propri stakeholders in quanto consapevole della delicatezza delle informazioni in suo possesso. Tale impegno va, però, rivisto per arricchirsi della dimensione di tutela dei diritti degli interessati. Questa analisi, pertanto, tiene in debito conto il nuovo panorama di riferimento e si pone come obiettivo una corretta valutazione del rischio e della vulnerabilità, per adottare le più idonee misure di sicurezza.

Privacy – Analisi dei Rischi

Data: Marzo 2011

0.1 Stato attuale

Dall'analisi effettuata in Loco, in relazione al disciplinare tecnico in materia di misure minime di sicurezza (allegato B. Art da 33 a 36 del Codice), si evince che la struttura si trova a trattare dati di origine: comune, sensibile e giudiziaria.

Per quanto concerne la modalità di elaborazione del dato, questa può avvenire sia in forma cartacea che informatizzata.

I soggetti ai quali i dati trattati possono riferirsi sono: i pazienti; i dipendenti dell'azienda e i fornitori di beni e servizi.

L'utilizzo dei dati è effettuato soprattutto all'interno della struttura. La comunicazione dei dati con l'esterno è prevista per motivi di carattere ambulatoriale, sanitario o al fine di comunicazioni con le Istituzioni.

In genere, la modalità di comunicazione è a mezzo posta, a mezzo e-mail o attraverso il FSE (Fascicolo Sanitario Elettronico).

FRONT OFFICE E RACCOLTA DEI DATI:

Quasi ogni struttura è dotata di un front office diretto con l'utenza, inoltre c'è la disponibilità per colloqui privati con il personale, all'interno dei loro uffici.

Oltre che all'interessato, vengono fornite agli stakeholders le seguenti informative :

- Informativa dipendenti
- Informativa Curricula

- Informativa fornitori
- Informativa videosorveglianza

Non c'è la possibilità di fornire a terzi i dati dell'interessato, se non per l'adempimento delle funzioni Istituzionali dell'Azienda, secondo quanto riportato nel modello: "Informativa per l'interessato", oppure in conseguenza di esplicito e dettagliato consenso dell'interessato stesso.

GARANZIA RISERVATEZZA DEI DATI:

Vi è un corretto utilizzo di fax e stampanti nelle zone di libero accesso al pubblico. Nei corridoi sono presenti delle fotocopiatrici, munite di codice.

Vi è l'utilizzo di fax e stampanti multiuso, ma per la distruzione della documentazione cartacea, è presente nella maggioranza degli uffici una macchina distruggi documenti. C'è la presenza di contenitori per la raccolta differenziata carta, il cui smaltimento è affidato a soggetti esterni.

Per tutto il personale non c'è una casella di smistamento posta.

Ogni incaricato ha un pc personale.

PROTEZIONE AREE E LOCALI:

L'intera struttura è controllata con Sistemi di Sicurezza.

Privacy – Analisi dei Rischi

Data: Marzo 2011

PROTEZIONE ARCHIVI E SUPPORTI:

Non in tutti gli uffici vi è la presenza di armadi muniti di serratura dove vengono conservati documenti ed atti, e, inoltre, non sono correttamente tenuti chiusi a chiave.

Gli archivi non vengono chiusi a fine giornata e dopo la chiusura, potrebbe essere possibile accedervi.

Manca un registro di prelievo degli atti e documenti con l'indicazione dei nominativi, del giorno e della motivazione.

E manca l'individuazione di un responsabile che detenga la copia delle chiavi degli uffici al fine di poterla correttamente custodire.

Per quanto riguarda i supporti informatici (penne USB, hard disc portatili…) la situazione è da normare con apposito regolamento; infatti si utilizzano supporti personali che, in quanto tali, non sono controllati adeguatamente. Essi, ad esempio, possono essere portati fuori dalla struttura e questo può portare a un'impropria diffusione dei dati. Per cui, è necessario attuare una policy aziendale che normi il corretto utilizzo degli stessi.

MISURE DI SICUREZZA:

In merito al trattamento dei dati, tutti i soggetti che trattano dati sono stati debitamente informati sulle modalità di custodia ed uso dello strumento di autenticazione personale e vengono effettuati periodici controlli per verificare il rispetto delle istruzioni impartite.

Per l'attivazione del programma di autenticazione dell'utente vi è un corretto utilizzo di un sistema di autorizzazione basato su profili, in concomitanza all'utilizzo di password personale di accesso alla stazione.

Manca un registro delle violazioni o delle tentate violazioni, che individui situazioni potenzialmente anomale, ma è in corso di installazione un nuovo sistema informativo che consenta tale funzionalità.
Non viene effettuata, ad intervalli periodici, un'analisi del rischio del sistema informativo.
Non è possibile ricostruire l'attività svolta da un incaricato, e, inoltre, non sono state impartite delle istruzioni in merito all'uso riservato e sicuro di collegamenti con il mondo esterno (internet, posta elettronica), ma i sistemi sono comunque configurati per impedire un'intrusione dall'esterno o la fruizione di contenuti impropri dall'interno.
Manca un programma impostato per la suddivisione delle tipologie di dati sensibili critici, rispetto ad altri dati sensibili che limiti e controlli l'accesso a tali dati. Si sottolinea, però, che la compartimentazione è intrinseca a ciascuna area plicativo/gestionale del sistema informativo.
Il controllo delle operazioni svolte dagli addetti alla manutenzione software/hardware è esperito dall'Amministratore di Sistema *in House* nella persona del Dirigente Ufficio CED, **Dott. Vito Gianni**. Tale controllo è fatto per verificare che, durante tali operazioni, essi non possano accedere, nemmeno accidentalmente, a dati personali che non rientrino nel loro profilo di autorizzazione.
Vengono attuate delle procedure per salvaguardare la sicurezza dei dati, dopo il riavvio del sistema, in seguito al verificarsi di un'anomalia.
Sono stati installati applicativi che blocchino automaticamente un terminale se non viene utilizzato per un periodo predeterminato di attività.
Invece, non è stato sviluppato un piano di ripristino e continuità dell'operatività del sistema.
Esistono procedure che permettano di identificare con chiarezza i supporti informatici mobili o asportabili dove sono archiviati dati sensibili, per quanto attiene ai dati inerenti il sistema informativo aziendale.
Sono installati degli applicativi in grado di bloccare tempestivamente virus o possibili tentativi di

penetrazione dall'esterno e vengono effettuate a scadenza regolare le verifiche circa l'aggiornamento dei sistemi operativi.

Non sono usate particolari cautele in merito all'utilizzo di personal computer mobili come notebook, laptop, macchine fotografiche digitali, cellulari con tastiera e simili, questo perché tali dispositivi non accedono all'infrastruttura informatica aziendale.

È stato sviluppato un piano di ripristino e di continuità dell'operatività del sistema, ma l'ultima sperimentazione è stata fatta in momenti precedenti superati.

Non è stata effettuata, in maniera sistematica, un'analisi delle vulnerabilità presenti sulle reti di comunicazione elettronica, sia all'interno che all'esterno della struttura di trattamento dei dati.

Il tutto sarà oggetto di tempestiva verifica ed opportuni accorgimenti, anche attraverso un nuovo strumento regolamentare per l'utilizzo degli strumenti elettronici.

PIANIFICAZIONE DELLE MISURE MINIME DI PROTEZIONE E PREVENZIONE:

- Impianto d'allarme: adottato
- Protezione con serratura: adottato
- Estintori/impianti anti-incendio: adottato
- Gruppo statico di continuità (UPS): adottato
- Password personale di accesso: adottato
- Sistema di autorizzazione basato su profili: adottato
- Accesso mediante controllo di indirizzo di rete: da adottare
- Backup: adottato
- Copie multiple: adottato

- Informazione/formazione specifica sul rischio: adottata
- Proxy server: adottato
- Firewall: adottato
- Antivirus: adottato.
- Manutenzione hw/assistenza sw: adottata

1. Le dimensioni della sicurezza

Sostanzialmente, la protezione dei dati è garantita mediante una sicurezza a tre dimensioni:

- **logica**
- **fisica**
- **organizzativa/comportamentale**

1.1 sicurezza logica

Il campo di applicazione della *sicurezza logica* riguarda principalmente la protezione dell'informazione, e di conseguenza di dati, applicazioni, sistemi e reti, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo. Le contromisure di *sicurezza logica* sono da intendersi come l'insieme di misure di carattere tecnologico e di natura procedurale ed organizzativa che concorrono nella realizzazione del livello di sicurezza da raggiungere.

E' importante che siano sempre disponibili e funzionanti i prodotti software posti a presidio della sicurezza dei dati trattati e che sia garantita la puntualità dei salvataggi per la continuità del servizio.

Inoltre, per garantire la riservatezza delle informazioni, l'accesso ai dati non deve essere consentito a persone non autorizzate e i dati devono essere resi disponibili solo a chi ha necessità di utilizzarli per svolgere le proprie funzioni. Pertanto i Responsabili del trattamento dovranno assicurare:

1. l'assegnazione delle relative autorizzazioni, ad ogni incaricato;
2. l'applicazione di metodologie nell'area della sicurezza della gestione degli User ID e la revisione periodica delle autorizzazioni agli accessi ai software applicativi ed ai relativi dati personali;
3. la congruità tra le autorizzazioni rilasciate e le definizioni di sicurezza dei sistemi informatici su cui transitano i dati personali;
4. l'uso di metodologie di controllo accessi che prevengano violazioni di sicurezza intenzionali o accidentali.

È esempio di corretta diligenza che l'Azienda conduca specifici audit periodici sulla corretta esecuzione, da parte del responsabile, delle misure tecniche
di sicurezza. Poiché eventuali errori esporrebbero l'Azienda a responsabilità per danni particolarmente accurata deve essere la procedura interna e relativa sia alla verifica della veridicità dell'informazione, sia alla correzione dei dati personali accertati come errati.

1.2 sicurezza fisica

Sono le funzioni di sicurezza che il sistema dovrà garantire su tutte le piattaforme ed a tutti i livelli di elaborazione. Sono individuati i seguenti servizi di sicurezza:

- autenticazione: verificare e confermare che l'identità dichiarata di un utilizzatore sia autentica;
- controllo accessi: i dati personali saranno fisicamente protetti dall'accesso non autorizzato da parte di terzi che non siano incaricati del trattamento o utenti;

- **confidenzialità;**
- **integrità: assicurare che i dati trattati non siano alterati o falsificati;**
- **non ripudio: assicurare il trattamento sia probabile.**

1.3 sicurezza organizzativa/comportamentale

Accanto all'adozione di misure tecnologiche, è necessario che vengano definite una serie di norme e procedure miranti a regolamentare gli aspetti organizzativi del processo di sicurezza e regole comportamentali per gli Incaricati dei trattamenti.

Gli aspetti organizzativi riguardano principalmente:

- **la definizione di ruoli, compiti e responsabilità per la questione di tutte le fasi de processo di sicurezza;**
- **l'adozione di specifiche procedure che vadano a completare e rafforzare le contromisure tecnologiche adottate.**

Un ulteriore aspetto inerente la sicurezza organizzativa è quello concernente i controlli sulla consistenza e sulla affidabilità degli apparati. In ordine alle norme di comportamento, si rimanda a quanto è definito nei documenti di nomina per l'assegnazione di responsabilità ed incarichi.

2. Sicurezza minima e Sicurezza adeguata

Il D. Lgs. 196/2003, nell'Allegato B "Disciplinare Tecnico in materia di Misure minime di sicurezza", individua le misure minime da adottare in caso di trattamento dei dati con o senza strumenti elettronici.

Il Titolare e i Responsabili hanno l'obbligo di adottare delle misure tecnico-informatiche, organizzative e logico-procedurale, in grado di rispettare quanto previsto dalla normativa.

Le misure minime devono garantire che i dati siano riservati, vale a dire che si mettano in atto tute le forme di prevenzione per scongiurare i rischi di utilizzi indebiti di informazioni. In pratica i dati devono essere accessibili solo alle persone autorizzate, pertanto è necessaria un'ottima conoscenza del flusso dei dati dall'interno all'esterno dell'attività.

Tuttavia la misura minima può non essere quella che garantisce al Titolare e ai Responsabili del trattamento il rispetto delle più generiche, ma più pressanti prescrizioni dell'art.31 del D. Lgs. 196/2003, che impone specificatamente che vengano adottate idonee e preventive misure di sicurezza.

tra le misure minime individuate, è presente la stessa Analisi dei Rischi. Essa ha lo scopo di individuare i principali eventi potenzialmente dannosi per la sicurezza dei dati, valutarne le conseguenze e la gravità e porli in correlazione con le misure previste. In altre parole, oggetto dell'analisi deve essere la valutazione di conformità dell'Azienda alle misure minime ma soprattutto il giudizio di adeguatezza del sistema di sicurezza adottato dalla stessa.

Contrariamente alle minime, le misure idonee non sono identificate analiticamente ma sono identificabili dai Titolari e da Responsabili del trattamento al fine di ridurre al minimo i rischi di:

- distruzione o perdita, anche accidentale dei dati stessi;

- **accesso non autorizzato;**
- **trattamento non consecutivo;**
- **trattamento non conforme alle finalità della raccolta.**

Il giudizio di adeguatezza, come indicato dall'art.33 del D. Lgs. 196/2003, deve essere parametrizzato in base ai seguenti criteri:

- **le conoscenze acquisite in base al processo tecnico;**
- **la natura dei dati;**
- **le specifiche caratteristiche del trattamento.**

La sicurezza è il frutto di un'attività composita e permanente. Non esiste una sicurezza assoluta ma una tendenza ottimale verso la minimizzazione del rischio in considerazione della tutela dei diritti. Essa richiede interventi di tipo organizzativo, fisico e logico sottoposti a continuo aggiornamento e verifica. Il tutto condito con un adeguato programma di informazione e sensibilizzazione ai diversi livelli dei responsabili dei dati personali e degli eventuali servizi esterni.

I dati personali devono essere protetti senza considerare la loro forma o il supporto (cartaceo, informatico o di altro tipo) su cui sono registrati. Si ricorda, infatti, che entrano nella definizione di dato personale anche immagini e suoni quando idonei ad individuare un soggetto.

Le misure minime di sicurezza devono essere adottate da tutti coloro che, per le attività svolte rientrano nell'ambito applicativo del D. Lgs. 196/2003; quindi non solo dall'Azienda, Titolare del trattamento, e pertanto dai membri della stessa, ma anche da quei terzi che utilizzano tali dati per conto dell'Azienda.

3. Piano dell'analisi

Sulla base delle precedenti considerazioni, l'Analisi dei Rischi in oggetto è stata effettuata applicando due distinti criteri di valutazione:

a. verifica della conformità formale alle misure minime prescritte dal D. Lgs. 196/2003;
b. verifica dell'adeguatezza del sistema di sicurezza operante presso l'Azienda.

4. Metodologia

L'analisi dei rischi ha tenuto conto obiettivamente dell'aderenza delle misure adottate dall'Azienda Sanitaria Locale Salerno con quelle minime prescritte dal Disciplinare. Si è poi effettuata una valutazione dell'efficacia di tali misure, frutto del giudizio degli analisti, che ha tenuto conto anche dell'odierno sviluppo tecnologico.

L'analisi del rischio tiene conto di tutti i rischi, anche potenziali, a cui sono soggetti i dai trattati dall'Azienda e delle cause che li possono attivare. L'azione di riduzione o eliminazione del rischio può, quindi, agire su due elementi: eliminazione o riduzione del rischio, eliminazione o riduzione delle cause che lo possono attivare.

La conduzione di un'efficace analisi del rischio necessità di elementi di conoscenza relativi all'attività nel suo complesso, al flusso di dati, allo stati e alla gestione della struttura, alle metodologie. Devono altresì essere analizzati i fattori di rischio legati ad eventi accidentali legati alla specifica attività dell'Azienda, nonché quelli legati ad attività saltuarie.

Tutte le informazioni necessarie sono state raccolte intervistando i membri dell'Azienda.

Perché i dati siano soggetti ad un rischio occorre che una minaccia sfrutti una o più vulnerabilità presenti nel sistema di sicurezza. E' ovvio che a parità di minaccia, livelli di vulnerabilità diverse, generano livelli di rischio differenti.

5. Definizioni

MINACCIA (M)

Intendiamo per minaccia, un qualsiasi incidente potenziale che mette in pericolo le informazioni ed i dati in possesso dell'Azienda. Ciò avviene quando, per cause intenzionali o accidentali, una minaccia è in grado di sfruttare una carenza dei sistemi, dell'organizzazione, delle applicazioni e dei servizi.
L'individuazione preventiva delle minacce consente di meglio tarare il sistema di sicurezza dell'Azienda in relazione ai rischi che potrebbe incontrare.
Le minacce possono essere distinte in base a:

- *ORIGINE*:
  - interna: dovuta al comportamento dei membri dell'Azienda;
  - esterna: dovuta al comportamento degli utenti o di terzi;
  - ambientale: dovuta ad eventi accidentali, sia tecnici sia disastrosi, che possono danneggiare il sistema informativo nel suo complesso o qualcuno dei suoi componenti chiave;
- *CAUSA*:
  - carenze organizzative: responsabilità non bene individuate o assegnate, carenze procedurali o di controllo;

- **colpa: incuria, ignoranza o imperizia nei comportamenti degli addetti o degli utenti;**
- **dolo: volontà di impossessarsi indebitamente delle informazioni o di recare danno.**

Le più importanti minacce prese in considerazione sono:

- **<u>intercettazione</u>: accesso no autorizzato alle informazioni da parte di terzi interni o esterni non autorizzati;**
- **<u>alterazione</u>: modificazione non autorizzata da parte di persone non autorizzate delle informazioni o del software di gestione dati;**
- **<u>perdita</u>: distruzione, danneggiamento o impedimento all'uso dei dati, apparecchi o dei supporti informatici;**
- **<u>divulgazione</u>: accesso da parte di soggetti non autorizzati per legge a informazioni personali e/o dati sensibili non divulgabili;**
- **<u>trattamento illecito o non conforme alle finalità della raccolta</u>: consiste nella realizzazione di situazioni di fatto non conformi alla finalità della raccolta e comunque alle prescrizioni di legge.**

Privacy – Analisi dei Rischi

Data: Marzo 2011

VULNERABILITÀ (V)

Intendiamo per vulnerabilità, la capacità del sistema di sicurezza dell'Azienda di contrastare le minacce valutate.

DANNO (D)

Intendiamo per danno l'insieme delle conseguenza derivanti dal verificarsi dell'evento negativo.

Il rischio viene valutato applicando la seguente formula:

RISCHIO = PROBABILITA' MINACCIA x VULNERABILITA' x DANNO

$$R = M \times V \times D$$

La valutazione del livello di rischio per ogni area è stata effettuata tenendo conto dei seguenti elementi:

a. **livelli di vulnerabilità;**
b. **minacce ipotizzabili;**
c. **probabilità di accadimento;**

d. **qualità delle informazioni (anonime, personali, sensibili).**

Il numero indicato con la lettera R, risultante del prodotto di fattori MxVxD, rappresenta per l'Azienda Salernitana un indice della gravità dello specifico rischio residuo. In funzione del valore numerico di R vengono programmati gli eventuali interventi di miglioramento del livello di prevenzione e protezione.

6. Analisi di conformità

L'analisi dei rischi che incombono sui dati prende in considerazione le entità da proteggere e le circostanze potenziali che possono causare un danno.
Lo scopo che ci si pone è anche rapportare al rischio lo sforzo umano ed economico da compiere per difendere un bene, che si presenta sia sotto forma materiale che immateriale (il dato, l'informazione).
Risulta difficile stimare sia la probabilità di un evento, sia la probabilità che un individuo riesca a sfruttare bachi o mancati aggiornamenti di un sistema operativo o di un programma, o particolari situazioni venutesi a creare a livello di social engineering o di rapporto interpersonale.
Tutte le considerazioni che seguono sono quindi una stima, approssimata, del rischio e dei costi correlati.

6.01. Minacce per le risorse hardware

Le principali minacce per le risorse hardware sono:

- ***Mal funzionamenti dovuti a guasti*: Le minacce dovute ai guasti delle apparecchiature informatiche (server ed apparecchiature di rete) possono avere effetti diversi a seconda**

dell'importanza della macchina in questione.

Nel caso si tratti di un computer di sportello questo può essere facilmente e velocemente sostituito da una riserva, sempre disponibile, in quanto prevista o reperibile nel retro ufficio; nel caso il guasto riguardi server o nodi di reti invece il rischio può essere molto elevato e potrebbe bloccare le sedi ospedaliere per alcuni giorni.

Questo causerebbe possibili aggravamenti dei problemi di salute dei pazienti, in quanto potrebbero mancare referti importanti e necessari per il monitoraggio di patologie gravi ed acute.

Vi sarebbe un grave disagio in quanto dovrebbero essere riattivati dei pedonaggi per il trasporto di informazioni, precedentemente aboliti grazie alla informatizzazione (basti pensare alle prenotazioni di prestazioni per interni ed alla ricezione dei referti dai servizi di Laboratorio Analisi, Centro Trasfusionale ed Anatomia Patologica). Si avrebbe quindi una situazione di P (probabilità) variabile da 2 a 3 (da poco probabile a probabile, vista l'esperienza empirica degli ultimi 5 anni) con un possibile danno D, sia per possibili rivalse assicurative, sia per i costi economici dovuti alla perdita di ore lavorative che superebbero facilmente i 32.000 euro (supponendo che per due giorni 200 persone perdano 1 ora di lavoro a testa ogni giorno) a causa di un blocco completo del sistema informatico; a questo si aggiungerebbero danni rilevanti per l'immagine dell' Azienda, ed il lavoro necessario per un ripristino, probabilmente difficile, della situazione. Il problema diverrebbe anche sociale e politico. Si avrebbe quindi come risultato (R=PxD) un Range per lo meno grave ma probabilmente gravissimo.

- *Mal funzionamenti dovuti a sabotaggi, furti, manomissioni*: **le considerazioni sono analoghe a quelle precedenti, per quel che riguarda le probabilità ed i costi che ne scaturirebbero.**
  Misure di sicurezza di tipo fisico: custodia e presidio dei locali; chiusura a chiave degli stessi; verifica della robustezza e funzionalità dei sistemi di chiusura.

- *Mal funzionamenti dovuti ad incendi o catastrofi naturali*: **le considerazioni sono analoghe a quelle precedenti, forse con una probabilità minore.**
  Misure di sicurezza di tipo fisico: dotazione di dispositivi antincendio, conservazione delle copie di sicurezza e dei supporti ausiliari di memorizzazione in un locale diverso da quello ove sono custoditi i server; per il resto risulta difficile una protezione contro catastrofi naturali, per fortuna poco probabili; c'è da osservare che una catastrofe naturale (ad esempio un terremoto) probabilmente bloccherebbe comunque i Presidi Ospedalieri.

- *Intercettazioni, in particolare per le reti e le connessioni wireless*: **Per quel che riguarda le intercettazioni, queste possono essere fatte accedendo al mezzo fisico che trasporta i segnali elettrici o elettromagnetici;**
  Nel primo caso un computer connesso alla rete potrebbe, mediante opportuni programmi, intercettare pacchetti in rete; nel secondo caso, un computer dotato di un'antenna ed un ricevitore anche integrati in una scheda wireless potrebbe ricevere segnali trasmessi anche da notevoli distanze.
  Per quel che riguarda la probabilità questa potrebbe nel primo caso variare ancora da poco probabile a probabile, nel secondo caso potrebbe essere da probabile a molto probabile, visti i casi noti, anche involontari, di intercettazione di altrui reti non protette. Il danno potrebbe

variare da 1 a 4 a seconda del fatto che non possa o possa essere richiesto un risarcimento in sede civile, per carenze di privacy.

Per quel che riguarda il primo caso si ricorre alle misure di sicurezza di tipo logico: in particolare, si predispone un sistema centralizzato antivirus, si realizzano dei sistemi antintrusione sulle linee di comunicazione, si monitorizza l'accesso alla rete le particolari tipologie di collegamenti, nonché le schede di rete attive in modalità promiscua, mediante un sistema IDS. Si ricorre inoltre ad un sistema di policy per definire cosa è permesso e cosa è vietato; tali policy, implementate inizialmente localmente e poi progressivamente mediante dominio, andranno a bloccare comportamenti potenzialmente pericolosi, quali l'installazione di software, il cambio delle configurazioni nei computer, l'attivazione di periferiche hardware (schede wireless, periferiche usb, dischi removibili, etc.) oltre a quelle previste.

Per quel che riguarda le comunicazioni wireless, si ricorda che la portata di una comunicazione, nelle bande di frequenza utilizzate, può essere riassunta nella seguente formula approssimata:

Portata in Km= 4 x Radice_quadrata (altezza antenna in m)

Esempio: se l'antenna si trova a 25 metri di altezza, la portata è di 20 km; Se l'antenna si trova in una zona collinare che si affaccia sulla pianura, a 300 m di quota, la portata è di circa 68 km. Con antenne direttive anche di piccole dimensioni, ed eventualmente un amplificatore di segnale, può essere captato un segnale anche debole da notevole distanza.

In pratica non si può contare sul confinamento del campo elettromagnetico in una zona limitata, per cui tale tipo di comunicazione dovrà essere obbligatoriamente crittografata e sicura, o non permessa.

- *Malfunzionamenti dovuti a black-out ripetuti o di durata anomala, o a sbalzi eccessivi dell'energia elettrica*: **L'interruzione dell'energia elettrica può procurare notevoli danni ai server, causando la corruzione di files riguardanti il sistema operativo o i database, o comunque causando la corruzione di transazioni in atto e non completate. La probabilità è elevata, soprattutto nella stagione estiva; possiamo senz'altro ipotizzare che P vari da 3 a 4; il danno può variare da 1 a 4.**

  Per tale motivo si intende utilizzare dei sistemi che garantiscano la continuità dell'energia elettrica per i server. La situazione minima da garantire è la presenza di un gruppo di continuità statica; la soluzione ottimale quella di un gruppo elettrogeno con controllo della continuità della tensione erogata e del suo valore.

  Per questa minaccia si fa riferimento alle misure di sicurezza di tipo fisico: ridondanza e continuità della alimentazione elettrica.

6.02. Minacce per le risorse software

- *Presenza di errori involontari dovuti alla fase di progettazione e/o di implementazione o di installazione del software*: **Questo tipo di errore è molto frequente, anche dato il notevole numero di pacchetti software installati su tutti i server sia Unix, che Windows; la probabilità di un errore di tale tipo sarà sicuramente di un valore che va da 3 a 4 (probabile, altamente probabile) nella fase di prima installazione ed avviamento di una nuova procedura. I problemi generalmente creati sono l'impossibilità di utilizzo di una particolare procedura e più frequentemente di una particolare maschera della procedura; generalmente il problema è risolvibile nel giro di poco tempo; il danno comunque potrebbe essere di tipo Lieve o Medio (1**

o 2) con una risultante di valore Medio.

Misure di sicurezza di tipo logico: in particolare si eseguirà un test sistematico degli applicativi, in ambiente di prova, prima della messa in produzione. In modo analogo si effettuerà un test, in ambiente di prova di tutte le modifiche e gli aggiornamenti, prima che vengano messe in produzione.

- *Presenza di codice malizioso o di virus, worms, trojans*: **A questo tipo di minaccia, frequentissima per quel che riguarda la presenza di virus e la possibilità di ingresso attraverso i canali di comunicazione con l'esterno, a cui senza dubbio, vedendo a posteriori il numero di casi intercettati nelle console dell'antivirus, si da probabilità P pari a 4; per quel che riguarda gli effetti economici e di immagine, questi possono essere notevoli, basti pensare al possibile blocco di server degli applicativi basati su Windows 2000, o al blocco di un servizio importante quale un laboratorio analisi, un centro trasfusionale o una anatomia patologica che abbiano tutti client di tipo Windows per le funzioni fondamentali di accettazione o refertazione. Questo causerebbe possibili aggravamenti dei problemi di salute dei pazienti, in quanto potrebbero mancare referti importanti e necessari per il monitoraggio di patologie gravi ed acute.**

  In tali casi il danno economico può essere notevole, comportando il blocco (in taluni casi) dei pc e la necessaria riformattazione e reinstallazione degli stessi. Anche l'immagine dell'Azienda sarebbe notevolmente deteriorata. Nel 2004 le maggiori casistiche rilevate da McAfee per quel che riguarda i virus che impattano sulle imprese sono le seguenti:

- **Bots: programma automatico che risponde ai comandi remoti, paragonabile ad un robot, e che può eseguire il download ed installazione di adware nella macchina della vittima;**
- **Mass Mailers: programmi che hanno la capacità di propagarsi via posta elettronica, disponendo di un motore proprio per la posta e della capacità di utilizzare gli indirizzi di posta della vittima;**
- **Exploits: programmi che sfruttano le vulnerabilità del software;**
- **Adaware/Spyware: programmi che raccolgono informazioni sulla vittima con scopi commerciali.**

Le misure per ridurre il rischio sono: predisposizione ed aggiornamento antiviurs, mediante sistemi centralizzati ed automatici.

- *Attacchi di tipo "interruzioni di servizio", attacchi non distruttivi ma capaci di saturare le capacità di risposta di un sistema*: **Gli attacchi di questo tipo possono avere origine dall'esterno della rete aziendale, con conseguenze anche gravi. Si stima che la probabilità possa essere di valore 2 o 3, il danno si stima lieve in quanto per ripristinare le normali funzionalità basterà riavviare i servizi o i sistemi; si intende ridurre tale probabilità sia adottando delle protezioni perimetriche mediante appositi software di firewalling, sia utilizzando software antivirus, sia utilizzando un apposito software antiintrusione, sia adottando delle particolari configurazioni per i router. Si fa riferimento alle Misure di sicurezza di tipo logico.**

6.03. Minacce a cui sono sottoposti e dati trattati

- *Accesso non autorizzato agli archivi*: **L'accesso non autorizzato agli archivi di dati è una minaccia che può essere probabile se non vengono adottate le necessarie misure logiche ed organizzative; senza tali misure la probabilità P si può supporre essere alta (P=4), mentre il costo di questo evento potrebbe essere quello della richiesta di uno o più risarcimenti in sede civile, dovuti a violazione della privacy delle informazioni personali. A tali minacce si risponde, al fine di ridurre sia la probabilità che il danno, con l'insieme delle misure fisiche, logiche ed organizzative, in particolare facendo riferimento ai profili di autorizzazione.**

- *Modifiche deliberate dei dati*: **Vale quanto detto per il punto precedente; più difficile risulta controllare la modifica deliberata, da parte di un utente autorizzato; questo comporterebbe che ogni applicativo registri le modifiche effettuate di qualunque tipo queste siano, e tenga anche una storia delle modifiche, non memorizzando solo l'utente che ha eseguito l'ultima modifica su un record.**
  Si fa riferimento alle misure di sicurezza logiche (sistema di autorizzazione, codici identificativi personali) e l'esecuzione periodica dei salvataggi.

- *Errori involontari commessi dagli incaricati del trattamento*: **In questo caso la probabilità dell'errore involontario può essere ridotta aumentando l'insieme dei controlli sulla consistenza relazionale e sulle regole di validità dei dati utilizzati dalle procedure, utilizzando programmi user-friendly ed ad interfaccia grafica, e con una adeguata formazione.**
  Per gli errori involontari dovuti a cancellazioni di uno o più record, si ricorre all'utilizzo dei

salvataggi, per i quali vengono date precise istruzioni.

A tale scopo si fa riferimento al paragrafo relativo alla formazione degli incaricati del trattamento, per quel che riguarda i salvataggi periodici dei dati.

6.04. Minacce per i supporti di memorizzazione

- *Distruzione o alterazione a causa di eventi naturali:* **In questo caso il rischio è che vengano persi copie di dati o dati storici; la misura precauzionale consiste nell'avere più copie dei supporti ritenuti importanti e di conservarli in luoghi fisici distinti, in appositi contenitori (armadi, meglio se armadi ignifughi, casseforti ignifughe).**

  Generalmente questi eventi, sono poco probabili. I danni possono essere enormi. Si fa riferimento in questo caso alle misure fisiche di sicurezza.

- *Azioni accidentali e comportamenti intenzionali:* **Anche in questo caso si intende predisporre un numero multiplo di copie per gli archivi ritenuti più importanti. Inoltre i supporti fisici vanno conservati entro locali o contenitori chiusi a chiave.**

  Si fa riferimento in questo caso alle misure fisiche di sicurezza.

- *Deterioramento nel tempo*: **Tale deterioramento coinvolge tutti i supporti magnetici, in quando il supporto stesso può presentare un deterioramento nel tempo: un esempio calzante è quello dei dischetti o dei nastri magnetici depositati in armadi da molto tempo. La probabilità di avere dati importanti in qualche floppy o nastro magnetico è improbabile (P=1) in quanto i dati fondamentali sono accentrati nei server sanitari ed amministrativi; il danno potrà essere lieve.**

Privacy – Analisi dei Rischi

Data: Marzo 2011

- *L'evoluzione tecnologica e del mercato*: **Va tenuta in considerazione anche la veloce obsolescenza di apparati e sistemi di input/output; per tale motivo alcuni sistemi di lettura/scrittura non sono già più utilizzabili (basti pensare ai dischi da 5 pollici ed ¼ oppure ad alcuni tipi di nastri magnetici). Inoltre va tenuto in considerazione anche il modo con cui i dati sono memorizzati nei supporti stessi, ovvero il programma utilizzato per eseguire tale memorizzazione.**

  Se il programma non è disponibile perché obsoleto, va fatta la conversione in modo che i dati siano memorizzati in un formato leggibile. Valgono le stesse considerazioni fatte al punto precedente. Quando si attiverà il protocollo informatico, diventerà un punto fondamentale da considerare.

- *Imperizia degli utilizzatori*: **I supporti di memorizzazione vanno trattati conoscendone le specificità tecniche, le modalità di registrazione su di essi, la durata e le modalità di conservazione del supporto stesso.**

  Per questo si fa riferimento alle misure di sicurezza di tipo organizzativo: formazione per gli utenti del sistema informatico aziendale.

7. Conclusioni

Dall'analisi effettuata in merito alla conformità della Azienda rispetto al D. Lgs. 196/2003 emergono principalmente gli aspetti che possono essere così sintetizzati:

a. **L'Azienda opera una gestione informatizzata dei dati personali sostanzialmente in linea con gli standard di sicurezza richiesti;**
b. **non sono state rilevate carenze sostanziali.**

Inoltre va effettuata:

1) **verifica dell'attuazione della *suite* di procedure e istruzioni operative redatte per la gestione ed il monitoraggio dei principali eventi di rilievo ai fini della sicurezza dei dati:**
   - **procedura di assegnazione, monitoraggio e revoca degli User ID e password;**
   - **procedura di backup dei dati;**
   - **procedura di gestione delle work station dell'Azienda;**
   - **procedura di accesso agli archivi non informatizzati;**
   - **procedura di verifica periodica su rispetto delle misure di sicurezza adottate (audit) e revisione annuale del DPS;**
2) **pianificazione di una giornata di formazione nella quale sensibilizzare i membri dell'Azienda sui rischi generati dalla gestione dei dati personali della stessa;**

3) **diffusione dell'informativa e acquisizione del consenso al trattamento dei dati presso i soggetti attivi del Percorso Privacy;**
4) **gestione della posta elettronica: ogni mail deve contenere la dicitura che invita a segnalare se la mail è recapitata a persone non facenti parte dell'Azienda o comunque non coinvolte e ad esprimere la volontà di non voler ricevere altre mail.**

La modifica dello stato di fatto presente in questo documento è da aggiornare in seguito alla verifica ispettiva interna atta a verificare lo stato di attuazione di tutta la documentazione.