



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

(D.LGS. n. 196 DEL 30/06/2003 PUBBLICATO SULLA G.U. N. 174 DEL 29/7/2003)

Sommario

1.	INTRODUZIONE	2
2.	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	7
2.1.	Introduzione	7
2.2.	Titolare del trattamento dati	7
2.3.	Responsabili del trattamento dati	7
2.4.	Censimento dei trattamenti e delle banche dati	8
2.5.	Trattamenti effettuati con supporti informatici.....	8
2.6.	Amministratore di sistema	8
2.7.	Misure di sicurezza relative all'accesso dall'esterno	9
2.8.	Misure di sicurezza relative all'accesso dall'interno	10
2.9.	Misure di sicurezza relative ai rischi di distruzione o perdita dei dati ..	11
2.10.	Incaricati dei singoli trattamenti.....	11
2.11.	Fornitori	11
2.12.	Trattamenti effettuati con supporti cartacei	12
2.13.	Trattamenti a livello di singola Unità Operativa	12
3.	ELENCO DEI TRATTAMENTI INFORMATICI	13
4.	ANALISI DEI RISCHI.....	21
4.1	Individuazione delle risorse da proteggere.....	21
4.2	Individuazione delle minacce	21
4.3	Individuazione delle vulnerabilità	24
4.4	Individuazione delle contromisure	25
5.	MISURE DI SICUREZZA PER LA PROTEZIONE DEI DATI INFORMATICI INVIATI ALL'ESTERNO DELL'AZIENDA.....	32
6.	AGGIORNAMENTO DEL PIANO	32

1. INTRODUZIONE

Art. 1) Definizioni e denominazioni dei soggetti che entrano all'interno del processo di trattamento dei dati

Ai fini del presente documento i soggetti che qui di seguito si elencano vengono identificati con le figure istituzionali appresso indicate:

a) Titolare del trattamento dei dati

Il titolare del trattamento dei dati, ai sensi dell'art. 4 comma 1 lett. f, è l'Azienda Ospedaliera, legalmente rappresentata dal Direttore Generale.

Al titolare spettano le decisioni in ordine alle modalità e finalità del trattamento dei dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

b) Responsabili del trattamento dei dati

Le funzioni di responsabilità relative al trattamento dei dati sono attribuite ai Direttori responsabili delle Unità Operative aziendali, ai Dirigenti Sanitari responsabili dei Presidi Ospedalieri di pertinenza dell'Azienda, ai Responsabili di sottostrutture organizzative cui sono demandati compiti istituzionali legati al trattamento dei dati personali, sensibili e giudiziari, ai Dirigenti non medici responsabili dei Settori Amministrativi e Tecnici presenti in Azienda, ai quali, ai sensi e per gli effetti dell'art. 29 della Legge n. 196/2003 e succ. modifiche ed integrazioni spetta la responsabilità di qualsiasi trattamento dei dati personali effettuato all'interno delle strutture organizzative cui sono preposti, sia manuale che informatizzato, di carattere sanitario, amministrativo, gestionale, contabile o altro, nonché della sicurezza organizzativa, fisica e logica delle banche dati, nello svolgimento delle loro funzioni istituzionali e nei limiti stabiliti da leggi e regolamenti o qualsiasi altro atto avente forza di legge; rientrano altresì nella sfera di responsabilità dei predetti soggetti anche la custodia, gestione e tenuta dei dati contenuti su supporti cartacei ove presenti.

c) Incaricato del trattamento dei dati

Si identifica come tale la persona incaricata, per iscritto, di compiere le operazioni di trattamento dei dati da parte del Responsabile e che opera sotto la sua diretta autorità;

d) misure minime

Si intende il complesso di misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi di cui all'art. 33 della Legge n. 196/2003 e che vengono analiticamente descritte nell'allegato B) al predetto Decreto;

e) Strumenti

Si intendono i mezzi elettronici o comunque automatizzati con cui è effettuato il trattamento;

f) Amministratori di sistema

Soggetti cui è conferito il compito di sovrintendere alle risorse del sistema e/o sottosistema informativo aziendale e di consentirne l'utilizzazione; essi possono essere identificati in soggetti interni all'Azienda o in soggetti esterni con i quali l'Azienda stipula appositi contratti per la fornitura di servizi;

g) Responsabile della gestione delle abilitazioni

Soggetto cui è conferito il compito di assegnare e revocare i "codici personali utenti" e le corrispondenti "parole chiave" (password).

Art. 2) Quadro normativo di riferimento

L'art. 31 del D.Lgs. n. 196/2003 stabilisce che i dati personali oggetto di trattamento devono essere 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.

L'art. 34 del D.Lgs. n. 196/2003 stabilisce che qualora il trattamento di dati sensibili sia realizzato mediante strumenti elettronici, devono essere rispettate le misure minime previste dal disciplinare tecnico contenuto nell'allegato B) della legge stessa, e che quindi deve essere predisposto e aggiornato con cadenza annuale un documento programmatico sulla sicurezza dei dati finalizzato alla definizione dei sottoelencati elementi, sulla base dell'analisi dei rischi, dell'attribuzione dei compiti e delle responsabilità nell'ambito delle Unità Operative deputate al trattamento dei dati stessi:

- i criteri tecnici ed 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 locali medesimi;
- i criteri e le procedure per assicurare l'integrità dei dati;

- i criteri e le procedure per la sicurezza delle trasmissioni dei dati, ivi compresi quelli per le restrizioni d'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 danni.

Art. 3) Ambito di applicazione

Il documento in oggetto, nell'ambito delle attività svolte dalle singole Unità Operative aziendali ed a fronte delle misure di sicurezza previste dall'art. 33 del D.Lgs. n. 196/2003, nonché degli standard minimi delineati dall'Allegato B) al predetto Decreto, intende definire gli elementi di riferimento necessari per l'adozione, l'adeguamento, lo sviluppo e l'implementazione gestionale di misure di sicurezza relative a:

- trattamenti di dati personali (definiti dall'art. 4 comma 1 lettera b), riferiti a dati senza particolare rilevanza caratteristica e di dati personali sensibili e giudiziari definiti all'art. 4 comma 1 lettere d) ed e), trattati con riguardo a quanto previsto dagli artt. 34 e 35 del D.Lgs. n. 196/2003;
- gestione di archivi cartacei (correnti, di deposito, storici) e di banche dati conservate su supporti informatizzati-automatizzati (memorie di rete, hard-disk, floppy disk, cd-rom);
- gestione di archivi contenenti documenti confidenziali di particolare rilevanza.

Art. 4) Trattamento dei dati mediante procedure informatizzate del sistema informativo aziendale

1. I Responsabili, nominati ai sensi dell'art. 29 del D.Lgs. n. 196/2003, provvedono per iscritto alla designazione dei soggetti Incaricati, cui conferire le credenziali autorizzative all'uso delle procedure informatizzate, specificando per ciascuno a quali funzioni e/o insiemi di dati debbono essere in grado di accedere. I Responsabili, con le medesime modalità, impartiscono agli Incaricati le necessarie istruzioni per il corretto utilizzo di dette procedure. Il soggetto Responsabile della gestione delle abilitazioni provvede ai propri compiti con le seguenti modalità:
 - a ciascun Incaricato che, per esigenze di servizio, deve poter utilizzare una procedura informatizzata ed accedere di conseguenza alle informazioni contenute negli archivi della stessa, è assegnato un "codice personale utente" ed una "parola chiave" segreta (password) individuale e riservata in modo esclusivo
 - ciascun Incaricato, per mezzo di detto codice di accesso, è abilitato all'utilizzo delle funzionalità necessarie allo svolgimento delle attività allo stesso assegnate e può contemporaneamente accedere ai soli dati strettamente necessari allo scopo.
2. Ciascuna procedura informatizzata deve essere strutturata in modo da consentire di:

- segmentare le abilitazioni di accesso ed utilizzo in base alle necessità dell'Unità Operativa di riferimento
 - individuare a posteriori l'autore di ciascuna operazione effettuata sui dati trattati attraverso procedure di tracciamento degli accessi (LOG). Il rispetto dei requisiti di cui al presente punto 2 deve essere certificato e garantito dal fornitore o dal produttore di ciascuna procedura informatizzata in uso all'interno del sistema informativo aziendale.
3. E' fatto obbligo a ciascun incaricato, di cui al presente articolo, di non comunicare ad altri il proprio codice identificativo personale, né la parola chiave (password) segreta, di non lasciare la stazione di lavoro situata al proprio posto di lavoro collegata ed incustodita, di non utilizzare i dati consultabili per fini non strettamente attinenti alle esigenze di servizio.

Art.5) Trattamento dei dati mediante procedure informatizzate delle Unità Operative

Le misure di sicurezza previste dal presente documento si applicano anche alle procedure informatizzate gestite dalle singole Unità Operative aziendali al di fuori del sistema informativo integrato.

Art. 6) Trattamento dei dati mediante strumenti diversi da quelli elettronici o comunque automatizzati

1. I Responsabili, ai sensi dell'art. 30 del D.Lgs. n. 196/2003, nel designare per iscritto gli Incaricati e nell'impartire le istruzioni, devono prescrivere che i soggetti designati abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere i compiti loro assegnati.
2. Gli atti e i documenti contenenti i dati devono essere conservati in archivi ad accesso controllato e, se affidati agli Incaricati del trattamento, devono essere da questi ultimi conservati e restituiti al termine delle operazioni eseguite.
3. Nel caso di dati "sensibili" o di natura "giudiziaria", di cui rispettivamente agli artt. 4 comma 1 lettere d) ed e) del D.Lgs. n. 196/2003, oltre alle misure di cui ai punti 1 e 2 del seguente articolo, devono essere osservate le seguenti modalità:
 - se affidati agli Incaricati, gli atti e i documenti concernenti i dati vanno conservati, sino alla restituzione, in contenitori muniti di serratura;
 - l'accesso agli archivi va controllato e devono essere identificati e registrati i soggetti che vi accedono dopo l'orario di chiusura degli archivi stessi.
4. Le medesime modalità di cui al presente articolo si applicano alla conservazione anche dei supporti non informatici contenenti la riproduzione di informazioni relative al trattamento dei dati di cui al citato art. 4 comma 1 lettere d) ed e) del D.Lgs. n. 196/2003

Art. 7) Norma finale

Le disposizioni del presente Documento Programmatico - Piano Operativo sono adeguate, con cadenza annuale, in esito alla verifica dell'efficacia delle misure di sicurezza in esso determinate, nonché in relazione alle modificazioni delle misure minime individuate secondo il disciplinare tecnico contenuto nell'allegato B) del D.Lgs n. 196/2003, ed in relazione all'evoluzione tecnica del settore ed all'esperienza maturata.

2. DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

2.1. Introduzione

Nel presente documento sono esposte le misure di sicurezza individuate dall'Azienda Ospedaliera Ospedali Riuniti "Villa Sofia – Cervello". di Palermo in ottemperanza a quanto disposto dall'art. 33 del D.Lgs. n. 196/2003. Si tratta cioè delle misure minime di sicurezza, così come delineate nel disciplinare tecnico contenuto nell'allegato B) del predetto Decreto.

In realtà, alla luce delle valutazioni tecniche effettuate, tali misure coincidono con quelle suggerite dal sopra richiamato art. 33, ovvero con quanto oggi attuabile sulla scorta delle conoscenze acquisite sulla base del progresso tecnico, così da ridurre al minimo i rischi di distruzione o perdita dei dati, di accesso non autorizzato ai medesimi o di trattamento non consentito o non conforme.

In tal senso, quanto esposto nel seguito sarà oggetto di verifica alla fine dell'anno in corso.

2.2. Titolare del trattamento dati

Per tutti i trattamenti effettuati presso l'Azienda Ospedaliera Ospedali Riuniti " Villa Sofia –Cervello" di Palermo, in conformità a quanto previsto dal D.Lgs. n. 196/2003, art. 4, il Titolare è l'Azienda Ospedaliera stessa, legalmente rappresentata dal Direttore Generale al quale competono i compiti di rappresentanza legale.

Al Titolare spettano le decisioni in ordine alle finalità e modalità del trattamento dei dati personali ed alle misure organizzative utilizzate, in materia di privacy, ivi compreso il profilo della sicurezza; nella sua attività si avvale del supporto dell' "Unità Organizzativa Gestione Privacy" (deliberazione n. 1032 del 16/10/2008).

2.3. Responsabili del trattamento dati

In ambito aziendale sono individuati e designati, in conformità a quanto previsto dal D.Lgs. n. 196/2003, , quali Responsabili del trattamento, ognuno per le proprie funzioni e competenze le seguenti figure:

Per l'area amministrativa

- Il Direttore Amministrativo;
- I Direttori di Struttura Complessa;
- I Dirigenti in staff alla Direzione Generale

Per l'area sanitaria

- Il Direttore sanitario;
- I Direttori di Struttura Operativa Complessa
- I Dirigenti di Struttura semplice, qualora ricoprano posizioni strategicamente rilevanti al fine del trattamento dati.

Le figure di cui sopra sono state individuate da questa Azienda con proprio provvedimento n. 181 dell'11/02/2011, che qui si intende integralmente richiamato.

2.4. Censimento dei trattamenti e delle banche dati

L'Azienda Ospedaliera Ospedali Riuniti Villa "Sofia – Cervello" di Palermo ha provveduto ad avviare il censimento di tutti i trattamenti e di tutte le banche dati, elettroniche e cartacee, presenti presso le proprie Unità Operative e Strutture Organizzative presenti in Azienda.

Tale rilevazione ha avuto lo scopo di valutare l'eventuale sussistenza di trattamenti non attinenti alle finalità istituzionali dell'Azienda.

Stante che l'elenco dei trattamenti è in continua evoluzione, si redige il presente documento con i trattamenti attualmente in essere e ci si riserva di farlo evolvere ogni qualvolta si dovesse introdurre un nuovo tipo di trattamento.

Lo scopo del censimento continuo è l'individuazione delle tipologie di dati gestiti, le fasi di cui si compone ciascun trattamento, le eventuali misure di sicurezza già attivate, l'interconnessione con altre banche dati interne od esterne, la necessità di comunicazione o diffusione dei dati raccolti, e le indicazioni normative e le esigenze organizzative interne attraverso le quali detti trattamenti vengono effettuati.

2.5. Trattamenti effettuati con supporti informatici

Tutti i trattamenti a livello aziendale effettuati con supporti informatici rientrano, in considerazione degli aspetti logistici dell'Azienda Ospedaliera Ospedali Riuniti Villa Sofia - Cervello di Palermo, tra quelli classificati nel disciplinare tecnico in materia di misure minime di sicurezza del più volte citato D. Lgs. 196/2003 e dovranno essere trattati, replicati e custoditi secondo le modalità prescritte dall'allegato B) al Decreto.

In tale ottica l'Azienda ha in corso di attuazione un progetto per il miglioramento delle condizioni di sicurezza del Sistema Informativo Aziendale che sarà portata a termine entro il corrente anno.

2.6. Amministratore di sistema

Con delibera n. 184 del 11/02/2011, si è proceduto alla nomina dell'Amministratore di Sistema Informativo Aziendale (in applicazione del D.lgs. n. 196 del 30/06/2003) con i seguenti compiti:

- Monitorare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici, conforme a quanto previsto dai punti da 1 a 10 del Disciplinare tecnico, allegato B) al D.lgs. n. 196/2003;
- Monitorare e gestire un sistema di autorizzazione per gli incaricati dei trattamenti di dati personali effettuati con strumenti elettronici, conforme a quanto previsto dai punti da 12 a 14 del Disciplinare tecnico allegato B) al D.lgs. n. 196/2003;

- Verificare costantemente che l'Azienda abbia adottato le misure minime di sicurezza per il trattamento dei dati personali, previste dall'art. 34 del D.lgs. n. 196/2003, e dal Disciplinare tecnico, allegato B) al decreto legislativo medesimo, provvedendo senza indugio agli adeguamenti eventualmente necessari;
- Suggestire al titolare del trattamento l'adozione e l'aggiornamento delle più ampie misure di sicurezza atte a realizzare quanto previsto dall'art. 31 del D.lgs. n. 196/2003, che dispone che i dati personali oggetto di trattamento devono essere 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 accidentali, dei dati stessi, di accesso non autorizzato di trattamento non consentito o non conforme alle finalità della raccolta;
- Curare su incarico del titolare del trattamento, l'adozione e l'aggiornamento delle misure "idonee" di cui al punto precedente;
- Attivare e aggiornare con cadenza almeno mensile idonei strumenti elettronici atti a proteggere i dati trattati attraverso gli elaborati del sistema informativo, contro il rischio di intrusione e contro l'azione dei virus informatici;
- Pianificare l'aggiornamento periodico, con frequenza almeno semestrale, dei programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti;
- Impartire a tutti gli incaricati istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale;
- Adottare procedure per la custodia delle copie di sicurezza dei dati e per il ripristino delle disponibilità dei dati e dei sistemi;
- Predisporre ed aggiornare entro il 31 Marzo di ogni anno, il documento programmatico sulla sicurezza previsto dal punto 19 del Disciplinare tecnico, allegato B) al D.lgs. n. 196/2003;
- Predisporre un piano di controlli periodici, da eseguire con cadenza almeno annuale, dell'efficacia delle misure di sicurezza adottate in azienda.

2.7. Misure di sicurezza relative all'accesso dall'esterno

Tutti i soggetti esterni all'Azienda che risultino interessati ad accedere al sistema informatico aziendale devono essere autorizzati per iscritto dal Responsabile del Servizio Sistema Informatico Aziendale (se l'accesso richiesto è relativo ad attività tecnologiche).

Sulla scorta di tale autorizzazione, che deve specificare gli elaboratori, le procedure, le funzionalità ed i dati per i quali l'accesso deve essere consentito, gli amministratori di sistema procedono ad assegnare i codici di accesso, le password, i profili di abilitazione e le relative istruzioni sulle modalità da seguirsi per rendere operativo l'accesso medesimo.

A tal fine, l'Azienda Ospedaliera Ospedali Riuniti Villa Sofia - Cervello di Palermo ha già attivato, per taluni servizi e attrezzature informatiche, gli

strumenti di sicurezza per il controllo di accesso dall'esterno; tali prodotti hardware e software vengono individuati e saranno configurati secondo quanto previsto nell'ipotesi progettuale allegata che ha preso in considerazione tutte le tecnologie oggi a disposizione per la gestione di tali problematiche.

Va comunque precisato che attualmente per la maggior parte dei sistemi presenti in Azienda sono stati previsti strumenti di controllo degli accessi che effettuano la registrazione di tutti gli accessi agli stessi sistemi sia dall'esterno che dall'interno, consentendo così una puntuale verifica di eventuali accessi non autorizzati.

2.8. Misure di sicurezza relative all'accesso dall'interno

Tutti i soggetti interni all'Azienda che risultino interessati ad accedere al sistema informatico aziendale per finalità legate alla loro attività professionale, devono essere autorizzati per iscritto dal Responsabile della Unità Operativa presso la quale prestano la propria attività.

Sulla scorta di tale autorizzazione, che deve specificare le funzionalità ed i dati per i quali l'accesso deve essere consentito, gli amministratori di sistema procedono ad assegnare i codici di accesso, le password, i profili di abilitazione e le relative istruzioni sulle modalità da seguirsi per rendere operativo l'accesso medesimo.

Tale attivazione coincide con la nomina a "incaricato" dei trattamenti dei dati cui sono stati abilitati.

L'incaricato riceve, quindi, in busta chiusa il proprio codice di accesso e la propria password personale e segreta, accompagnati dalle istruzioni sul corretto utilizzo di tali codici e sui comportamenti da assumersi ai fini di garantire (in relazione ai dati di cui verrà a conoscenza) il rispetto di quanto disposto dalla D. Lgs. n. 196/2003 e successive integrazioni e modificazioni.

Tale comunicazione scritta e riservata viene effettuata dal Responsabile dell'Unità Operativa cui il dipendente è proposto; il Responsabile, nella qualità di Responsabile di tutti i trattamenti informatizzati e non informatizzati trattati dalla Unità Operativa dallo stesso diretta, deve altresì informare il medesimo dipendente di quale sia la natura ed il contenuto dei dati personali, sensibili e giudiziari trattati, con l'invito a segnalare eventuali disfunzioni del software e/o di tutti i sistemi operativi e di rete in uso.

Poiché gli strumenti tecnologici in uso presso l'Azienda effettuano una registrazione di tutti gli accessi alla procedure informatiche aziendali, gli amministratori di sistema procederanno alla disabilitazione dei codici di accesso nel caso in cui dovessero essere rilevati utilizzi scorretti o la mancata utilizzazione per più di tre mesi.

2.9. Misure di sicurezza relative ai rischi di distruzione o perdita dei dati

Gli amministratori dei server presenti in Azienda (siano essi dipendenti o personale esterno all'Azienda, appositamente autorizzato) garantiscono che gli addetti al Data Center del Sistema Informativo, nominati a tal fine "incaricati" di tale trattamento, procedano con la cadenza temporale stabilita all'effettuazione delle copie di salvataggio dei data base contenenti i dati personali, sensibili e giudiziari gestiti a livello aziendale.

Gli amministratori dei server procedono in prima persona all'eventuale ripristino di detti data base, ove se ne verificasse la necessità.

Le copie di salvataggio divenute superate (ovvero non convenientemente aggiornate) vengono rese inutilizzabili dagli incaricati (addetti alla sala macchine).

2.10. Incaricati dei singoli trattamenti

Ciascun incaricato ad un trattamento riceve tale nomina secondo le modalità specificate al precedente punto 2.8. In sintesi, le principali regole cui l'incaricato deve attenersi sono:

- non comunicare il proprio codice di accesso e la propria password ad altri
- modificare periodicamente la propria password personale
- non abbandonare la propria postazione di lavoro attiva e collegata al sistema informatico aziendale tramite il proprio codice di accesso
- non alterare fisicamente la postazione di lavoro fornitagli dall'Azienda
- non caricare ed utilizzare sulla propria stazione di lavoro programmi diversi da quelli fornitigli dall'ufficio del Sistema Informativo
- utilizzare i dati personali e sensibili di cui viene a conoscenza nello svolgimento dei trattamenti cui è abilitato rigorosamente per le finalità istituzionali che gli sono assegnate
- non comunicare tali dati al di fuori delle necessità implicite per il corretto completamento dei processi aziendali cui l'incaricato partecipa.

2.11. Fornitori

Il Servizio Informativo Aziendale deve richiedere a tutti i fornitori di attrezzature informatiche e programmi utilizzati a livello aziendale una dichiarazione scritta circa la compatibilità tecnologica dei relativi prodotti alle misure di sicurezza sopra descritte.

Ove le caratteristiche tecnologiche di alcuni prodotti non risultassero pienamente soddisfacenti, i fornitori in questione dovranno indicare all'Azienda le soluzioni alternative realmente applicabili, dimostrandone la compatibilità con le misure minime di sicurezza riportate dall'Allegato B al D.Lgs. n. 196/2003 contenente il disciplinare tecnico in materia di misure minime di sicurezza.

2.12. Trattamenti effettuati con supporti cartacei

Ciascuna Struttura Organizzativa competente in relazione a trattamenti effettuati con supporti cartacei, a livello aziendale, deve:

- nominare gli incaricati, prescrivendone l'accesso ai soli dati necessari all'adempimento dei compiti loro assegnati;
- garantire che i documenti siano conservati in archivi ad accesso selezionato;
- garantire che tali documenti, quando affidati agli incaricati, siano custoditi in contenitori muniti di serratura;
- garantire che l'accesso agli archivi sia controllato e che i soggetti che vi accedono dopo l'orario di chiusura vengano identificati e registrati.

2.13. Trattamenti a livello di singola Unità Operativa

I Responsabili delle singole Strutture Operative aziendali, nella loro qualità di Responsabili dei trattamenti ivi gestiti, dovranno agire in conformità a quanto esposto nei precedenti punti.

3. ELENCO DEI TRATTAMENTI INFORMATICI DEI DATI PERSONALI IN AZIENDA

Qui di seguito viene riportato l'elenco dei trattamenti informatici dei dati personali e sensibili effettuate da quest'Azienda soggetti alla tutela di cui al D. Lgs. 196/2003:

Tabella 3.1- Elenco dei trattamenti : informazioni essenziali

ID 1 Accettazione/Trasferimento/Dimissioni Pazienti		Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
		S	G			
Finalità perseguita o attività svolta	Categorie di interessi	S	G			
Dati anagrafici e informazioni mediche e medico-legali	Pazienti	X		Direzione Medica di Presidio	U.O.C. Sistema Informativo e Statistico. UU.OO.CC per la definizione della SDO	Procedura informatica di tipo client server

ID 2 Prenotazione ed erogazione prestazioni sanitari		Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
		S	G			
Finalità perseguita o attività svolta	Categorie di interessati	S	G			
Prenotazione ed erogazione prestazioni sanitarie in regime ambulatoriale	Utenti	X		Ufficio CUP- Ticket	U.O.C Sistema Informativo e Statistico; Accettazione Amministrativa; UU.OO.CC. Interessate all'erogazione delle prestazioni ambulatoriali per quanto di competenza.	Procedura informatica di tipo web server

ID 3 Prestazioni erogate presso area di Emergenza P.O. Villa Sofia		Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
Finalità perseguita o attività svolta	Categorie di interessati	S	G			
Dati anagrafici e informazioni mediche e medico - legali trattate dal D.E.A.U. e da tutte le Unità Organizzative che operano con il predetto Dipartimento per il trattamento delle urgenze e delle emergenze.	Pazienti	X		D.E.A.U.	UU.OO.CC. Coinvolte nel trattamento delle urgenze e delle emergenze	Procedura informatica di tipo web server

ID 4 Prestazioni erogate presso area di Emergenza P.O. Cervello		Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
Finalità perseguita o attività svolta	Categorie di interessi	S	G			
Dati anagrafici e informazioni mediche e medico - legali trattate dal D.E.A.U. e da tutte le Unità Organizzative che operano con il predetto Dipartimento per il trattamento delle urgenze e delle emergenze.	Pazienti	X		D.E.A.U.	UU.OO.CC. Coinvolte nel trattamento delle urgenze e delle emergenze	Procedura informatica di tipo client server

ID 5 Trattamento dei dati sanitari dei Certificati di Assistenza al Parto (CEDAP)		Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
Finalità perseguita o attività svolta	Categorie di interessati	S	G			
Dati anagrafici e informazioni mediche e medico - legali trattate dalla Direzione Sanitaria		X		Direzione Medica di Presidio	U.O.C. Ginecologia e Ostetricia; U.O.C Sistema Informativo e Statistico	Procedura informatica di tipo client server

ID 6 Trattamento dei dati personali dei dipendenti: dati anagrafici, fiscali, previdenziali, assistenziali e di presenza in servizio		Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
Finalità perseguita o attività svolta	Categorie di interessati	S	G			
Dati anagrafici e informazioni amministrative di diversa natura relative al personale dipendente (dati stipendiali, attestazione presenza in servizio, dati previdenziali ed assistenziali, etc.)	Dipendenti	X	X	U.O.C. Settore Affari del Personale	U.O.C Controllo di Gestione; U.O.C Settore Economico Finanziario; Società SE.RIN(esterna)	Procedura informatica di tipo client server

ID 7 Trattamento dei dati personali relativi ai fornitori, professionisti e clienti dell'Azienda		Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
Finalità perseguita o attività svolta	Categorie di interessati	S	G			
Dati personali dei fornitori, dei professionisti e dei clienti concernenti la loro anagrafica per la corrispondenza, nonché le situazioni debitorie/creditorie relative a rapporti contrattuali instaurati con l'Azienda.	Fornitori			U.O.C. Settore Economico Finanziario	U.O.C. Settore Appalti e Forniture; Società Selfin (esterna)	Modulo della Procedura del Sistema amministrativo contabile

ID 8 Trattamento di dati personali contenuti in procedure di gestione di attività documentali		Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
Finalità perseguita o attività svolta	Categorie di interessati	S	G			
Dati personali, sensibili e giudiziari che vengono trattati nei processi di gestione di procedure documentali quali la gestione delle deliberazioni e la gestione del protocollo informatico	Utenti, Dipendenti	X	X	Settore Affari Generali e Legali	Società RS Sistemi	Procedura informatica di tipo web server

ID 9 Gestione e trattamento dei dati personali da parte dell'UU.OO. Di Medicina Immuno-trasfusionale		Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
Finalità perseguita o attività svolta	Categorie di interessati	S	G			
Dati anagrafici e sanitari, informazioni mediche e medico-legali attualmente trattate dalle UU.OO. coinvolte	Pazienti	X		UU.OO.CC Medicina Immuno-trasfusionale		Procedura Informatica di tipo client server

ID 10 Gestione e trattamento dei dati personali da parte delle UU.OO. Di Patologia Clinica e Microbiologia del P.O. "Villa Sofia"		Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
Finalità perseguita o attività svolta	Categorie di interessati	S	G			
Dati anagrafici e sanitari, informazioni mediche e medico legali attualmente trattate dalle singole UU.OO. coinvolte	Pazienti ed utenti esterni	X		U.O.C. Patologia Clinica; U.O.C Microbiologia	Tutte le UU.OO.CC per la richiesta e la ricezione degli esiti degli esami di laboratorio (Order Management)	Procedura informatica di tipo web server

ID 11 Gestione e trattamento dei dati personali da parte delle U.O. Di Patologia Clinica P.O. "Cervello"		Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
Finalità perseguita o attività svolta	Categorie di interessati	S	G			
Dati anagrafici e sanitari, informazioni mediche e medico legali attualmente trattate dalle singole UU.OO. coinvolte.	Pazienti ed utenti esterni	X		U.O.C. Patologia Clinica;	Tutte le UU.OO.CC per la richiesta e la ricezione degli esiti degli esami di laboratorio	Procedura informatica di tipo web server

ID 12 Gestione e trattamento dei dati personali da parte delle UU.OO. di Medicina, Ematologia I, Gastroenterologia P.O. "Cervello"		Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
Finalità perseguita o attività svolta	Categorie di interessati	S	G			
Dati anagrafici e sanitari, informazioni mediche e medico legali attualmente trattate dalle singole UU.OO. coinvolte	Pazienti	X		UU.OO.CC Medicina, Ematologia I, Gastroenterologia		Procedura informatica di tipo client Server

ID 13 Gestione e trattamento dei dati personali da parte dell' U.O. di Radiologia		Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
Finalità perseguita o attività svolta	Categorie di interessati	S	G			
Dati anagrafici e sanitari, informazioni mediche e medico legali attualmente trattate dalle singole UU.OO. coinvolte	Pazienti	X		U.O.C Radiologia	Tutte le UU.OO.CC per la richiesta e la visione degli esami radiologici	Procedura informatica di tipo web server

ID 14 Gestione e trattamento dei dati personali da parte dell' U.O. di Anatomia Patologica		Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
Finalità perseguita o attività svolta	Categorie di interessati	S	G			
Dati anagrafici e sanitari, informazioni mediche e medico legali attualmente trattate dalle singole UU.OO. coinvolte	Pazienti	X		U.O.C. di Anatomia Patologica	Tutte le UU.OO.CC per la richiesta e la visione degli esami patologici	Procedura informatica di tipo client server

Tabella 3.2 - Elenco dei trattamenti: ulteriori elementi per descrivere gli strumenti.

Identificativo del trattamento	Eventuale banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
1	Database Server - Piattaforma Isolabella	Data Center P.O. CERVELLO	PC Desktop	LAN Aziendale
2	Database Server - OLOCUP3	Data Center Sede Legale	PC Desktop	LAN Aziendale
3	Database Server - Gestione DEAU	Data Center Sede Legale	PC Desktop	LAN Aziendale
4	Database Server - Modulo Vebena piattaforma Isolabella	Data Center P.O. CERVELLO	PC Desktop	LAN Aziendale
5	Database Server - Modulo Vebena piattaforma Isolabella	Data Center P.O. CERVELLO	PC Desktop	LAN Aziendale
6	Database - Procedura Ser.In	Data Center Sede Legale	PC Desktop	LAN Aziendale
7	Database - Procedura Selfin - Sistema amministrativo contabile	Data Center Sede Legale	PC Desktop	LAN Aziendale
8	Database Server - Gestione Protocollo e Delibere - Sud Team	Data Center Sede Legale	PC Desktop	LAN Aziendale
9	Database Server - Emonet	U.O.C Medicina Trasmisoria	PC Desktop	LAN Aziendale
10	Database Server - Piattaforma Galileo	Data Center . P.O. Villa Sofia	PC Desktop	LAN Aziendale
11	Database Server - Metafora	U.O.C Patologia Clinica P.O. Cervello	PC Desktop	LAN Aziendale
12	Database Server- Euristic	U.O.C Medicina P.O. Cervello	PC Desktop	LAN Aziendale
13	Database Server AGFA	U.O.C Radiologica P.O. Villa Sofia - P.O. Cervello	PC Desktop	LAN Aziendale
14	Database Server	U.O.C. Anatomia Patologica P.O. Cervello	PC Desktop	LAN Aziendale

4. ANALISI DEI RISCHI

L'analisi dei rischi consente di acquisire consapevolezza e visibilità sul livello di esposizione al rischio del proprio patrimonio informativo e avere una mappa preliminare dell'insieme delle possibili contromisure di sicurezza da realizzare.

L'analisi dei rischi consiste nella:

- individuazione di tutte le risorse del patrimonio informativo;
- identificazione delle minacce a cui tali risorse sono sottoposte;
- identificazione delle vulnerabilità;
- definizione delle relative contromisure.

4.1 Individuazione delle risorse da proteggere

Le risorse da proteggere sono:

- personale;
- dati/informazioni;
- documenti cartacei;
- hardware;
- software;

4.2 Individuazione delle minacce

Minacce a cui sono sottoposte le risorse hardware

Le principali minacce alle risorse hardware sono:

- malfunzionamenti dovuti a guasti;
- malfunzionamenti dovuti a eventi naturali quali terremoti, allagamenti, incendi;
- malfunzionamenti dovuti a blackout ripetuti ed in genere a sbalzi eccessivi delle linee di alimentazione elettrica;

Minacce a cui sono sottoposte le risorse connesse in rete

Le principali minacce alle risorse connesse in rete possono provenire dall'interno, dall'esterno o da una combinazione interno/esterno e sono relative:

all'utilizzo della LAN/Intranet (interne);

ai punti di contatto con il mondo esterno attraverso Internet (esterne);

- allo scaricamento di virus e/o trojan per mezzo di posta elettronica e/o alle operazioni di download eseguite tramite il browser (interne/esterne).

L'utilizzo di programmi di sniffing e port scanning é riservato esclusivamente all'amministratore di sistema per la misura/diagnostica delle prestazioni della rete locale LAN, tali programmi non sono in nessun caso utilizzati su reti

esterne a quella della rete locale LAN.

La lettura in chiaro dei pacchetti in transito può solo essere autorizzata dalla Autorità Giudiziaria.

Minacce a cui sono sottoposti i dati trattati

Le principali minacce ai dati trattati sono:

- accesso non autorizzato agli archivi contenenti le informazioni riservate (visione, modifica, cancellazione, esportazione) da parte di utenti interni e/o esterni;
- modifiche accidentali (errori, disattenzioni) agli archivi da parte di utenti autorizzati.

Minacce a cui sono sottoposti i supporti di memorizzazione

Le principali minacce ai supporti di memorizzazione sono:

- distruzione e/o alterazione a causa di eventi naturali;
- imperizia degli utilizzatori;
- sabotaggio;
- deterioramento nel tempo (invecchiamento dei supporti);
- difetti di costruzione del supporto di memorizzazione che ne riducono la vita media;
- l'evoluzione tecnologica del mercato che rende in breve tempo obsoleti alcuni tipi di supporti.

Nella tabella seguente sono elencati gli eventi potenzialmente in grado di determinare danno a tutte o parte delle risorse

Rischi	Deliberato	Accidentale	Ambientale
Terremoto			X
Inondazione	X	X	X
Uragano			X
Fulmine			X
Bombardamento	X	X	
Fuoco	X	X	
Uso di armi		X	
Danno volontario	X		
Interruzione di corrente		X	
Interruzione di acqua		X	
Interruzione di aria condizionata	X	X	
Guasto hardware		X	
Linea elettrica instabile		X	X
Temperatura e umidità eccessive			X
Polvere			X
Radiazioni elettromagnetiche		X	
Scariche elettrostatiche		X	
Furto	X		

Uso non autorizzato dei supporti di memoria	X		
Deterioramento dei supporti di memoria		X	
Errore del personale operativo		X	
Errore di manutenzione		X	
Masquerading dell'identificativo dell'utente	X		
Uso illegale di software	X	X	
Software dannoso		X	
Esportazione/importazione illegale di software	X		
Accesso non autorizzato alla rete	X		
Uso della rete in modo non autorizzato	X		
Guasto tecnico di provider di rete		X	
Danni sulle linee	X	X	
Errore di trasmissione		X	
Sovraccarico di traffico	X	X	
Intercettazione (Eavesdropping)	X		
Infiltrazione nelle comunicazioni	X		
Analisi del traffico		X	
Indirizzamento non corretto dei messaggi		X	
Reindirizzamento dei messaggi	X		
Ripudio	X		
Guasto dei servizi di comunicazione	X	X	
Mancanza di personale		X	
Errore dell'utente	X	X	
Uso non corretto delle risorse	X	X	
Guasto software	X	X	
Uso di software da parte di utenti non autorizzati	X	X	
Uso di software in situazioni non autorizzate	X	X	

4.3 Individuazione delle vulnerabilità

Nelle tabelle seguenti sono elencate le vulnerabilità del sistema informativo che possono essere potenzialmente sfruttate qualora si realizzasse una delle minacce indicate al para 4.2 .

Infrastruttura	Hardware	Comunicazioni
Mancanza di protezione fisica dell'edificio (porte finestre ecc.)	Mancanza di sistemi di rimpiazzo	Linee di comunicazione non protette
Mancanza di controllo di accesso	Suscettibilità a variazioni di tensione	Giunzioni non protette
Linea elettrica instabile	Suscettibilità a variazioni di temperatura	Mancanza di autenticazione
Locazione suscettibile ad allagamenti	Suscettibilità a umidità, polvere, sporcizia	Trasmissione password in chiaro
	Suscettibilità a radiazioni elettromagnetiche	Mancanza di prova di ricezione/invio
	Manutenzione insufficiente	Presenza di linee dial-up (con modem)
	Carenze di controllo di configurazione (update/upgrade dei sistemi)	Traffico sensibile non protetto
		Gestione inadeguata della rete
		Connessioni a linea pubblica non protette

4.4 Individuazione delle contromisure

Le contromisure individuano le azioni che si propongono al fine di annullare o di limitare le vulnerabilità e di contrastare le minacce, esse sono classificabili nelle seguenti tre categorie:

- contromisure di carattere fisico;
- contromisure di carattere procedurale;
- contromisure di carattere elettronico/informatico.

Contromisure di carattere fisico

- Le apparecchiature informatiche critiche (server di rete, computer utilizzati per il trattamento dei dati personali o sensibili/giudiziari e apparecchiature di telecomunicazione, dispositivi di copia) e gli archivi cartacei contenenti dati personali o sensibili/giudiziari sono situati in locali ad accesso controllato;
- i locali ad accesso controllato (Data Center) sono all'interno di aree sotto la responsabilità del responsabile del trattamento;
- i locali sono provvisti di sistema di allarme e di estintore;
- sono programmati interventi atti a dotare i locali ad accesso controllato di porte blindate, armadi ignifughi, impianti elettrici dedicati, sistemi di condizionamento, apparecchiature di continuità elettrica.

Contromisure di carattere procedurale

- l'ingresso nei locali ad accesso controllato è consentito solo alle persone autorizzate;
- il responsabile dell'area ad accesso controllato deve mantenere un effettivo controllo sull'area di sua responsabilità;
- nei locali ad accesso controllato è esposta una lista delle persone autorizzate ad accedere, che è periodicamente controllata dal responsabile del trattamento o da un suo delegato;
- i visitatori occasionali delle aree ad accesso controllato sono accompagnati da un incaricato;
- per l'ingresso ai locali ad accesso controllato è necessaria preventiva autorizzazione da parte del Responsabile del trattamento e successiva registrazione su apposito registro;
- è controllata l'attuazione del piano di verifica periodica sull'efficacia degli allarmi e degli estintori;
- l'ingresso in locali ad accesso controllato da parte di dipendenti o estranei per operazioni di pulizia o di manutenzione avviene solo se i contenitori dei dati sono chiusi a chiave e i computer sono spenti oppure se le operazioni si svolgono alla presenza dell'Incaricato del trattamento di tali dati;
- i registri, contenenti dati comuni e particolari, durante l'orario di lavoro devono essere tenuti in e affidati al responsabile di turno. Al termine dell'orario di lavoro vengono depositati e successivamente raccolti da un incaricato del trattamento e conservati in luogo sicuro per essere riconsegnati da un incaricato del trattamento all'inizio dell'orario di lavoro.
- il responsabile del trattamento dei dati è responsabile della riservatezza

del registro personale in cui sono annotati dati comuni e particolari. Fuori dall'orario di servizio il registro viene conservato nell'armadietto del responsabile del trattamento dei dati che è chiuso a chiave, una chiave di riserva è mantenuta con le dovute cautele dalla ditta ;

Contromisure di carattere elettronico/informatico

Le misure di carattere elettronico/informatico adottate sono:

- utilizzo di server con configurazioni di ridondanza
- presenza di gruppi di continuità elettrica per il server
- attivazione di un sistema di backup centralizzato e automatizzato con periodicità settimanale e storico di un mese (indicare se la misura è attiva o entro quando sarà adottata). Alla data di questo documento i responsabili delle copie sono indicati nell'Allegato 1 relativo al censimento dei trattamenti dei dati;
- installazione di un firewall con hardware dedicato per proteggere la rete dagli accessi indesiderati attraverso internet (indicare se la misura è attiva o entro quando sarà adottata);
- definizione delle regole per la gestione delle password per i sistemi dotati di sistemi operativi Windows 2000, XP e Windows 7, di seguito specificate;
- installazione di un sistema antivirus su tutte le postazioni di lavoro, configurato per controllare la posta in ingresso, la posta in uscita, per eseguire la procedura di aggiornamento in automatico con frequenza settimanale e la scansione periodica dei supporti di memoria
- definizione delle regole per la gestione di strumenti elettronico/informatico, di seguito riportate;
- definizione delle regole di comportamento per minimizzare i rischi da virus, di seguito riportate:

Regole per la gestione delle password

Tutti gli incaricati del trattamento dei dati personali accedono al sistema informativo per mezzo di un codice identificativo personale (in seguito indicato User-id) e password personale.

User-id e password iniziali sono assegnati, dal custode delle password.

User-id e password sono strettamente personali e non possono essere riassegnate ad altri utenti.

La User-id è costituita dalla prima lettera del nome seguita dal cognome. In caso di omonimia si procede con successiva notazione numerica.

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

Ogni sei mesi (tre nel caso di trattamento dati sensibili) ciascun incaricato provvede a sostituire la propria password e a consegnare al custode delle password una busta chiusa sulla quale è indicato il proprio user-id e al cui interno è contenuta la nuova password; il custode delle password provvederà a sostituire la precedente busta con quest'ultima.

Le password verranno automaticamente disattivate dopo tre mesi di non utilizzo.

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

In caso di manutenzione straordinaria possono essere comunicate, qualora necessario, dall'amministratore di sistema al tecnico/sistemista addetto alla manutenzione le credenziali di autenticazione di servizio. Al termine delle operazioni di manutenzione l'amministratore di sistema deve ripristinare nuove credenziali di autenticazione che devono essere custodite in cassaforte.

Le disposizioni di seguito elencate sono vincolanti per tutti i posti lavoro tramite i quali si può accedere alla rete e alle banche dati contenenti dati personali e/o sensibili:

le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione e al primo utilizzo;

per la definizione/gestione della password devono essere rispettate le seguenti regole:

- la password deve essere costituita da una sequenza di minimo otto caratteri alfanumerici e non deve essere facilmente individuabile;
- deve contenere almeno un carattere alfabetico ed uno numerico;
- non deve contenere più di due caratteri identici consecutivi;
- non deve contenere lo user-id come parte della password;
- al primo accesso la password ottenuta dal custode delle password deve essere cambiata;
- la nuova password non deve essere simile alla password precedente;
- la password deve essere cambiata almeno ogni sei mesi, tre nel caso le credenziali consentano l'accesso ai dati sensibili o giudiziari;
- la password termina dopo sei mesi di inattività;
- la password è segreta e non deve essere comunicata ad altri;
- la password va custodita con diligenza e riservatezza;
- l'utente deve sostituire la password, nel caso ne accertasse la perdita.

Regole per la gestione di strumenti elettronico/informatico

Per gli elaboratori che ospitano archivi (o hanno accesso tramite la rete) con dati personali sono adottate le seguenti misure:

- l'accesso agli incaricati ed agli addetti alla manutenzione è possibile solo in seguito ad autorizzazione scritta;
- gli hard disk non sono condivisi in rete se non temporaneamente per operazioni di copia;
- tutte le operazioni di manutenzione che sono effettuate on-site avvengono con la supervisione dell'incaricato del trattamento o di un suo delegato;
- le copie di backup realizzate su ...(indicare il dispositivo, CD, cassetta, ecc...) sono conservate in...(specificare il tipo di contenitore es. armadio chiuso a chiave , e indicare la sua ubicazione)
- divieto di utilizzare floppy disk come mezzo per il backup;
- divieto per gli utilizzatori di strumenti elettronici di lasciare incustodito, o accessibile, lo strumento elettronico stesso. A tale riguardo, per evitare errori e dimenticanze, è adottato uno screensaver automatico dopo 10 minuti di non utilizzo, con ulteriore password segreta per la prosecuzione del lavoro.
- divieto di memorizzazione di archivi con dati sensibili di carattere personale dell'utente sulla propria postazione di lavoro non inerenti alla funzione svolta;
- divieto di installazione di software di qualsiasi tipo sui personal computer che contengono archivi con dati sensibili senza apposita autorizzazione scritta da parte del responsabile del trattamento dati;
- divieto di installazione sui personal computer di accessi remoti di qualsiasi tipo mediante modem e linee telefoniche.
- Il fax si trova in locale ad accesso controllato e l'utilizzo è consentito unicamente agli incaricati del trattamento

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

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

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

Regole di comportamento per minimizzare i rischi da virus

Per minimizzare il rischio da virus informatici, gli utilizzatori dei PC adottano le seguenti regole:

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

- conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge;
- conservare la copia originale del sistema operativo e la copia di backup consentita per legge;
- conservare i driver delle periferiche (stampanti, schede di rete, monitor ecc. fornite dal costruttore).

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

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

Incident response e ripristino

Tutti gli incaricati del trattamento dei dati devono avvisare tempestivamente il Responsabile del Sistema Informatico Aziendale o l'Amministratore di Sistema o il responsabile del trattamento dei dati, nel caso in cui constatino le seguenti anomalie:

- discrepanze nell'uso degli user-id;
- modifica e sparizione di dati;
- cattive prestazioni del sistema (così come percepite dagli utenti);
- irregolarità nell'andamento del traffico;
- irregolarità nei tempi di utilizzo del sistema;
- quote particolarmente elevate di tentativi di connessione falliti.

In caso di incidente sono considerate le seguenti priorità:

1. evitare danni diretti alle persone;
2. proteggere l'informazione sensibile o proprietaria;
3. evitare danni economici;
4. limitare i danni all'immagine dell'organizzazione.

Garantita l'incolumità fisica alle persone si procederà a:

1. isolare l'area contenente il sistema oggetto dell'incidente;
2. isolare il sistema compromesso dalla rete;
3. spegnere correttamente il sistema oggetto dell'incidente(vedi tabella 3).
Una volta spento il sistema oggetto dell'incidente non deve più essere riacceso;
4. documentare tutte le operazioni.

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

Altrimenti il titolare del trattamento, il responsabile del trattamento e l'amministratore di sistema coinvolgeranno esperti e/o autorità competenti. La successiva fase di indagine e di ripristino del sistema sarà condotta da personale esperto di incident response, tenendo presente quanto sotto indicato:

- eseguire una copia bit to bit degli hard disk del sistema compromesso;
- se l'incidente riguarda i dati il restore dei dati può avvenire sulla copia di cui al punto 1 precedente a partire dalle ultime copie di backup ritenute valide;
- se l'incidente riguarda il sistema operativo il ripristino deve essere effettuato reinstallando il sistema operativo su nuovo supporto.

5. MISURE DI SICUREZZA PER LA PROTEZIONE DEI DATI INFORMATICI INVIATI ALL'ESTERNO DELL'AZIENDA

L'Azienda Ospedaliera Villa Sofia e Cervello di Palermo invia con cadenza costante all'Assessorato Regionale della Salute i dati relativi all'attività, ivi compresi i dati clinici e medico legali dei pazienti.

Per l'invio, l'Assessorato ha previsto un formato criptato con chiave simmetrica a 128 bit, che consente la massima sicurezza in termini di protezione delle informazioni.

6. AGGIORNAMENTO DEL PIANO

Il presente piano è soggetto a revisione annua obbligatoria con scadenza entro il 31 marzo, ai sensi dell'art. 19 allegato B del D.L.vo 30/06/2003 Num. 196. Il piano deve essere aggiornato ogni qualvolta si verificano le seguenti condizioni:

- modifiche all'assetto organizzativo della ditta ed in particolare del sistema informativo (sostituzioni di hardware, software, procedure, connessioni di reti, ecc.) tali da giustificare una revisione del piano;
- danneggiamento o attacchi al patrimonio informativo della ditta tali da dover correggere ed aggiornare i livelli minimi di sicurezza previa analisi dell'evento e del rischio.