Documento Programmatico Sulla Sicurezza
ARNAS Ospedali “Civico - Di Cristina – Benfratelli”

Palermo

Anno 2011

Sommario

1 Riferimenti documentali

Titolo del Documento	**Documento Programmatico di Sicurezza**
Data ultimo aggiornamento	**12/03/11**

2 Principali riferimenti normativi

Visto il d.l. 196/2003 in particolare

"Titolo V - Sicurezza dei dati e dei sistemi -, capo II - misure minime di sicurezza -,

Art. 31
(Obblighi di sicurezza)
1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della
raccolta.

Art. 33
(Misure minime)
"1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

Art. 34
(Trattamenti con strumenti elettronici)
1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
a) autenticazione informatica;
b) adozione di procedure di gestione delle credenziali di autenticazione;
c) utilizzazione di un sistema di autorizzazione;
d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
g) tenuta di un aggiornato documento programmatico sulla sicurezza;
h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Visti anche il punto 19 e i relativi sottopunti dell'allegato B del d.l. 196/2003

Documento programmatico sulla sicurezza
19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:
19.1. l'elenco dei trattamenti di dati personali;
19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombono sui dati;
19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;
19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

L'azienda ha ritenuto opportuno adottare il presente "**Documento Programmatico sulla Sicurezza**".

3 Oggetto e scopo del documento

Come autorevolmente affermato dall'AIPA[1] (Autorità per l'Informatica nella Pubblica Amministrazione) la sicurezza del Sistema Informativo Automatizzato non dipende solo da aspetti tecnici, ma anche se non principalmente, da quelli organizzativi, sociali e legali[2].

L'Azienda, coglie l'occasione dell'adempimento imposto dal d.l. 196/2003, per adottare un documento programmatico sulla sicurezza come utile strumento per:

- formalizzare, razionalizzare e finalizzare le strategie aziendali in materia di sicurezza;
- definire opportune strategie per l'informazione e la formazione degli utenti aziendali sugli aspetti di sicurezza.

[1] Oggi CNIPA.

[2] AIPA, "Linee guida per la definizione di un piano per la sicurezza dei sistemi informativi automatizzati nella pubblica amministrazione", gruppo di lavoro AIPA-ANASIN-ASSINFORM-ASSINTEL

4 Elenco dei trattamenti di dati personali

In questo capitolo verranno descritti i trattamenti dei dati personali effettuati all'interno delle strutture della Azienda ai sensi del punto 19 (regola 19.1) dell'allegato B al DL 196/2003.

Nella colonna "Descrizione degli strumenti utilizzati", adotteremo la codifica DB <Nome Ditta> per indicare il Database dell'Azienda fornitrice del software deputato al trattamento in oggetto.

Laddove si fa riferimento all'applicazione indicata col nome "DB Selfin", si intende la serie di moduli funzionali acquisiti dalla società Selfin Spa, e distribuiti per le seguenti aree funzionali:

1. Area Amministrativo/Contabile
    a. CoGe (Contabilità Generale)
    b. CoGs (Contabilità Analitica)
    c. GeOr (gestione Ordini)
    d. GeMg + GeFa (Gestione Magazzini e Farmacia)
    e. GeUt (Gestione Ufficio Tecnico ed Inventario)
    f. CoGs (Contabilità Cespiti)
    g. GeCa + GeCe (Fatturazione attiva e gestione Casse economali)
    h. AnGen (Analisi Generalizzate)
    i. OsDi (Osservatorio Direzionale)
    j. Protocollo Informativo
2. Area Ufficio Personale
    a. Gsti (gestione Stipendi)
    b. RilPres (Rilevazione Presenze)
    c. StatG (Stato Giuridico)
    d. PiOr (Pianta Organica)
3. Area Sanitaria
    a. ADT (Accettazione Degenza e Trasferimenti)
    b. SDO/DRG (Scheda dimissione Ospedaliera)
    c. CUP (Centro Unico di Prenotazione)
    d. SeRad (Radiologia)
    e. DEA (Dipartimento Emergenza ed Accettazione)
    f. GeAm (Gestione Ambulatori)

Tabella 5.1

ID trattamento	Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Descrizione degli strumenti utilizzati
		S	G		
O1	Gestione anagrafica dei contatti con la struttura ospedaliera;			UU.OO. Amm.ve	DB Selfin
O2	Gestione Laboratorio Analisi ed Anatomia Patologica	S		U.O. Patologia Clinica ed U.O. Anatomia Patologica	DB Metafora
O3	Gestione Pronto Soccorso	S		U.O. Med. e Chir. d'acc. e d'urgenza	DB Selfin
O4	Gestione ricoveri (intesa come gestione amministrativa del ricovero e parte sanitaria di ricovero, esclusa gestione cartella clinica);	S		U. O. Direzione Sanitaria di Presidio, U.O. Med. e Chir. d'acc. e d'urgenza, U.O. Ostetricia e Ginecologia, U.O. 1^ Anestesia e Rianimazione, U.O. ISMETT	DB Selfin

O7	Gestione amministrativa delle grandi diagnostiche (Radiologia, medicina nucleare): comprendente almeno la schedulazione delle prestazioni in collegamento con il CUP, la gestione dei referti, la registrazione delle prestazioni erogate;	S		UU. OO. Radiologie P.O. Civico, Ascoli, Di Cristina	DB Selfin
O8	Sistema di gestione della documentazione iconografica e magazzino dei dati : sottosistema di immagazzinamento della documentazione iconografica prodotta dalle diagnostiche digitali o digitalizzate; lavora in stretta connessione con i sottosistemi di gestione amministrativa delle grandi diagnostiche;	S		UU. OO. Radiodiagnostica e TAC	
O9	Gestione Centro Unico di Prenotazione – CUP - sistema di programmazione interno delle attività, come ad esempio le consulenze interne, indagini diagnostiche per ricoverati, ecc…;	S		U.O. Direzione Sanitaria di Presidio	DB Selfin
O11	Gestione farmacia ospedaliera (comprensivo di gestione richieste da parte dei reparti, gestione ordini ai fornitori, gestione magazzini farmaceutici e gestione della reportistica per il controllo direzionale e di consumo in reparto)			U.O. Farmacia, III Sett. Amm.vo	DB Selfin
O12	Gestione Call Center e URP – ufficio rapporti con il pubblico – Ospedaliero;			U.O. Formazione, Aggiornamento Professionale ed URP	MS Office
O13	Attività di office automation ospedaliera: produzione di documenti non ascrivibili in maniera diretta ai trattamenti ospedalieri sopra elencati;	S		Tutte le UU.OO.	MS Office
O14	Gestione dei flussi informativi ospedalieri obbligatori con la regione e i ministeri: gestione della mobilità, registri sanitari, CEDAP, ecc…	S		U.O. Sistema Informativo e Statistico, Direzioni Sanitarie di Presidio, U.O. Ostetricia e Ginecologia	DB Selfin, DB Access
O15	Gestione Centro Trasfusionale.	S		U.O. Medicina Trasfusionale	DB EMONET
A1	Gestione del personale (comprensivo di trattamento economico, rilevazione della presenza assenza, gestione concorsi, gestione stato giuridico matricolare, pianta organica, aspetti contributivi e previdenziali);	S		Area Risorse Umane	DB Selfin
A2	Gestione logistica (comprensivo di gestione richieste dal reparto, gestione ordini, gestione magazzini, gestione fatturazione passiva);			Area Provveditorato, Area Tecnica Patrimoniale, Area AA.GG., Area Risorse Economiche	DB Selfin
A3	Controllo di gestione e supporto decisionale alla direzione aziendale (comprensivo di sistema di generazione dinamica della reportistica e del data warehouse dei costi e dei ricavi);			U.O. Statistica aziendale, programmazione e Controllo di Gestione	DB Selfin
A4	Gestione contabile (comprensiva di contabilità generale, gestione cespiti, fatturazione attiva, recupero crediti e flussi			II Settore Amm.vo	DB Selfin

	per la messa a ruolo dei mandati di pagamento);				
A6	Gestione inventario aziendale (eventualmente integrato con la gestione tecnica dei servizi di supporto);			U.O Patrimoniale e Tecnico	DB Selfin
A7	Gestione protocollo			U.O. Affari Generali	DB Selfin
A8	Gestione delibere			U.O. Affari Generali	MS SQL Server
A9	Gestione casse	S		U.O. Direzione Sanitaria di Presidio	DB Access (applicazione Ticket-Office V. 2.5)
A11	Gestione Ufficio Affari Legali (comprensivo della gestione di ingiunzioni, pignoramenti, transazioni, citazioni, diffide, ricorsi, ordinanze, gestione aspetti assicurativi, tenuta repertorio contratti, consulenza interna agli altri servizi)	S	G	Area Affari Generali e Legali	MS Office
T1	Network Management e monitoraggio della rete;			U.O. Sistemi Informatici e Telecomunicazioni	Enterasys Netsigth+ Tools Open Source
T2	Security Management (comprendente almeno la gestione degli utenti e dei profili abilitativi e delle apparecchiature di presidio del confine aziendale tipo Firewall e Access Server);			U.O. Sistemi Informatici e Telecomunicazioni	Tools Open Source
T5	Gestione degli elenchi telefonici aziendali			U.O. Sistemi Informatici e Telecomunicazioni	MS Office
T6	Gestione dell'accesso ad INTERNET ed INTRANET per servizi di connettività: mail, browsing, FTP, Telnet, ecc…			U.O. Sistemi Informatici e Telecomunicazioni	Firewall, IDS, Antivirus, Mail Server, Web Server
T7	Gestione dell'autorizzazione e dell'accreditamento delle strutture sanitarie;			U.O. Sistema Qualità Aziendale	MS Office
S1	Gestione del Servizio Attività Tecniche (eventualmente integrato con la gestione cespiti e la gestione contabile per quanto attiene al ciclo passivo);			Area Tecnico Patrimoniale	DB Selfin
Data di aggiornamento **12/03/11**					

Tabella 5.2

ID tratta mento	DataBase	Ubicazione Fisica dei Supporti di Memorizzazione	Tipologia dei dispositivi d'accesso	Tipologia di intercon-nessione
O1	DB Selfin	Cluster Geografico Aziendale	PC	LAN
O2	DB Metafora	Cluster Geografico Aziendale	PC	LAN
O3	DB Selfin	Cluster Geografico Aziendale	PC	LAN
O4	DB Selfin	Cluster Geografico Aziendale	PC	LAN
O7	DB Selfin (SeRad)	Cluster Geografico Aziendale	PC	LAN
O8	DB General Electric	PC Server di reparto	PC	LAN
O9	DB Selfin	Cluster Geografico Aziendale	PC	LAN
O11	DB Selfin	Cluster Geografico Aziendale	PC	LAN
O12	MS Office	PC di UO	PC	
O13	MS Office	PC di UO	PC	
O14	DB Selfin, DB Access	Cluster Geografico Aziendale	PC	LAN
O15	DB Emonet	Cluster Geografico Aziendale	PC	LAN
A1	DB Selfin	Cluster Geografico Aziendale	PC	LAN

A2	DB Selfin	Cluster Geografico Aziendale	PC	LAN
A3	DB Selfin	Cluster Geografico Aziendale	PC	LAN
A4	DB Selfin	Cluster Geografico Aziendale	PC	LAN
A6	DB Selfin	Cluster Geografico Aziendale	PC	LAN
A7	DB Selfin	Server IT	PC	LAN
A8	MS Office	PC Server di UO	PC	LAN
A9	Ticket-Office V.2.5 su MS Access DB	PC WXP	PC	LAN
A11	MS Office	PC Server di UO	PC	LAN
T1	Tools Open Source	PC Server di UO	PC	LAN
T2	Tools Open Source	PC Server di UO	PC	LAN
T5	MS Office	PC di UO	PC	LAN
T6	Firewall, IDS, Antivirus, Mail Server, Web Server	PC Server di UO	PC	LAN
T7	MS Office	PC di UO	PC	LAN
S1	DB Selfin	Cluster Geografico Aziendale	PC	LAN
Data di aggiornamento **12/03/11**				

5 Distribuzione dei compiti e delle responsabilità

Il Titolare del Trattamento nomina quali Responsabili del trattamento i soggetti che ricoprono le seguenti posizioni:

- DIRIGENTE UNITA' OPERATIVA INFORMATIZZAZIONE E TELECOMUNICAZIONI
- DIRIGENTE UNITA' OPERATIVA COMPLESSA SANITARIA
- DIRIGENTE AREA AMMINISTRATIVA
- DIRIGENTE UNITA' OPERATIVA SEMPLICE DIPARTIMENTALE SANITARIA
- DIRIGENTE STAFF DIREZIONE GENERALE/AMMINISTRATIVA/SANITARIA

Con l'articolazione che segue:

- Il soggetto di cui al punto A. è unico responsabile del trattamento in relazione alle politiche di sicurezza per la gestione centralizzata dei dati personali con strumenti elettronici. Per quanto appena esposto è pertanto unico soggetto autorizzato a decidere su aspetti quali: gestione dei requisiti delle credenziali di autenticazione per l'accesso al dominio ed agli applicativi centralizzati, gestione delle politiche di protezione dei dati e dei sistemi, gestione delle politiche di back-up e disaster recovery. In relazione a tali aspetti assume anche il ruolo di Amministratore di sistema, identificando quali tra i suoi collaboratori possano assumere a loro volta tale ruolo.
- Tutti i soggetti nominati responsabili del trattamento, ognuno nell'ambito di propria competenza, possono:
  - Identificare i soggetti da nominare quali incaricati del trattamento
  - In relazione all'incarico di trattamento con strumenti elettronici:
    i. Richiedono al soggetto di cui al Punto A. l'attivazione, modifica o blocco delle credenziali di autenticazione per l'accesso al dominio o ai gestionali centralizzati
    ii. Identificano le politiche di sicurezza relativamente alla gestione periferica con l'ausilio di strumenti elettronici (con particolare riferimento a strumenti scientifici stand alone ed a eventuali files o basi di dati creati su singoli client), identificando i relativi Amministratori di sistema e dandone comunicazione al soggetto di cui al Punto A.
    iii. Identificano le politiche di sicurezza relativamente alla gestione periferica senza l'ausilio di strumenti elettronici
  - In relazione all'incarico di trattamento con senza l'ausilio di strumenti elettronici identificano le politiche di sicurezza relativamente alla gestione periferica del trattamento dei dati personali in formato cartaceo.

Nel quadro dei propri doveri di vigilanza, il Titolare del trattamento:

- avvalendosi del soggetto di cui al Punto A. e della Direzione Sanitaria, effettua controlli a campione sulla gestione periferica dei dati personali trattati con l'ausilio degli strumenti elettronici
- avvalendosi della Direzione Sanitaria, effettua controlli a campione sulla gestione periferica dei dati personali trattati senza l'ausilio degli strumenti elettronici

Quanto all'identificazione degli incaricati del trattamento, i Responsabili del Trattamento si attengono alle seguenti linee guida generali:

- L'identificazione deve avvenire preferibilmente per categorie omogenee, costituite da persone fisiche che rivestano mansioni sovrapponibili (es. infermieri, tecnici sanitari, addetti contabilità e amministrazione), con l'identificazione di idonee modalità di informazione agli incaricati sulla propria categoria di appartenenza.
- Dove emergano peculiarità, si procede con la designazione nominativa o con la creazione di categorie omogenee di dettaglio (es. infermieri caposala, tecnici di radiologia)

I relativi documenti sono e custoditi ed aggiornati a cura dei soggetti sopra identificati in relazione ai compiti assegnati.

Con nota prot. n. 1132/DG del 16/12/2009 il Direttore Generale, nella qualità di titolare del trattamento dati, ha nominato i Responsabili del trattamento dati.

Ogni Responsabile è incaricato di redigere ed archiviare i modelli indicati nell'appendice 8 – Modelli DPS – entro il primo di febbraio di ogni anno. Tali modelli, debitamente compilati descrivono non solo la distribuzione dei

compiti e delle responsabilità di ogni responsabile e degli incaricati per le singole unità operative, ma un vero e proprio DPS nell'ambito della stessa unità operativa.

Ogni responsabile è tenuto a comunicare al responsabile della U.O. Sistemi Informatici per ognuno degli incaricati l'elenco delle funzionalità alla quali abilitare/disabilitare l'incaricato mediante il MODELLO E (vedasi appendice 7).

Ogni Responsabile è tenuto a comunicare tempestivamente al responsabile della U.O. Sistemi Informatici la modifica/revoca delle abilitazioni di un incaricato nel caso in cui quest'ultimo cambi mansioni, venga trasferito ad altro reparto o cessi il rapporto con l'Azienda Ospedaliera.

6 La valutazione del rischio

6.1 Analisi del rischio

L'analisi del rischio costituisce una fase fondamentale di ogni percorso di sicurezza.

Questo piano programmatico in larga misura tratta dell'adozione di misure minime di sicurezza, obbligatorie per legge, e quindi non graduabili. La valutazione del rischio sarà comunque utilizzata per tutte quelle situazioni in cui l'adozione di misure minime sia non sufficiente e pertanto si debba valutare una gradazione delle misure adottabili. I rischi d a considerare sono quelli che hanno un impatto sulle seguenti caratteristiche che la legge impone di tutelare:

1. Disponibilità
2. Riservatezza
3. Integrità

In tali contesti, cioè qualora sia necessaria una graduazione delle misure adottabili, si dovrà adottare una valutazione del rischio basata sui seguenti criteri:

1. si considerano gravi le minacce che possono limitare e/o rendere difficoltosa l'erogazione della attività assistenziale e/o rese al pubblico;
2. si considerano gravi le minacce che portano alla divulgazione/modifica/produzione illegittima di dati sensibili o che comportino un danno patrimoniale per l'azienda;

In particolare:

3. si considerano **gravi le minacce che possono limitare la disponibilità di servizi informatici a supporto delle attività assistenziali o delle attività rese al pubblico**;
4. si considerano **gravi le minacce che portano alla modifica illecita di messaggi - e quindi di informazioni gestite dall'azienda - qualora tali messaggi abbiano un valore medico-legale o la loro modifica comporti un danno patrimoniale per l'azienda**;
5. si considerano **gravi le minacce di fraudolenta impersonificazione - masquerade - qualora ciò porti alla produzione di falsi atti con valore medico-legale o che comportino un danno patrimoniale per l'azienda**;
6. si considerano **gravi le minacce di fraudolenta impersonificazione - masquerade - qualora ciò porti alla modifica fraudolenta di atti con valore medico-legale originariamente legittimi, o qualora ciò porti ad un danno patrimoniale per l'azienda**;
7. si considerano **gravi le minacce di intercettazione qualora i dati intercettabili riguardino dati personali di natura sensibile ai sensi della legge sulla tutela dei dati personali**.

Si considerano in genere trascurabili le minacce di analisi del traffico e di ripetizione, a patto che esse non portino a conseguenze elencate nei punti sopra elencati.

6.2 Le Misure di Sicurezza poste in atto

La protezione dei dati in Azienda è basata su un insieme di misure di sicurezza complementari. Esse sono di tipo :

1. **Fisico.** Quando si parla di Sicurezza Fisica si fa riferimento a misure atte a garantire la sicurezza dei locali che ospitano gli apparati hardware da:
    a. accessi indesiderati,
    b. danneggiamenti dovuti a eventi naturali, quali incendi, allagamenti etc.,
    c. interruzione di corrente,
    d. sabotaggi,
    e. furti,
    f. alla necessità di salvaguardare i dati e le procedure (Software) da problemi causati dal cedimento di qualche componente elettronico o meccanico (Hardware).

2. **Organizzativo.** Tali misure sono rappresentate dalle Procedure in vigore in Azienda. E' compito di tutti i livelli di supervisione garantirne la necessaria applicazione.

3. **Logico o informatico.** Per la Sicurezza Logica si fa riferimento alle misure atte a garantire la sicurezza dei dati e del software da:

a. accesso non autorizzato con visualizzazione di informazioni riservate
b. furto di programmi sorgente
c. virus
d. errori nella progettazione e sviluppo
e. errori di utilizzo
f. modifica e/o cancellazione accidentale
g. modifica e/o cancellazione fraudolenta

Nel capitolo 7 sono discusse le motivazioni che hanno portato alla implementazione delle misure di sicurezza adottate, le Politiche di sicurezza che l'Azienda ha deciso di adottare e le modalità di gestione del rischio. Di seguito, con un moderato livello di sintesi, si descrivono le misure adottate.

Misure di tipo "Fisico":

F1- Sicurezza dei locali.

Il centro stella della dorsale di rete è concentrato in armadi protetti da chiusura di sicurezza, ubicati nel piano terra della palazzina "Amministrazione". Il CED, realizzato nella stessa palazzina, ma ubicato al primo piano, è normalmente chiuso a chiave. L'utilizzo degli ambienti è sempre presidiato da addetti della UU.OO. Informatizzazione e Telecomunicazioni che gestisce la struttura. I locali sono protetti da impianto di allarme volumetrico ed ogni addetto possiede un proprio codice personale per la attivazione/disattivazione dello stesso. L'impianto di allarme è connesso per via telefonica alla vigilanza.

F2- Sicurezza dei locali (Uffici). In ogni ufficio l'accesso è riservato al solo personale autorizzato.

F3- Sicurezza dei locali (CED).

L'azienda ha riservato tre locali con funzioni di sala macchine. Il primo, di seguito indicato con CED1, è sito al piano primo della palazzina Amministrazione. L'accesso al locale "CED 1", e' consentito solo al personale in possesso di autorizzazione. La rete elettrica è alimentata da un sistema UPS di continuità. Il sistema di condizionamento è indipendente. Un gruppo elettrogeno protegge i sistemi da prolungati periodi di assenza di alimentazione esterna. La sala è dotata di impianto di allarme volumetrico, antincendio e antiallagamento e termostato. L'impianto di allarme è connesso per via telefonica alla vigilanza.

Il secondo locale, di seguito indicato con CED2, è sito al piano terra della palazzina della Chirurgia toracica. L'accesso al locale "CED 2", e' consentito solo al personale in possesso di autorizzazione. La rete elettrica è alimentata da un sistema UPS di continuità. Il sistema di condizionamento è indipendente. Un gruppo elettrogeno protegge i sistemi da prolungati periodi di assenza di alimentazione esterna. La sala è dotata di impianto di allarme volumetrico.

Il terzo locale, di seguito indicato con CED3, è sito al piano terra della palazzina Amministrazione. L'accesso al locale "CED 3", e' consentito solo al personale in possesso di autorizzazione. La rete elettrica è alimentata da un sistema UPS di continuità. Il sistema di condizionamento è indipendente. Un gruppo elettrogeno protegge i sistemi da prolungati periodi di assenza di alimentazione esterna.

F4- Sicurezza dei locali (Ufficio del Dirigente).

Il PC del Dirigente è ubicato all'interno di una stanza, alla quale si accede dopo avere varcato una sala d'ingresso che è presidiata da personale di segreteria. In assenza del dirigente, la stanza è chiusa a chiave e la chiave è in possesso del Dirigente.

F6-Sicurezza dei componenti informatici (Server).

I Server dei database amministrativi e sanitario utilizzano una soluzione SAN ridondata per lo storage dei dati. Il loro Backup è affidato a personale Tecnico della Ditta SELFIN. Il database Oracle contenente i dati amministrativi e sanitari è ospitato da un sistema cluster geografico costituito da due nodi gemelli (server e SAN IBM) e gestiti in configurazione di failover attivo-attivo. Il primo nodo, è sito presso il CED al primo piano del padiglione amministrativo, mentre il secondo è sito al piano terra della chirurgia Toracica. I dati vengono registrati in tempo reale su entrambi i nodi garantendo così la salvaguardia degli stessi in caso di disastro che interessasse uno dei due siti.

F7-Sicurezza dei componenti informatici (Rete). La struttura a "collapsed back-bone" è composta da apparati di rete Enterasys posti nei diversi padiglioni. Gli switches ubicati in alcuni padiglioni, raccolgono traffici locali e traffici di altri padiglioni. In particolare, i collegamenti attuali sono riportati nell'allegato T-6.2-2, mentre

l'elenco delle Virtual LAN (VLAN) è definito nell'allegato T-6.2-3. Le dorsali di collegamento sono pertanto le seguenti:

1. Amministrazione
    a. Nuova Emergenza
    b. Chir. Toracica
    c. Medicina
    d. Chirurgie
    e. Osp. Dei Bambini
    f. Maternità
2. Medicina
    a. Medicina2
    b. Maternità
3. Nuova Emergenza
    a. Chir. Plastica
    b. Amministrazione
    c. Medicina
    d. Chir. Toracica
4. Chir. Toracica
    a. Oncologico
    b. Amministrazione
    c. Nuova Emergenza
    d. Chir. Specialistica
5. Oncologico
    a. Magazzino
    b. Farmacia
    c. Chirurgie
    d. Amministrazione
    e. Chir. Toracica
6. Chir. Specialistica
    a. Cardiochirurgia
    b. Chir. Vascolare
    c. Chir. Toracica

La rete è pertanto magliata in più punti, e questo consente di gestire in maniera automatica condizioni di failover localizzate. L'algoritmo di Spanning-Tree degli switch effettua infatti in automatico il re-routing dei link in standby in caso di fallimento dei link primari. La connessione fra le varie aree e' realizzata in fibra.
L'assistenza e la manutenzione della rete è affidata con contratto di outsourcing alla Telecom Italia Spa con livelli di servizio prefissati.
La connessione ad Internet avviene tramite Firewall Netfilter su Sistema Operativo Linux.

F8-Sistemi di gestione e monitoraggio traffico di rete. Per la gestione e la individuazione degli errori viene utilizzato uno Sniffer. Il sistema permette di controllare il carico della rete ed i pacchetti in transito.
La rete è monitorata attraverso il software enterasys NetSight Manager.

F9-Sicurezza dei componenti informatici (PC e stampanti). La manutenzione è gestita sulla base delle condizioni di garanzia del produttore. E' attivo un contratto di manutenzione del parco installato di PC e stampanti con tempo di risposta non definito.

F10-Sicurezza dei supporti di backup
I supporti di backup vengono archiviati in apposita cassaforte ignifuga ed antiscasso sita presso i locali della U.O. Informatizzazione e Telecomunicazioni.

F11- Contratti di manutenzione
L'hardware ed i software utilizzati dall'ARNAS sono coperti da contratti di manutenzione che vengono rinnovati alla scadenza.

F12- Registrazione degli accessi degli amministratori ai sistemi informatici
E' stato posto in essere un sistema di raccolta dei dati di accesso degli amministratori ai sistemi informatici contenenti dati personali o sensibili. Il primo DVD è stato prodotto e conservato nella cassaforte ignifuga presso

la UO Sistemi Informatici. Il Sistema di rilevazione raccoglie i log giornalmente e li archivia sul server di dominio. Periodicamente verranno effettuai i salvataggi dei dati su supporto DVD ed archiviati.

Misure di tipo "Organizzativo" :
O1-Istruzioni per incaricati al trattamento dei dati personali. Con nota prot. n. 1132/DG del 16/12/2009 si è incaricato ogni Responsabile del Trattamento di distribuire a tutti i collaboratori apposita lettera, per partecipare a ciascuno, il ruolo di incaricato, con relative istruzioni comportamentali. Ogni Responsabile è tenuto ad archiviare le lettere di incarico/revoca ed inviarle al responsabile della U.O. Informatizzazione e Telecomunicazioni qualora tali incarichi comportino la definizione/modifica/cancellazione di profili utente,

O2-Autorizzazione per incaricati al trattamento dei dati personali particolari. Vedi la lettera distribuita (e firmata per accettazione) agli incaricati al trattamento di Dati Particolari. Con l'autorizzazione si definiscono anche i vincoli comportamentali.

O3-Autorizzazione per Amministratori di Sistemi. Vedi la lettera distribuita (e firmata per accettazione) a tutti i dipendenti assegnati alla Funzione "Sistemi Informatici e Telecomunicazioni". Con l'autorizzazione si definiscono anche i vincoli comportamentali.

O5-Misure di sicurezza per il trattamento dei Dati personali (legge 675/96 –DPR 318/99, Legge 196/2003). Vedi la Circolare interna n° 1132/DG del 16/12/2009 che divulga l'informativa della Legge e fornisce una guida per l'applicazione delle misure di sicurezza per il trattamento dei dati personali.

O6- Linee guida per l'accesso e l'utilizzo dei servizi informatici aziendali. Vedi appendice 6 "Regole Tecniche per la sicurezza dei Sistemi informatici Aziendali".

O7- Guida Amministratori di sistemi
Vedi la nota operativa per l'area Sistemi Informativi, dove vengono descritte le linee guida per la configurazione delle workstation e per la creazione e gestione del codice identificativo personale che e' assegnato agli utenti abilitati ad accedere alle procedure informatiche.

O8-Piano di Emergenza. E' la procedura, ampiamente diffusa e nota a tutti i dipendenti, da applicare in caso di emergenza. Classificato l'evento, sono univocamente definiti i compiti ed i comportamenti di ogni persona presente in Istituto. Ciò allo scopo di ottenere :

- la protezione delle persone presenti
- il contenimento immediato dell'emergenza
- la minimizzazione dei danni all'ambiente ed ai beni aziendali
- la bonifica e la messa in sicurezza della zona coinvolta
- la corretta trasmissione di informazioni agli Enti preposti ed agli organi di informazione.

O9-Formazione e manuali operativi
Sensibilizzazione legge 675 e della 196/2003**:** formazione per gli incaricati del trattamento di Dati Particolari sui rischi individuati e sulle modalità per prevenirli.
Per le procedure informatiche in occasione dell'avviamento o di un aggiornamento di release vengono organizzati dei corsi di formazione per gli utenti preposti all'utilizzo. Inoltre per le procedure più critiche viene realizzato anche un manuale d'uso.

O10-Politica dei salvataggi. Vedi politica di backup dove vengono descritte la frequenza e le modalità con cui vengono salvati i dati dei vari sistemi informativi di Istituto.

O11- Normativa per l'utilizzazione di Internet
Vedi linee guida per l'uso di Internet.

Sono di tipo "Logico o informatico" :
L1-Codice di accesso e parola chiave. L'accesso all'elaboratore per le operazioni di trattamento dei dati o di manutenzione può avvenire esclusivamente tramite codice identificativo e password personale. La password iniziale è impostata ad un valore predefinito e ne viene automaticamente richiesta la modifica al primo accesso. La username per il personale esterno, per i quali è richiesta l'abilitazione alle operazioni di manutenzione dei server e della rete è gestita manualmente.

La password, strettamente personale, è gestibile dall'incaricato in maniera autonoma. In particolare la password iniziale è impostata ad un valore predefinito e ne viene richiesta la modifica al primo accesso ed, in quasi tutti i sottosistemi, anche a scadenze periodiche (6 mesi).

L2-Accesso ai computer ed ai dati in rete. I dati del sistema informativo aziendale sono classificati e ripartiti in relazione alle procedure informatiche preposte per la loro gestione. L'accesso ai dati è concesso mediante una serie di permessi impostati con tecnicismi differenti a seconda dei vari sistemi (Windows, Unix), rispondenti, comunque, ad una unica regola: la user-id può accedere solamente alle funzioni cui è stata autorizzata, in osservanza alle procedure in vigore.
Ancora, i database aziendali sono custoditi su particolari server il cui accesso diretto (tramite user-id e password) è consentito solo agli Amministratori di Sistema. Quanto ad altri utilizzatori, i database sono accessibili solamente attraverso il regolare uso delle applicazioni.

L3-Protezione dei sistemi da virus. Mediante adeguati programmi di intercettazione, è garantita la protezione del sistema informatico aziendale e dei dati in esso custoditi contro la minaccia di intrusione rappresentata da "virus".
Il software di controllo Symantec Antivirus Corporate Editino Versione 10.0 è installato su un server (IP: 172.16.64.130) che, giornalmente, si connette ai servizi Internet del produttore per acquisire la versione più aggiornata dell'antivirus. Questa versione è poi distribuita in automatico sui PC della rete interna. Non è presente alcun controllo che verifichi che il software antivirus sia installato ed aggiornato sui PC della rete interna.
Ogni utente può controllare sempre e facilmente se la funzione "antivirus" è presente .

L4-Protezione dei sistemi da accessi esterni non autorizzati.
Per evitare che reti non autorizzate accedano alla Lan aziendale è presente un sistema con funzione di firewall Software.
Il firewall è stato configurato con una struttura scalabile e facilmente gestibile, tramite la definizione di 3 aree: INSIDE (Amministrazione, rete Intranet) , OUTSIDE HDSL, DMZ.
La DMZ è l'area in cui vengono definiti gli indirizzi delle macchine WWW e Mail relay.
L' INSIDE e' l'area che comprende tutta la Intranet.
L'OUTSIDE e' l'area in cui e' definito il router Cisco 2600 per il collegamento ad Internet. Tale router è stato acquisito nell'ambito del contratto di noleggio della linea HDSL da 2 Mbps della Telecom Spa. La configurazione e la gestione del router è a totale carico della Telecom Spa.
Inoltre, un sistema di network IDS, in ascolto dei taffici presenti sulla dorsale rileva le anomalie presenti nei pacchetti in transito riportando gli allarmi. Per la configurazione del Firewall e del sistema IDS, vedasi il documento "Configurazione del Firewall"

L5-Protezione da errori nella progettazione e sviluppo.
Il software di base viene aggiornato alle ultime versioni o releases di cui si abbia certezza di mancanza di errori.
E' stata posta in essere una soluzione con SUS server che forza l'aggiornamento dei PC centralmente, una volta scaricati dal sito Microsoft gli hotfix, i Service Packs, etc.

L6-Protezione della disponibilità e della integrità dei dati.
Il database Oracle contenente i dati amministrativi e sanitari è ospitato da un sistema cluster geografico ad alta affidabilità costituito da due nodi gemelli e gestiti in configurazione di failover.

6.2.1 RISCHI DI MAGGIORE RILEVANZA E SOGLIE DI ACCETTABILITÀ

Ai fini delle analisi seguenti si presuppone di poter individuare un dominio di sicurezza aziendale di cui è possibile definire un confine, che discrimina l'interno e l'esterno. Il dominio di sicurezza è rappresentato dall'insieme di attrezzature, procedure organizzative e risorse umane che fanno riferimento ad una medesima autorità in grado di determinare le politiche e gli strumenti di sicurezza adeguati allo scopo e rispondenti alla normativa vigente.

Di seguito, per ogni trattamento, descritto nel capitolo precedente, sono state messe a confronto le "minacce" con le Misure di Sicurezza in atto per fare emergere eventuali vulnerabilità che espongono il servizio ad un certo livello di rischio.
Per sintetizzare in maniera tabellare quanto attiene a questo paragrafo, sono state codificate le "Misure di sicurezza in atto" descritte nel paragrafo precedente e le possibili Minacce.

Codice	Misure di sicurezza in atto

F1	Sicurezza dei locali.
F2	Sicurezza dei locali (Uffici)
F3	Sicurezza dei locali (CED)
F4	Sicurezza dei locali (Ufficio del Dirigente)
F6	Sicurezza dei componenti (server).
F7	Sicurezza dei componenti (rete)
F8	Sistemi di gestione e monitoraggio traffico di rete
F9	Sicurezza dei comp. (PC-Printer)
F10	Sicurezza dei supporti di backup
F11	Contratto di manutenzione
O1	Istruzioni per Incaricati (dati Personali)
O2	Autorizzaz. per Incaricati (dati Sensibili)
O3	Autorizzazione per Amministratori Sistemi
O4	Politiche di sicurezza IT
O5	Circolare Trattamento dati Personali
O6	Linee guida per l'accesso e l'utilizzo dei servizi informatici aziendali
O7	Guida Amministratori di sistemi
O8	Piano di emergenza di Istituto
O9	Formazione
O10	Politica dei salvataggi.
O11	Normativa per l'utilizzazione di Internet
L1	Codice di accesso e parola chiave
L2	Accesso ai computer ed ai dati in rete
L3	Protezione dei sistemi da virus.
L4	Protezione dei sistemi da accessi esterni
L5	Protezione da errori di progettaz. e sviluppo

Codice	**Minacce**
M1	Eventi naturali, quali incendi, allagamenti
M2	Interruzione di corrente
M3	Guasti hardware
M4	Sabotaggi e furti degli apparati
M5	Errori nella progettazione e sviluppo delle applicazioni
M6	Errori di utilizzo (modifica e/o cancellazione)
M7	Virus
M8	Accesso non autorizzato a informazioni riservate, abuso di privilegi

Ai fini della valutazione del livello di rischio, verranno inoltre utilizzate le seguenti tabelle esplicative:

6.3 Tavola delle Probabilità

Livello di Probabilità	**Definizione di Probabilità**
Alto	La fonte della minaccia è molto motivata e sufficientemente capace. I controlli per prevenire che la vulnerabilità si attui sono inefficaci.
Medio	La fonte della minaccia è motivata e sufficientemente capace, ma sono stati messi in atto controlli che ne possono impedire l'attuazione.
Basso	La fonte della minaccia non è motivata e/o sufficientemente capace. Controlli sono stati posti in essere per impedire l'attuazione della vulnerabilità.

6.4 Tavola degli Impatti

Valore d'impatto	**Definizione dell'impatto**

Alto	Lo sfruttamento della vulnerabilità (1) può portare alla perdita di beni e risorse essenziali; (2) può violare, danneggiare o impedire la missione, la reputazione o gli interessi aziendali; o (3) può persino portare alla perdita di vite umane
Medio	Lo struttamento della vulnerabilità (1) può portare alla perdita di beni e risorse; (2) può violare, danneggiare o impedire la missione, la reputazione o gli interessi aziendali; o (3) può provocare danni agli individui
Basso	Lo struttamento della vulnerabilità (1) può portare alla perdita di alcuni beni e risorse or (2) può violare, danneggiare o impedire la missione, la reputazione o gli interessi aziendali

6.5 Matrice del Livello di Rischio

	Impatto		
Probabilità della Minaccia	***Basso*** (10)	***Medio*** (50)	***Alto*** (100)
Alto (1.0)	**Basso** 10 X 1.0 = 10	**Medio** 50 X 1.0 = 50	**Alto** 100 X 1.0 = 100
Medio (0.5)	**Basso** 10 X 0.5 = 5	**Medio** 50 X 0.5 = 25	**Medio** 100 X 0.5 = 50
Basso (0.1)	**Basso** 10 X 0.1 = 1	**Basso** 50 X 0.1 = 5	**Basso** 100 X 0.1 = 10

Scala del Rischio: Alto (>50 e <100); Medio (>10 e <50); Basso (tra 1 e 10)

6.6 Scala dei Rischi ed Azioni necessarie

Livello di Rischio	**Descrizione del Rischio e Azioni necessarie**
Alto	In caso di Alto rischio, vanno prese urgentemente azioni correttive.
Medio	In caso di Medio rischio, le azioni correttive sono necessarie e deve essere predisposto un piano d'azione per realizzare le protezioni necessarie in un tempo ragionevole.
Basso	In caso di Basso rischio l'azienda deve determinare se sono necessarie azioni correttive o decidere se accettare il livello di rischio residuo.

In generale si considera accettabile un rischio inferiore o uguale a 10
Per tutti i trattamenti per i quali l'indice di rischio supera la soglia di accettabilità s adottare le misure di abbattimento del rischio di seguito illustrate:

1. Firewall
2. Antivirus
3. Controllo configurazione
4. Backup

5. Analisi dei log
6. Scadenza password (Policy aziendale)
7. Verifica periodica delle vulnerabilità

6.7 Elenco dei trattamenti e dei rischi associati

O1- Gestione anagrafica dei contatti con la struttura ospedaliera

		MISURE DI SICUREZZA	**VULNERABILITA'**	**Rischio (Effetti x Probabilita')**
Minacce	**M1**	F1 F3 F6 F10 F11	---	---
	M2	F3	---	---
	M3	F6 F11	Scadenza contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---
	M5	L5		Medio (30)
	M6	L1 L2 L4 O4 O6 O9 O10	Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6	---	Basso (10)
	M8	F1 F3 F6 O3 O4 O6 O7 L1 L2 L3 L4	---	---

O2- Gestione Laboratorio Analisi ed Anatomia Patologica

		MISURE DI SICUREZZA	**VULNERABILITA'**	**Rischio (Effetti x Probabilita')**
Minacce	**M1**	F1 F3 F6 F10 F11	---	---
	M2	F3	---	---
	M3	F6 F11	Scadenza contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---
	M5	L5		Medio (30)
	M6	L1 L2 L4 O4 O6 O9 O10	Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6	---	Basso (10)
	M8	F1 F3 F6 O3 O4 O6 O7 L1 L2 L3 L4	---	---

O3 - Gestione Pronto Soccorso

		MISURE DI SICUREZZA	**VULNERABILITA'**	**Rischio (Effetti x Probabilita')**
Minacce	**M1**	F1 F3 F6 F10 F11	---	---
	M2	F3	---	---
	M3	F6 F11	Scadenza contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---
	M5	L5		Medio (30)
	M6	L1 L2 L4 O4 O6 O9 O10	Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6	---	Basso (10)

	M8	F1 F3 F6 O3 O4 O6 O7 L1 L2 L3 L4	---	---

O4 - Gestione ricoveri

		MISURE DI SICUREZZA	**VULNERABILITA'**	**Rischio (Effetti x Probabilita')**
Minacce	**M1**	F1 F3 F6 F10 F11	---	---
	M2	F3	---	---
	M3	F6 F11	Scadenza contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---
	M5	L5		Medio (30)
	M6	L1 L2 L4 O4 O6 O9 O10	Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6	---	Basso (10)
	M8	F1 F3 F6 O3 O4 O6 O7 L1 L2 L3 L4	---	---

O7 - Gestione amministrativa delle grandi diagnostiche

		MISURE DI SICUREZZA	**VULNERABILITA'**	**Rischio (Effetti x Probabilita')**
Minacce	**M1**	F1 F3 F6 F10 F11	---	---
	M2	F3	---	---
	M3	F6 F11	Scadenza contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---
	M5	L5		Medio (30)
	M6	L1 L2 L4 O4 O6 O9 O10	Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6	---	Basso (10)
	M8	F1 F3 F6 O3 O4 O6 O7 L1 L2 L3 L4	---	---

O8 - Sistema di gestione della documentazione iconografica e magazzino dei dati

		MISURE DI SICUREZZA	**VULNERABILITA'**	**Rischio (Effetti x Probabilita')**
Minacce	**M1**	F1 F3 F6	---	---
	M2	F3	---	---
	M3	F6 F11	Mancanza di parti spare e di contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---
	M5	L5		Medio (30)
	M6	L1 L2 L4 O4 O6 O9 O10	Mancanza di Backup centralizzato, Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6	Mancanza di controlli periodici	Medio (30)

	M8	F1 F3 O3 O4 O6 O7 L1 L2 L4	Mancanza verifica periodica vulnerabilità	Alto (90)

O9 - Gestione Centro Unico di Prenotazione – CUP

		MISURE DI SICUREZZA	**VULNERABILITA'**	**Rischio (Effetti x Probabilita')**
Minacce	**M1**	F1 F3 F6 F10 F11	---	---
	M2	F3	---	---
	M3	F6 F11	Scadenza contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---
	M5	L5		Medio (30)
	M6	L1 L2 L4 O4 O6 O9 O10	Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6	---	Basso (10)
	M8	F1 F3 F6 O3 O4 O6 O7 L1 L2 L3 L4	---	---

O11 - Gestione farmacia ospedaliera

		MISURE DI SICUREZZA	**VULNERABILITA'**	**Rischio (Effetti x Probabilita')**
Minacce	**M1**	F1 F3 F6 F10 F11	---	---
	M2	F3	---	---
	M3	F6 F11	Scadenza contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---
	M5	L5		Medio (30)
	M6	L1 L2 L4 O4 O6 O9 O10	Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6	---	Basso (10)
	M8	F1 F3 F6 O3 O4 O6 O7 L1 L2 L3 L4	---	---

O12 - Gestione Call Center e URP

		MISURE DI SICUREZZA	**VULNERABILITA'**	**Rischio (Effetti x Probabilita')**
Minacce	**M1**	F1 F3 F6	---	---
	M2	F3	---	---
	M3	F6 F11	Mancanza di parti spare e di contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---
	M5	L5		Medio (30)
	M6	L1 L2 L4 O4 O6 O9 O10	Mancanza di Backup centralizzato, Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6	Mancanza di controlli periodici	Medio (30)
	M8	F1 F3 O3 O4 O6 O7 L1 L2 L4	Mancanza verifica periodica vulnerabilità	Alto (90)

O13 - Attività di office automation ospedaliera

		MISURE DI SICUREZZA	VULNERABILITA'	Rischio (Effetti x Probabilita')
Minacce	**M1**	F1 F3 F6	---	---
	M2	F3	---	---
	M3	F6 F11	Mancanza di parti spare e di contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---
	M5	L5		Medio (30)
	M6	L1 L2 L4 O4 O6 O9 O10	Mancanza di Backup centralizzato, Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6		Medio (30)
	M8	F1 F3 O3 O4 O6 O7 L1 L2 L4	Mancanza di AntiPest, verifica periodica vulnerabilità	Alto (90)

O14 - Gestione dei flussi informativi ospedalieri obbligatori con la regione e i ministeri

		MISURE DI SICUREZZA	VULNERABILITA'	Rischio (Effetti x Probabilita')
Minacce	**M1**	F1 F3 F6	---	---
	M2	F3	---	---
	M3	F6 F11	Scadenza contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---
	M5	L5	Mancanza di aggiornamenti	Medio (30)
	M6	L1 L2 L4 O4 O6 O9 O10	Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6	---	Basso (10)
	M8	F1 F3 F6 O3 O4 O6 O7 L1 L2 L3 L4	---	---

O15 - Gestione Centro Trasfusionale

		MISURE DI SICUREZZA	VULNERABILITA'	Rischio (Effetti x Probabilita')
Minacce	**M1**	F1 F3 F6	---	---
	M2	F3	---	---
	M3	F6 F11	Scadenza contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---
	M5	L5	Mancanza di aggiornamenti	Medio (30)
	M6	L1 L2 L4 O4 O6 O9 O10	Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6	---	Basso (10)
	M8	F1 F3 F6 O3 O4 O6 O7 L1 L2 L3 L4	---	---

A1 - Gestione del personale

	MISURE DI SICUREZZA	VULNERABILITA'	Rischio (Effetti x Probabilita')

Minacce	**M1**	F1 F3 F6 F10 F11	---	---
	M2	F3	---	---
	M3	F6 F11	Scadenza contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---
	M5	L5		Medio (30)
	M6	L1 L2 L4 O4 O6 O9 O10	Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6	---	Basso (10)
	M8	F1 F3 F6 O3 O4 O6 O7 L1 L2 L3 L4	---	---

A2 - Gestione logistica

		MISURE DI SICUREZZA	**VULNERABILITA'**	**Rischio (Effetti x Probabilita')**
Minacce	**M1**	F1 F3 F6 F10 F11	---	---
	M2	F3	---	---
	M3	F6 F11	Scadenza contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---
	M5	L5		Medio (30)
	M6	L1 L2 L4 O4 O6 O9 O10	Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6	---	Basso (10)
	M8	F1 F3 F6 O3 O4 O6 O7 L1 L2 L3 L4	---	---

A3 - Controllo di gestione e supporto decisionale alla direzione aziendale

		MISURE DI SICUREZZA	**VULNERABILITA'**	**Rischio (Effetti x Probabilita')**
Minacce	**M1**	F1 F3 F6	---	---
	M2	F3	---	---
	M3	F6 F11	Scadenza contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---
	M5	L5		Medio (30)
	M6	L1 L2 L4 O4 O6 O9 O10	Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6	---	Basso (10)
	M8	F1 F3 F6 O3 O4 O6 O7 L1 L2 L3 L4	---	---

A4 - Gestione contabile

		MISURE DI SICUREZZA	**VULNERABILITA'**	**Rischio (Effetti x Probabilita')**
Mina	**M1**	F1 F3 F6 F10 F11	---	---
	M2	F3	---	---
	M3	F6 F11	Scadenza contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---

	M5	L5		Medio (30)
	M6	L1 L2 L4 O4 O6 O9 O10	Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6	---	Basso (10)
	M8	F1 F3 F6 O3 O4 O6 O7 L1 L2 L3 L4	---	---

A6 - Gestione inventario aziendale

		MISURE DI SICUREZZA	**VULNERABILITA'**	**Rischio (Effetti x Probabilita')**
Minacce	**M1**	F1 F3 F6 F10 F11	---	---
	M2	F3	---	---
	M3	F6 F11	Scadenza contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---
	M5	L5		Medio (30)
	M6	L1 L2 L4 O4 O6 O9 O10	Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6	---	Basso (10)
	M8	F1 F3 F6 O3 O4 O6 O7 L1 L2 L3 L4	---	---

A7 - Gestione protocollo

		MISURE DI SICUREZZA	**VULNERABILITA'**	**Rischio (Effetti x Probabilita')**
Minacce	**M1**	F1 F3 F6	---	---
	M2	F3	---	---
	M3	F6 F11	Scadenza contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---
	M5	L5		Medio (30)
	M6	L1 L2 L4 O4 O6 O9 O10	Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6		Medio (30)
	M8	F1 F3 O3 O4 O6 O7 L1 L2 L4		Alto (90)

A8 - Gestione delibere

		MISURE DI SICUREZZA	**VULNERABILITA'**	**Rischio (Effetti x Probabilita')**
Minacce	**M1**	F1 F3 F6	---	---
	M2	F3	---	---
	M3	F6 F11	Scadenza contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---
	M5	L5		Medio (30)
	M6	L1 L2 L4 O4 O6 O9 O10	Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6		Medio (30)

	M8	F1 F3 O3 O4 O6 O7 L1 L2 L4		Alto (90)

A9 - Gestione casse

		MISURE DI SICUREZZA	**VULNERABILITA'**	**Rischio (Effetti x Probabilita')**
Minacce	**M1**	F1 F3 F6	---	---
	M2	F3	---	---
	M3	F6 F11	Scadenza contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---
	M5	L5		Medio (30)
	M6	L1 L2 L4 O4 O6 O9 O10	Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6		Alto(99)
	M8	F1 F3 F6 O3 O4 O6 O7 L1 L2 L3 L4		Alto (90)

A11 - Gestione Ufficio Affari Legali

		MISURE DI SICUREZZA	**VULNERABILITA'**	**Rischio (Effetti x Probabilita')**
Minacce	**M1**	F1 F3 F6	---	---
	M2	F3	---	---
	M3	F6 F11	Mancanza di parti spare e di contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---
	M5	L5		Medio (30)
	M6	L1 L2 L4 O4 O6 O9 O10	Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6		Medio (30)
	M8	F1 F3 O3 O4 O6 O7 L1 L2 L4		Alto (90)

T1 - Network Management e monitoraggio della rete

		MISURE DI SICUREZZA	**VULNERABILITA'**	**Rischio (Effetti x Probabilita')**
Minacce	**M1**	F1 F3 F6	---	---
	M2	F3	---	---
	M3	F6 F11	Mancanza di parti spare e di contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---
	M5	L5	Mancanza di aggiornamenti	Alto (70)
	M6	L1 L2 L4 O4 O6 O9 O10	Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6	---	---
	M8	F1 F3 O3 O4 O6 O7 L1 L2 L4	Mancanza di un software di Inventory Management.	Medio (50)

T2 - Security Management

		MISURE DI SICUREZZA	VULNERABILITA'	Rischio (Effetti x Probabilita')
Minacce	**M1**	F1 F3 F6	---	---
	M2	F3	---	---
	M3	F6 F11	Mancanza di parti spare e di contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---
	M5	L5	Mancanza di aggiornamenti	Medio (30)
	M6	L1 L2 L4 O4 O6 O9 O10	Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6		Basso (10)
	M8	F1 F3 O3 O4 O6 O7 L1 L2 L4	Mancanza di aggiornamenti di prodotto e di release, Mancanza di ridondanza e di risorse adeguate (memoria, disco, etc.)	Alto (90)

T5 - Gestione degli elenchi telefonici aziendali

		MISURE DI SICUREZZA	VULNERABILITA'	Rischio (Effetti x Probabilita')
Minacce	**M1**	F1 F3 F6	---	---
	M2	F3	---	---
	M3	F6 F11	Mancanza di parti spare e di contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---
	M5	L5		Medio (30)
	M6	L1 L2 L4 O4 O6 O9 O10	Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6	Mancanza di controlli periodici	Medio (30)
	M8	F1 F3 O3 O4 O6 O7 L1 L2 L4		Alto (90)

T6 - Gestione dell'accesso ad INTERNET ed INTRANET per servizi di connettività

		MISURE DI SICUREZZA	VULNERABILITA'	Rischio (Effetti x Probabilita')
Minacce	**M1**	F1 F3 F6	---	---
	M2	F3	---	---
	M3	F6 F11	Mancanza di parti spare e di contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---
	M5	L5		Alto (70)
	M6	L1 L2 L4 O4 O6 O9 O10	Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6	---	---
	M8	F1 F3 O3 O4 O6 O7 L1 L2 L4		Alto (95)

T7 - Gestione dell'autorizzazione e dell'accreditamento delle strutture sanitarie

		MISURE DI SICUREZZA	VULNERABILITA'	Rischio (Effetti x Probabilita')
Minacce	**M1**	F1 F3 F6	---	---
	M2	F3	---	---
	M3	F6 F11	Mancanza di parti spare e di contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---
	M5	L5		Medio (30)
	M6	L1 L2 L4 O4 O6 O9 O10	Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6	Mancanza di controlli periodici	Medio (30)
	M8	F1 F3 O3 O4 O6 O7 L1 L2 L4		Alto (90)

S1 - Gestione del Servizio Attività Tecniche

		MISURE DI SICUREZZA	VULNERABILITA'	Rischio (Effetti x Probabilita')
Minacce	**M1**	F1 F3 F6	---	---
	M2	F3	---	---
	M3	F6 F11	Scadenza contratti di manutenzione HW	Alto (60)
	M4	F1 F3 O6	---	---
	M5	L5		Medio (30)
	M6	L1 L2 L4 O4 O6 O9 O10	Formazione sui problemi di Sicurezza	Alto (90)
	M7	L3 O6		Medio (30)
	M8	F1 F3 O3 O4 O6 O7 L1 L2 L4		Alto (90)

7 Misure adottate per garantire l'integrità e la disponibilità dei dati

A fronte dell'analisi esposta nel capitolo precedente, verranno adesso riportate le misure adottate al fine di ridurre a livelli accettabili i rischi di cui si è resa evidenza.

1. Aggiornamento del firewall: installazione di un server dedicato e dotato di alimentatori ridondanti e disco di sistema ridondato in configurazione RAID1 (shadow copy). Questa operazione consente l'installazione della versione aggiornata delle componenti del firewall: Kernel, SPI firewall (Netfilter), sottosistema IDS, sistema di analisi dei log, etc. La presenza di una macchina gemella in configurazione hardware analoga alla primaria consente le operazioni di ripristino della funzionalità del Firewall a fronte di una situazione disastrosa di perdita del sistema.

2. Installazione di un MAIL Relay server che isola il server di posta principale da Internet, in modo da evitare che il server con le caselle di posta elettronica degli utenti sia direttamente esposto alle attività degli hackers di Internet. Tale Mail Relay server è dotato di filtri antispam e da un antivirus con motore diverso dall'antivirus in esecuzione sui PC della rete interna. Questa particolarità offre uno scudo ancora più efficace alla protezione dalle infezioni che si trasmettono nei messaggi di posta elettronica.

3. Rimozione delle applicazioni e/o dei servizi non necessari da tutti i server.

4. Acquisizione di una cassaforte ignifuga per la conservazione dei backup.

5. Configurazione su tutti i PC interni dell'aggiornamento delle componenti, tramite SUS server che si collega al sito Microsoft e distribuisca poi le hotfix, Service Packs, etc.

6. Sistema di archiviazione centralizzata dei backup aziendali di tipo NAS – Cisco Strorage situato in luogo protetto ad accesso limitato e diverso dal luogo dove risiedono i dati.

7. Sistema di monitoraggio e controllo della rete in grado di generare allarmi tramite segnalazione su console grafica, invio di messaggi di posta elettronica e/o SMS nel caso un servizio critico ai processi aziendali non sia raggiungibile e/o abbia dei malfunzionamenti per mancanza di risorse, errata configurazione, etc.

8. Acquisizione di apparati di rete "spare" da utilizzare come componenti sostitutive in caso di guasto di apparati attivi. Tale considerazione vale soprattutto per gli apparati di dorsale, data la loro criticità.

9. Acquisizione di un sistema di System Rescue, in grado di ripristinare la configurazione del disco di sistema del Firewall, del Mail Relay, dell'Antivirus Server e dei server di Database a fronte di errori umani od eventuali compromissioni dall'esterno. Tale soluzione dovrebbe essere basata su un software di backup in grado di creare l'immagine fisica del disco, delle sue partizioni (primarie e/o estese), del Master Boot Record e della linked-list delle partioni e da un'unità di memorizzazione esterna (tape e/o USB disk).

10. Archiviazione automatica centralizzata dei log di accesso ai sistemi informatici degli utenti amministratore e non, con produzione di codice di controllo SHA1, a garanzia dell'immodificabilità, su DVD archiviati in cassaforte e/o unità NAS Cisco Storage. L'archiviazione automatica dei log avviene con cadenza settimanale.

8 Misure da adottare per migliorare i livelli di sicurezza e riservatezza delle informazioni

A fronte dell'analisi esposta nel capitolo precedente, verranno adesso riportate le misure che questa ARNAS si ripropone di adottare al fine di ridurre i rischi di cui si è resa evidenza.

1. Installazione del sistema di Inventory management ed Integrity check, Tivoli, in grado di effettuare un polling periodico di tutte le postazioni di lavoro e dei server dell'Azienda, e tale da consentire l'individuazione della installazione di software arbitrari non licenziati e/o scaricati in modo fraudolento e senza la consapevolezza dell'utente durante le normali operazioni di navigazione su Internet e/o di lettura della posta.

2. Protezione del locale CED 2 con impianto di video sorveglianza, implementazione dell'impianto dall'allarme con rilevatori di temperatura, allagamento ed incendio. Protezione del locale CED 3 con impianto di video sorveglianza, e nuovo impianto dall'allarme con rilevatori volumetrici, di temperatura, allagamento ed incendio.

9 Criteri e modalità per il ripristino dei dati

In caso di necessità, deve essere necessario ripristinare nel più breve tempo possibile i servizi che trattano dati personali, siano essi dati sensibili che dati da cui dipende la salvaguardia delle vite umane.

In generale, le tecnologie a cui si può ricorrere per far fronte all'ipotesi della perdita di un servizio critico, con la conseguente indisponibilità dei dati da esso trattati, sono riassumibili nella lista seguente:

1. Ridondanza
2. Backup
3. Contratti di manutenzione
4. Parti di ricambio
5. Gestione degli incidenti

Il server principale, da cui dipende la maggioranza dei processi di trattamento dei dati, è costituito da un cluster server geografico in configurazione di tipo disaster tolerant con nodo gemello ubicato in luogo diverso. Il primo nodo è situato presso i locali del CED al primo piano del padiglione amministrazione, il secondo nodo è posto presso il locale CED al piano terra del padiglione della Chirurgia Toracica.

Anche la rete aziendale è ampiamente ridondata, almeno nelle componenti di dorsale. Il sistema di rete ripristina automaticamente i percorsi di dorsale a fronte di una singola failure.

L'adozione delle misure di ulteriore protezione discusse nel precedente capitolo, consentirà di definire una politica e una serie di procedure operative per il ripristino dei dati in casi eccezionali di compromissione e perdita completa dei sistemi o di parziale indisponibilità delle risorse.

10 Politiche di sicurezza e gestione del rischio

10.1 Obiettivi della politica di sicurezza della azienda

Gli obiettivi di sicurezza che l'azienda si pone con la redazione del seguente piano e con l'attuazione delle misure di sicurezza previste sono:

1. per tutti i dati assoggettati al Decreto Legislativo 196 del 2003, dare attuazione a quanto previsto dall'art. 31 laddove dice che "1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta."
1. Dare attuazione a quanto previsto dall'allegato B del D.L. 196/2003
2. dare attuazione a misure di sicurezza ulteriori - rispetto a quelle previste dal D.L. 196/2003 - che l'azienda ritenga opportune e necessarie nell'ottica del perseguimento degli obiettivi istituzionalmente attribuiti.
3. ridurre a livelli ritenuti accettabili i principali rischi di sicurezza a cui il sistema informativo aziendale è sottoposto;
4. mantenere, compatibilmente con i vincoli di sicurezza sopra enunciati, il massimo livello di usabilità del sistema.

Misure per il perseguimento degli obiettivi di sicurezza individuati

Si ritiene che gli obiettivi di sicurezza siano raggiungibili mediante la predisposizione delle seguenti misure:

- nomina dei responsabili dei trattamenti e degli incaricati dei trattamenti;
- attuazione delle misure di tutela fisica degli apparati;
- attuazione delle misure di sicurezza logica degli apparati;
- definizione delle procedure di continuità ed emergenza;
- definizione delle misure di recupero da disastro;
- definizione di regole di buon uso del sistema informativo aziendale;
- attuazione delle misure di contenimento dei virus informatici;
- attuazione delle misure organizzative e tecniche per la gestione dei documenti informatici;
- attuazione delle misure di informazione e formazione del personale aziendale sugli aspetti di sicurezza informatica;
- misure di sicurezza relative alla salvaguardia delle informazioni detenute su supporto cartaceo.

10.2 Nomina dei responsabili dei trattamenti e degli incaricati del trattamento

10.2.1 NOMINA DEI RESPONSABILI

L'art. 4 del D.L. 196/2003 definisce

f) "**titolare**", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

g) "**responsabile**", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

h) "**incaricati**", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

i) "**interessato**", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

Al titolare e ai responsabili compete la definizione del profilo di sicurezza del sistema informativo aziendale e la messa in atto delle idonee misure di attuazione.

10.2.2 NOMINA DEGLI INCARICATI DEL TRATTAMENTO

Secondo quanto prescritto dall'allegato B del D.L. 196/2003
12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
14. Periodicamente, e comunque almeno annualmente**,** è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Allo scopo di dare attuazione a quanto sopra richiamato occorre che **i responsabili dei trattamenti** - per tutti quei trattamenti per i quali un responsabile sia stato individuato - o **il titolare** - per tutti quei trattamenti per i quali un responsabile non sia stato nominato - diano comunicazione scritta all'U.O. Sistemi Informatici e Telecomunicazioni della avvenuta assegnazione di autorizzazioni di accesso, affinché questi possano attuare le dovute configurazioni tecniche sui sistemi, tali da dare attuazione e cogenza alle dette disposizioni.

Allo scopo rendere possibile ciò:

- si predispone un elenco delle funzionalità assegnabili suddivise per ambito applicativo;
- si individua un modulo così detto di CONCESSIONE/REVOCA/MODIFICA abilitazioni applicative[3] che i responsabili utilizzeranno per le comunicazioni del caso all**'** U.O. Sistemi Informatici e Telecomunicazioni. Sarà compito dell'U.O. Sistemi Informatici e Telecomunicazioni conservare con la dovuta cura tali dichiarazioni. In ogni momento dovrà essere possibile dimostrare la corrispondenza fra le abilitazioni applicative realmente concesse e le autorizzazioni al trattamento conservate in detto archivio.

Almeno una volta all'anno dovrà essere formalizzato un verbale in cui il responsabile del trattamento attesti la sussistenza delle condizioni che determinano la concessione delle abilitazioni applicative vigenti. A tale scopo l'U.O. Sistemi Informatici e Telecomunicazioni dovrà produrre l'elenco aggiornato delle abilitazioni applicative assegnate e vigenti che i responsabili del trattamento certificheranno come corrispondenti alle necessità operative delle rispettive mansioni e minime a tal fine.

Gli elenchi delle richieste di abilitazioni e le vigenti abilitazioni applicative potranno essere comunque sempre confrontati, dagli aventi diritto, rivolgendosi all'U.O. Sistemi Informatici e Telecomunicazioni c/o Staff della Direzione Aziendale.

Per quanto riguarda l'autorizzazione dei dipendenti alla firma di documenti informatici, si veda la Sezione relativa ai documenti informatici.

10.3 Tutela fisica degli apparati

Al fine di predisporre le adeguate misure di tutela fisica degli apparati è necessario poter disporre degli inventari delle attrezzature.
Si dispone pertanto la compilazione e l'aggiornamento - ogni volta che si renda necessario - dei seguenti elenchi:

- elenco dei server - apparati di elaborazione multiutente - e loro rispettiva collocazione: **riportato in allegato T-6.2-1 - Elenco server**;
- elenco degli apparati attivi di rete e loro rispettiva collocazione: **riportato in allegato T-6.2-2 - Elenco apparati attivi di rete**;

10.3.1 COLLOCAZIONE DEI SERVER E DEGLI APPARATI DI RETE

Tutti gli apparati di categoria server - apparti di elaborazione multiutente - dovranno essere collocati presso i locali della U.O. Sistemi Informatici e Telecomunicazioni. I locali soddisfano i seguenti requisiti:

locali chiusi ad accesso controllato: l'accesso ai locali nei quali sono ospitati i sistemi di elaborazione o i sistemi di comunicazione è interdetto a chiunque, fatta eccezione per il personale autorizzato. Se eventualmente si rendesse necessario l'accesso a detti locali da parte di personale non autorizzato - per es. da parte di tecnici della manutenzione di ditte fornitrici, ecc… -, i visitatori andranno opportunamente identificati e accompagnati

[3] Si veda a questo proposito l'appendice "Modulistica"

durante tutta la loro permanenza in detti locali da personale autorizzato. Deroghe a tale regola potranno essere concesse solo dietro precisa motivazione e andranno comunque segnalate ai responsabili della gestione dei server.
locali dotati di opportuno condizionamento: i locali posseggono condizioni idonee di microclima - in termini di temperatura, polverosità, umidità;
locali dotati di impianto antincendio ed antiallagamento: i locali sono dotati di un adeguato impianto antincendio e antiallagamento collegati all'impianto di allarme;

Tutti gli apparati attivi di rete andranno collocati in armadi chiusi a chiave che garantiscano le seguenti caratteristiche di microclima:

- valori corretti di temperatura;
- valori corretti di polverosità;
- valori corretti di umidità.

Per quegli armadi che risultino essere particolarmente sollecitati dalle prove di carico del gruppo ettrogeno sono previsti opportuni stabilizzatori in grado di limitare le sovratensioni generate dalla partenza del gruppo elettrogeno.

10.3.2 CARATTERISTICHE HARDWARE DEI SERVER

Tutti i sistemi di elaborazione di categoria server in uso in azienda - non importa se di proprietà, o a qualsiasi altro titolo detenuti e di cui si abbia la responsabilità - devono avere almeno le seguenti caratteristiche: per quanto possibile andranno privilegiate configurazioni hardware dei server ridondanti che garantiscano la continuità di servizio - per es. doppio alimentatore in configurazione ridondante, configurazione di server in cluster con funzionalità di "Mutual Take Over" o similari, doppia scheda di rete al fine di creare macchine "Multi Homed" in grado di poter resistere a guasti singoli sulla scheda di rete, ecc…-.

- tutte le aree di memoria su disco magnetico destinate a contenere i dati dovranno essere tutelate da misure di ridondanza - con tecniche almeno di mirroring, preferibilmente RAID -; ogni server dovrà possedere un dispositivo di backup di adeguate dimensioni e velocità - unità di backup -, nel caso l'azienda disponga di sistemi di backup centralizzato, tale informazione andrà dettagliata nella scheda che accompagna i server aziendali
- ogni server dovrà riportare affissa una scheda individuale nella quale dovrà essere obbligatoriamente indicato dove è possibile trovare copia delle informazioni per l'accesso - USERID e PASSWORD del super utente - per manovre di emergenza sull'elaboratore. Tali informazioni andranno conservate in luogo presidiato e sotto chiave e dovranno essere conservate in busta sigillata e firmata dal locale responsabile della gestione del server. Andrà tenuto registro di chi ha accesso a tali informazioni e andrà indicato succintamente il motivo.

10.3.3 POLITICHE DI GESTIONE DEI BACKUP

Al fine di tutelare adeguatamente i dati gestiti nei vari sistemi di elaborazione è necessario predisporre un adeguato piano di backup.
Di seguito vengono indicate le politiche di backup e ripristino per i vari server e le varie banche dati Aziendali:

NomeServer	TipoServer	Informazioni	BANCHE DATI	Politiche di ripristino	Politiche di backup	Software di backup	Archiviazione supporti
ARNASCLU1	SERVER VIRTUALE	DOMINIO ARNASCIVICO.LOCAL DNS DHCP		Archiviazione annuale dell'immagine della macchina virtuale DVD ROM	Giornaliero su disco	Script batch	Cassaforte ignifuga sita presso CED 1 e/o sistema NAS Cisco Storage
ARNASCLU2	SERVER VIRTUALE	DOMINIO ARNASCIVICO.LOCAL DNS SUS Server		Archiviazione annuale dell'immagine della macchina virtuale DVD ROM	Giornaliero su disco	Script batch	Cassaforte ignifuga sita presso CED 1 e/o sistema NAS Cisco Storage
CLUSTERGEO NODO 1	IBM XSERIES 445	SERVER ORACLE IN CLUSTER GENOGRAFICO CON ClusterGeoNodo2	DB SELFIN – METAFORA-EMONET	Server ridondato in tutte	Esport della bancadati ORACLE	Script batch	Cassaforte ignifuga sita presso CED 1

			DBMS ORACLE RAC 10		DB una volte al giorno e esport degli archive log da tre a sei volte al giorno		e/o sistema NAS Cisco Storage
CLUSTERGEO NODO 2	IBM XSERIES 445	SERVER ORACLE IN CLUSTER GENOGRAFICO CON ClusterGeoNodo1	DB SELFIN – METAFORA-EMONET DBMS ORACLE RAC 10		Esport della bancadati ORACLE DB una volta al giorno e esport degli archive log da tre a sei volte al giorno	Script batch	Cassaforte ignifuga sita presso CED 1 e/o sistema NAS Cisco Storage
DELIBERA	SERVER	server delibere	DB DELIBERE	Archiviazione annuale della configurazione della macchina su DVD ROM	Giornaliero su disco	Script batch	Cassaforte ignifuga sita presso CED 1 e/o sistema NAS Cisco Storage
DOMINONET	IBM xseries 345	Protocollo Aziendale e Backup domino WEB	DB PROTOCOLLO	Archiviazione annuale della configurazione della macchina su DVD ROM	Giornaliero su disco	Script batch	Cassaforte ignifuga sita presso CED 1 e/o sistema NAS Cisco Storage
DOMINOWEB	IBM xseries 345	Portale dominoweb backup protocollo dominonet	DB PROTOCOLLO	Archiviazione annuale della configurazione della macchina su DVD ROM	Giornaliero su disco	Script batch	Cassaforte ignifuga sita presso CED 1 e/o sistema NAS Cisco Storage
DONATELLO	IBM xseries 360	DOMINIO ARNASCIVICO.LOCAL DNS DHCP FILE SHARING	DB PLASTICA - DB CONTROLLO DI GESTIONE	Archiviazione annuale della configurazione della macchina su DVD ROM	Giornaliero su disco	Script batch	Cassaforte ignifuga sita presso CED 1 e/o sistema NAS Cisco Storage
RAFFAELLO	IBM xseries 360	PRIMARY CONTROLLER DOMINIO ARNASCIVICO.LOCAL DNS FILE SHARING	DB PLASTICA - DB CONTROLLO DI GESTIONE	Archiviazione annuale della configurazione della macchina su DVD ROM	Giornaliero su disco	Script batch	Cassaforte ignifuga sita presso CED 1 e/o sistema NAS Cisco Storage
ESX1	HPML570G3	SERVER CONSOLIDATION VMWARE ESX IN CLUSTER CON ESX2		Archiviazione annuale della configurazione della macchina su DVD ROM			Cassaforte ignifuga sita presso CED 1 e/o sistema NAS Cisco Storage
ESX2	HPML570G3	SERVER CONSOLIDATION VMWARE ESX IN CLUSTER CON ESX1		Archiviazione annuale della configurazione della macchina su DVD ROM			Cassaforte ignifuga sita presso CED 1 e/o sistema NAS Cisco Storage
FIREWAL PRIMARIO	IBM xseries 345	FIREWALL PRIMARIO		Archiviazione annuale della configurazione della macchina su DVD ROM			Cassaforte ignifuga sita presso CED 1 e/o sistema NAS Cisco Storage
FIREWALL BACKUP	IBM xseries 345	FIREWALL SECONDARIO BACKUP		Archiviazione annuale della configurazione della macchina su DVD ROM			Cassaforte ignifuga sita presso CED 1 e/o sistema NAS Cisco Storage

IT	SERVER	Server intranet			Giornaliero su disco	Script batch	Cassaforte ignifuga sita presso CED 1 e/o sistema NAS Cisco Storage
LOCALISA	HP PROLIANT 320	PROXY SERVER MS ISA VPN SERVER			Giornaliero su disco	Script batch	Cassaforte ignifuga sita presso CED 1 e/o sistema NAS Cisco Storage
NODO_CIVICO	HP DL380 G3	server adibito al laboratorio analisi hp DL380	SW TEMPO/ CONCERTO METAFORA	Archiviazione annuale della configurazione della macchina su DVD ROM			Cassaforte ignifuga sita presso CED 1 e/o sistema NAS Cisco Storage
NODO_CIVICO 2	HP DL380 G3	Server HP laboratorio Analisi DL380	SW TEMPO/ CONCERTO METAFORA	Archiviazione annuale della configurazione della macchina su DVD ROM			Cassaforte ignifuga sita presso CED 1 e/o sistema NAS Cisco Storage
POSTA1	SERVER VIRTUALE	SERVER WEB E POSTA ELETTRONICA OSPEDALECIVICOPA.ORG IN CLUSTER CON POSTA2		Archiviazione annuale dell'immagine della macchina virtuale DVD ROM	Giornaliero su disco	Script batch	Cassaforte ignifuga sita presso CED 1 e/o sistema NAS Cisco Storage
POSTA2	SERVER VIRTUALE	SERVER WEB E POSTA ELETTRONICA OSPEDALECIVICOPA.ORG IN CLUSTER CON POSTA1		Archiviazione annuale dell'immagine della macchina virtuale DVD ROM	Giornaliero su disco	Script batch	Cassaforte ignifuga sita presso CED 1 e/o sistema NAS Cisco Storage
PROXY1	HP PROL. DL140	PROXY SERVER WINGATE ANTIVIRUS			Giornaliero su disco	Script batch	Cassaforte ignifuga sita presso CED 1 e/o sistema NAS Cisco Storage
PROXY2	HP PROL. DL140	Proxy server di backup a Proxy1			Giornaliero su disco	Script batch	Cassaforte ignifuga sita presso CED 1 e/o sistema NAS Cisco Storage
REMAILER	IBM XSERIES 346	SERVER REMAILER REVERSE PROXY POSTA ELETTRONICA - ANTISPAMMINIG		Archiviazione annuale della configurazione della macchina su DVD ROM			Cassaforte ignifuga sita presso CED 1 e/o sistema NAS Cisco Storage
SUSERVER	SERVER	WSUS Server Windows 2003 Update Server X SERVERFARM		Archiviazione annuale della configurazione della macchina su DVD ROM			Cassaforte ignifuga sita presso CED 1 e/o sistema NAS Cisco Storage
SYMANTECP	SERVER VIRTUALE	SERVER ANTIVIRUS DISTRIBUZIONE VIRUS DEFINITION AI CLIENT		Archiviazione annuale dell'immagine della macchina virtuale DVD ROM			Cassaforte ignifuga sita presso CED 1 e/o sistema NAS Cisco Storage

10.3.4 POLITICHE DI GESTIONE DEI GUASTI

Per tutti i trattamenti che occorre tutelare da **minacce alla disponibilità - si veda a questo proposito l'elenco T-5.2-1** - si adottano le seguenti misure.

Trattamenti per i quali il guasto bloccante è altamente probabile:

1. Gestione Ufficio Affari Legali (comprensivo della gestione di ingiunzioni, pignoramenti, transazioni, citazioni, diffide, ricorsi, ordinanze, gestione aspetti assicurativi, tenuta repertorio contratti, consulenza interna agli altri servizi)

Trattamenti per i quali il guasto bloccante è mediamente probabile:

- Gestione dell'accesso ad INTERNET ed INTRANET per servizi di connettività: mail, browsing, FTP, Telnet, ecc…
- Help Desk Applicativo
- Gestione degli elenchi telefonici aziendali
- Gestione protocollo (protocollazione dei documenti amministrativi - se del caso integrato con il sistema di gestione del workflow delle pratiche amministrative -);

Trattamenti per i quali il guasto bloccante è poco probabile:

1. Gestione dei flussi informativi ospedalieri obblligatori con la regione e i ministeri: gestione della mobilità, registri sanitari, CEDAP, ecc…
2. Gestione anagrafica dei contatti con la struttura ospedaliera;
3. Gestione ricoveri (intesa come gestione amministrativa del ricovero e parte sanitaria di ricovero, esclusa gestione cartella clinica);
4. Gestione cartella clinica e scheda nosologica;
5. Gestione Pronto Soccorso
6. Gestione sale operatorie (registro di sala operatoria e programmazione delle sale);
7. Gestione amministrativa delle grandi diagnostiche (Radiologia, laboratorio analisi, anatomia patologica, medicina nucleare, cardiologia, ecc…): comprendente almeno la schedulazione delle prestazioni in collegamento con il CUP, la gestione dei referti, la registrazione delle prestazioni erogate;
8. Sistema di gestione della documentazione iconografica e magazzino dei dati - PACS - : sottosistema di immagazzinamento della documentazione iconografica prodotta dalle diagnostiche digitali o digitalizzate; lavora in stretta connessione con i sottosistemi di gestione amministrativa delle grandi diagnostiche;
9. Gestione Centro Unico di Prenotazione - CUP - :sistema di programmazione interno delle attività, come ad esempio le consulenze interne, indagini diagnostiche per ricoverati, ecc…;
10. Gestione della libera professione medica
11. Gestione del personale (comprensivo di trattamento economico, rilevazione della presenza assenza, gestione concorsi, gestione stato giuridico matricolare, pianta organica, aspetti contributivi e previdenziali, gestione della formazione del personale comprensiva degli aspetti di accreditamento dei corsi);
12. Gestione Call Center e URP - ufficio rapporti con il pubblico - Ospedaliero;
13. Gestione logistica (comprensivo di gestione richieste dal reparto, gestione ordini, gestione magazzini, gestione fatturazione passiva);
14. Gestione contabile (comprensiva di contabilità generale, gestione cespiti, fatturazione attiva, recupero crediti e flussi per la messa a ruolo dei mandati di pagamento);
15. Gestione casse
16. Gestione farmacia ospedaliera (comprensivo di gestione richieste da parte dei reparti, gestione ordini ai fornitori, gestione magazzini farmaceutici e gestione della reportistica per il controllo direzionale e di consumo in reparto)
17. Attività di office automation ospedaliera: produzione di documenti non ascrivibili in maniera diretta ai trattamenti ospedalieri sopra elencati;
18. Rilevazione della attività ospedaliera
19. Trattamenti operati dalla Direzione di stabilimento e/o di Presidio nell'ambito dei compiti istituzionali delle direzioni sanitarie (comprensive almeno degli aspetti di gestione degli espianti, riscontri autoptici, comunicazioni alla autorità giudiziaria, ecc...)
20. Attività di office automation di tipo amministrativo: produzione di documenti non ascrivibili in maniera diretta ai trattamenti amministrativi sopra elencati;
21. Gestione del Servizio Attività Tecniche (eventualmente integrato con la gestione cespiti e la gestione contabile per quanto attiene al ciclo passivo);
22. Gestione inventario aziendale (eventualmente integrato con la gestione tecnica dei servizi di supporto);
23. Gestione delibere e gestione documentale in genere (comprensiva se del caso di sistema di gestione dell'iter delle pratiche in grado di coadiuvare la gestione in trasparenza delle pratiche amministrative);

24. Gestione inventario delle infrastrutture informatiche e di telecomunicazione (eventualmente integrato con il sottosistema di gestione inventario e gestione cespiti);
25. Gestione dell'autorizzazione e dell'accreditamento delle strutture sanitarie (comprendente almeno la gestione documentale in modalità informatizzata);
26. Controllo di gestione e supporto decisionale alla direzione aziendale (comprensivo di sistema di generazione dinamica della reportistica e del data warehouse dei costi e dei ricavi);
27. Network Management e monitoraggio della rete;
28. Security Management (comprendente almeno la gestione degli utenti e dei profili abilitativi e delle apparecchiature di presidio del confine aziendale tipo Firewall e Access Server);

È responsabile della formulazione di adeguate politiche di gestione dei guasti l'U.O. Sistemi Informatici e Telecomunicazioni. Sono responsabili della attuazione dei passi previsti dalle politiche di gestione dei guasti i vari incaricati di tali mansioni.

10.4 Sicurezza logica

10.4.1 MISURE MINIME DI SICUREZZA

Misure minime di sicurezza relative a trattamenti che vengono messi a disposizione come servizi di elaboratori connessi in rete pubblica:

1. Il trattamento di dati personali è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato. (D.L. 196/2003 Allegato B, punti 1, 2,3 ,4)

Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi. Pertanto si dispone che ogni utente definito, non venga più cancellato, ma disabilitato nel caso cessi di essere in uso, in maniera tale da evitarne il riutilizzo (D.L. 196/2003 Allegato B, punti 6)

La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi. Qualora il sistema operativo dell'elaboratore su cui risiede l'applicativo lo consenta, è abilitato il cambio password, che l'incaricato potrà autonomamente effettuare in un qualsiasi momento successivo al primo accesso, e in ogni altro momento successivo; per quei sistemi operativi per i quali non sia disponibile tale modalità di cambio password, o non sia comunque abilitabile per ragioni tecniche, è individuata una procedura organizzativa opportuna per il cambio password mediante l'ausilio del personale tecnico della U.O. Informatizzazione e Telecomunicazioni (D.L. 196/2003 Allegato B, punti 5);
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia

delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato. (D.L. 196/2003 Allegato B, punti 7,8,9,10)

Sistema di autorizzazione
12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. NOTA BENE: per dettagli al riguardo si veda la Sezione dedicata alla individuazione degli incaricati del trattamento;
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione. (D.L. 196/2003 Allegato B, punti 12, 13, 14)
Altre misure di sicurezza
15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.
NOTA BENE: per dettagli al riguardo si veda la Sezione dedicata alle misure di irrobustimento dei server;
17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.
18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale. (D.L. 196/2003 Allegato B, punti 15, 16, 20, 17, 18)

Il reimpiego dei supporti di memorizzazione è vietato qualora siano serviti per la memorizzazione di dati personali o sensibili si veda a questo proposito la Sezione relativa al buon uso del sistema informativo e di comunicazione. È inoltre genericamente vietato l'utilizzo di supporti di memorizzazione rimovibili per lo scambio di dati sensibili (D.L. 196/2003 Allegato B, punti 21 e 22)

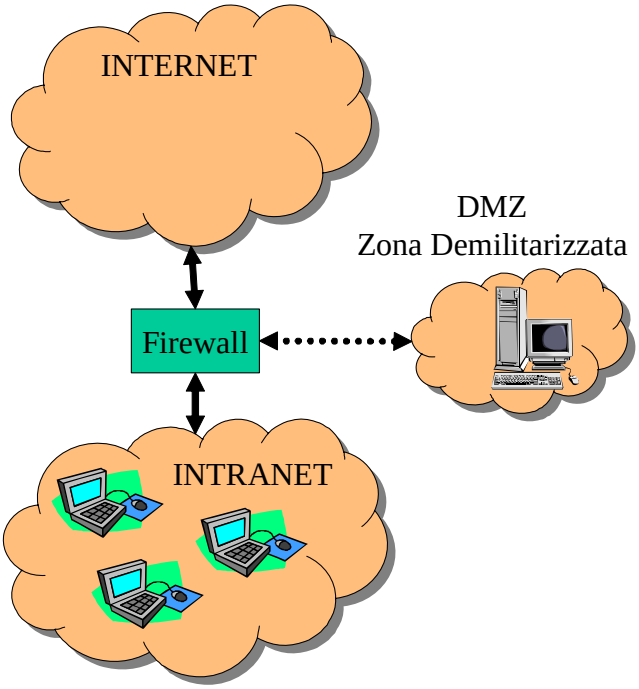
È responsabile della formulazione di opportune politiche di gestione dei sistemi di elaborazione che garantiscano il rispetto delle misure minime di sicurezza - e della attuazione delle misure attuative, per la parte di competenza - l'U.O. Sistemi Informatici e Telecomunicazioni.

10.4.2 MISURE ULTERIORI DI SICUREZZA

10.4.2.1 Architettura di sicurezza

In questa **Sezione** vengono illustrate le misure di sicurezza che esulano da quelle minime - richieste cioè dal **D.L. 196/2003 Allegato B** -. In particolare dall'analisi delle funzionalità maggiormente a rischio - si vedano in particolare gli elenchi **T-5.2-1, T-5.2-2, T-5.2-3, T-5.2-4** - e dall'analisi della localizzazione delle utenze e dei servizi si evince che la totalità delle utenze è collocata entro il confine aziendale e fruisce di servizi applicativi localizzati entro il confine aziendale;

L'architettura che offre il miglior rapporto fra minimizzazione dei i rischi complessivi del sistema e costi di realizzazione e gestione è del tipo seguente:



aggiungendo anche una breve descrizione dei più importanti blocchi funzionali:

- Firewall;
- Internet - con la doppia veste di mezzo di comunicazione per gli utenti aziendali che accedono in VPN e insieme di risorse accedute dai client posti nella intranet aziendale -;
- Intranet - sede della maggior parte dei client aziendale e dei server che erogano la maggior parte delle funzionalità applicative -;
- DMZ - sede di alcuni sistemi che devono essere visibili in internet, ma svolgono anche servizi applicativi aziendali-;

L'architettura individuata si basa sui seguenti criteri:

- avere un confine aziendale ben definito con un solo punto di attraversamento presidiato da un Firewall dispositivi facilmente controllabile, gestibile e monitorabile;
- avere una zona - la DMZ - con caratteristiche di sicurezza intermedia fra l'esterno e l'interno in cui porre tutti quegli elaboratori che pur facendo parte dei server che svolgono servizi applicativi per i client della intranet debbano in qualche modo essere visibili dalla rete internet;
- avere un piano di numerazione di rete interno non pubblico, ma convertito con tecniche NAT - Network Address Translation - per aumentare il livello complessivo di sicurezza;

L'attuazione delle misure tecniche che conducono alla realizzazione di una tale infrastruttura sono di competenza dell'U.O. Sistemi Informatici e Telecomunicazioni così come la successiva gestione di tale infrastruttura.

10.4.3 MISURE DI CONTENIMENTO DEL RISCHIO

Salvaguardia delle funzionalità di sicurezza

Si sceglie innanzitutto di mettere in atto tutte quelle misure che tendono a salvaguardare l'impianto di sicurezza del sistema quindi si adottano le seguenti misure:

- vengono adottate le migliori tecniche di tutela del Firewall che deve essere configurato e gestito da personale professionalmente competente e certificato in materia ;
- si configurano nella maniera più sicura possibile tutti i server che hanno un ruolo nel processo di autenticazione dell'utente, minimizzando il numero di funzionalità in uso su di essi e adottando tutte le opportune tecniche di irrobustimento;
- vengono adottate analoghe tutele anche per i sistemi di elaborazione dedicati al backup dei dati;
- tutte le sessioni di amministrazione di sistema e di concessione/revoca/modifica di abilitazioni applicative che non si svolgano in locale sul server devono essere rese completamente immuni da azioni di

intercettazione sulla rete e di fraudolenta impersonificazione - mediante tecniche opportune di gestione sicura della autenticazione del client e di crittografia di canale -.
- le password di amministrazione, devono avere almeno una lunghezza di 8 caratteri, con possibilità di inserire sia maiuscole che minuscole e segni di punteggiatura, hanno una scadenza imposta massima di 1 mese e non possono essere ripetute.

L'insieme di misure sopra descritte tende a minimizzare le minacce di:
- **disponibilità di servizio - relativamente alle funzionalità di sicurezza -;**
- **intercettazione sulla rete e modifica - relativamente alle funzionalità di sicurezza -;**
- **fraudolenta impersonificazione - relativamente alle funzionalità di sicurezza -;**

Salvaguardia delle funzionalità applicative

Si adottano le seguenti misure di salvaguardia:
- le autenticazioni devono essere effettuate in maniera sicura senza che la password viaggi in chiaro sulla rete - o che in rete viaggino informazioni che possano essere utilizzate per una fraudolenta impersonificazione -;
- si configurano nella maniera più sicura possibile tutti i server che forniscono funzionalità applicative, minimizzando il numero di funzionalità in uso su di essi e adottando tutte le opportune tecniche di irrobustimento;
- vengono adottate le necessarie misure di irrobustimento applicativo;
- le password applicative, devono avere almeno una lunghezza di 6 caratteri, con possibilità di inserire sia maiuscole che minuscole e segni di punteggiatura, hanno una scadenza imposta massima di 6 mesi e non possono essere ripetute.

L'insieme di misure sopra descritte tende a minimizzare le minacce di:
- **disponibilità di servizio - relativamente alle funzionalità applicative -;**
- **fraudolenta impersonificazione - relativamente alle funzionalità applicative -.**

Non vengono sistematicamente gestite - almeno all'interno del confine aziendale - misure tese a prevenire l'intercettazione e la modifica delle comunicazioni applicative considerando tali minacce poco rilevanti.

Invece nel caso di comunicazioni che attraversino il confine aziendale occorre che siano adeguatamente tutelati anche questi aspetti adottando opportune tecniche di crittografia di canale.

L'attuazione delle misure tecniche sopra descritte sono di competenza dell' U.O. Sistemi Informatici e Telecomunicazioni.

10.5 Procedure di continuità ed emergenza

Il guasto nell'ambito di un complesso sistema tecnologico, quale il sistema informatico aziendale, è un evento non deterministicamente prevedibile, ma probabilisticamente certo indipendentemente dal grado di sofisticazione degli accorgimenti tecnici messi in atto per aumentare l'affidabilità dei sistemi e il loro grado di ridondanza, pertanto occorre che i responsabili dei trattamenti di concerto con i servizi tecnici di competenza predispongano piani opportuni di gestione delle situazioni di malfunzionamento dei sistemi informatici al fine di evitare o minimizzare il disservizio arrecato degli utenti.

Il Piano di continuità operativa dei sistemi per l'elaborazione dell'informazione e del sistema di comunicazione (dati e fonia) generale di azienda viene riportato in appendice. Pertanto si rimanda a quelle indicazioni per tutti quei casi in cui il malfunzionamento della infrastruttura tecnologica porti ad un disservizio nella erogazione della attività aziendale.

La predisposizione e la successiva manutenzione dei Piani di Continuità ed Emergenza è di competenza dei responsabili dei trattamenti che si possono avvalere per gli aspetti strettamente tecnici della collaborazione dell' U.O. Sistemi Informatici e Telecomunicazioni.

10.6 Procedure di recupero da disastro

La predisposizione e la successiva manutenzione delle procedure di recupero da disastro è di competenza dei responsabili dei trattamenti e dell' U.O. Sistemi Informatici e Telecomunicazioni che si occuperà degli aspetti strettamente tecnici del recupero dall'evento disastroso.
La politica aziendale per la gestione degli Incidenti di Sicurezza è definita nel documento applicabile "Piano di Gestione degli Incidenti di Sicurezza".

10.7 Regole di buon uso del sistema informatico aziendale

La politica aziendale per il corretto uso dei sistemi informatici è definita nel documento applicabile "Uso accettabile dei Sistemi di Elaborazione Dati".

10.8 Crimine informatico e tutela del diritto d'autore

Allo scopo di formare e informare il personale aziendale al buon uso del sistema informatico e telematico aziendale e al fine di prevenire il crimine informatico si dispone che venga distribuito a tutti gli utenti del sistema il testo commentato della legge n.547 del 23/12/93 relativa al crimine informatico.

Vista la legge 248 del 18/08/2000 relativa alla tutela del diritto d'autore si vietata la riproduzione o la duplicazione con qualsiasi mezzo e a qualsiasi titolo dei programmi informatici e dei manuali a corredo dei programmi, si ricorda infatti che anche i manuali sono coperti dalla legge sul diritto di autore e possono essere riprodotti solo dietro autorizzazione del titolare dei diritti esclusivi. L'U.O. Sistemi Informatici e Telecomunicazioni, qualora tecnicamente possibile deve **predisporre copie di riserva dei programmi dotati di regolare licenza allo scopo di prevenire accidentali perdite dell'originale e quindi danni patrimoniali all'azienda**. Tale copia di riserva potrà essere usata soltanto per ripristinare le funzionalità del programma, quando non sia possibile utilizzare il programma originale.

Qualora l'utente installi sulla propria stazione di lavoro programmi SHAREWARE, copiati da BBS o internet, deve prestare attenzione alla scadenza temporale che l'autore concede come periodo per l'utilizzo gratuito. **Scaduto tale termine il programma dovrà essere rimosso o ne dovrà essere regolarizzata la detenzione**.

10.9 Tutela dei dati memorizzati sulle stazioni di lavoro personale e reimpiego dei supporti di memorizzazione

L'azienda persegue una politica di centralizzazione nella gestione dei dati aziendali, per cui progressivamente le gestioni locali di dati scompariranno sostituite da gestioni centralizzate su server. Fino a che questo processo non sarà stato portato a compimento potranno esistere gestioni locali di dati su stazioni di lavoro personali - personal computer non connessi in rete o connessi in rete, ma con la possibilità di gestire localmente documenti e/o dati - la cui tutela è demandata a all'utente finale. L'effettuazione dei salvataggi con frequenza opportuna - almeno comunque settimanale- su supporti magnetici e la conservazione degli stessi in luogo idoneo - possibilmente sotto chiave e in contenitori ignifughi - è compito del singolo dipendente che usa la stazione nel caso di stazioni di lavoro usate da un solo utilizzatore, da un incaricato opportunamente individuato dal responsabile del trattamento nel caso di stazioni di lavoro condivise.

È vietato l'uso di supporti di memorizzazione removibili per la memorizzazione di dati personali o sensibili. Deroghe a tale regola sono possibili solo nei casi in cui sia possibile dimostrare il corretto uso dei supporti di memorizzazione ai sensi del **D.L. 196/2003 Allegato B, punti 21 e 22**:

1. è possibile il reimpiego del supporto solo nel caso non siano più recuperabili le informazioni precedentemente memorizzate;
2. nel caso non sia garantibile il requisito di cui al punto (1), il supporto removibile dopo l'uso andrà distrutto.

In generale i supporti di memorizzazione - anche non removibili - che contengono dati personali o sensibili, nel caso non possano essere cancellati in maniera da renderne irrecuperabile il contenuto, una volta dimessi - per es. per obsolescenza o per guasto -, dovranno essere distrutti o smaltiti in maniera tale che il contenuto non sia più recuperabile.

10.10 Buon uso della rete di comunicazione

La rete di trasmissione dati e fonia è un prezioso bene aziendale condiviso e pertanto va gestita nel rispetto delle esigenze complessive di azienda. In funzione di ciò viene fatto esplicito e tassativo divieto di connettere in rete stazioni di lavoro se non dietro esplicita e formale autorizzazione della U.O. Sistemi Informatici e Telecomunicazioni. È altresì vietato alterare in qualsiasi modo la configurazione software della stazione di lavoro - o di altri dispositivi direttamente connessi alla rete, dati o fonia - per quanto attiene all'accesso alla rete. È anche fatto divieto di utilizzare in qualsiasi modo la rete aziendale per fini non espressamente autorizzati. In particolare tali divieti si possono tradurre, anche se non esaurire, nelle seguenti esplicite proibizioni:

- divieto di collocamento di documenti contenenti dati personali comunque riservati nelle cartelle condivise in rete (né dotate di password, né sprovviste di password);
- divieto di alterare la configurazione delle configurazioni di rete di stazioni di lavoro e altri dispositivi in rete (stampanti condivise, ecc…), comprendendo in ciò anche il divieto di aggiungere protocolli di rete o servizi in rete (per es. condivisione di stampanti in rete, browsing di risorse di rete, ecc…);
- divieto di monitorare ciò che transita in rete.

È inoltre vietata l'installazione non autorizzata di Modem per linee analogiche o digitali che sfruttino il sistema di comunicazione in fonia per l'accesso a banche dati esterne o interne all'azienda.

È vietata l'installazione di hardware o software di qualsiasi tipo che consenta o faciliti il *by pass* delle misure di presidio del confine aziendale - per es. software di comunicazione che garantiscano accessi che non passino dai Firewall Aziendali o dagli altri accessi autorizzati e presidiati -.

10.11 Doveri connessi alla corretta conservazione delle parole chiave di accesso e dei dispositivi di accesso

L'utente inoltre è tenuto a conservare nella massima segretezza la parola di accesso ai sistemi e qualsiasi altra informazione legata al processo di autenticazione.
Inoltre l'utente è tenuto a scollegarsi dal sistema ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro, o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima (per es. perché impegnato in compiti che richiedono totalmente la sua attenzione). Occorre prestare anche particolare attenzione alle stampe prodotte con sistemi informatizzati: la produzione dei documenti deve essere presidiata o collocata in locali ad accesso controllato.
L'utente è inoltre tenuto a conservare con la massima cura eventuali dispositivi per l'accesso ai sistemi aziendali e ad usarli conformemente alle specifiche indicazioni d'uso. La perdita o danneggiamento degli stessi sarà sanzionata.

È bene porre l'accento sulla necessità che i responsabili delle unità organizzative operino un costante e meticoloso controllo volto ad evitare pratiche che la normativa identifica come veri e propri crimini, ma che nella pratica comune risultano assai diffuse e a vari livelli tollerate.
Ciò risulta tanto più importante se si pensa che senza la collaborazione attiva di tutte le articolazione organizzative aziendali non sarà possibile arginare i costi sempre crescenti indotti da un cattivo uso delle attrezzature informatiche - si pensi a titolo esemplificativo al proliferare dei virus informatici che potrebbe essere arginato adottando semplici regole di controllo delle informazioni provenienti dall'esterno dell'azienda, ecc…-.

Si dispone quindi che i responsabili delle varie macro articolazioni organizzative, di concerto con il Sistema Informativo Aziendale adottino gli atti e le misure necessarie a garantire un adeguato controllo relativamente alle norme di buon uso dei sistemi informatici e di telecomunicazione dell'azienda.

10.12 I virus Informatici - malicious code -

Al fine di prevenire le infezioni virali si adottano le seguenti misure:

1. **si dotano tutte le attrezzature di confine di un adeguato software antivirale e si stabilisce l'aggiornamento delle firme almeno in ragione giornaliera. Le attrezzature da mantenere aggiornate sono riportate nell'allegato T-8-1 - Elenco attrezzature di confine su cui mantenere aggiornato il software antivirale -.**
2. **si dota di software antivirale** - e predispongono adeguati meccanismi per mantenere tale software aggiornato - **ogni client aziendale che abbia una o più delle seguenti caratteristiche**: sia dotato di

collegamenti che attraversano il confine aziendale - per es. collegamenti modem -, sia in qualche modo connesso con l'esterno dell'azienda per via diversa dalla rete aziendale. **Le attrezzature da mantenere aggiornate sono riportate nell'allegato T-8-2 - Elenco client critici su cui mantenere aggiornato il software antivirale -.**

3. **nel caso siano presenti file server all'interno del confine aziendale dotarli di software antivirale per la scansione dei documenti gestiti. Le attrezzature da mantenere aggiornate sono riportate nell'allegato T-8-3 - Elenco dei file server su cui mantenere aggiornato il software antivirale -.**
4. **ogni stazione di lavoro personale dotata di memorie di massa removibili - lettore di floppy disk e similari - che abbia strumenti di produttività personale e che mantenga documenti in locale deve essere dotata di software antivirale**. Nel caso non sia possibile predisporre adeguati meccanismi per mantenere il software antivirale aggiornato sarà cura del consegnatario della stazione di lavoro aggiornare il software almeno in ragione settimanale seguendo l'opportuna procedura tecnica di aggiornamento - si veda a questo proposito l'appendice relativa -.
5. **per quanto possibile si dovranno configurare i profili abilitativi di tutti gli utenti aziendali con privilegi che non consentano l'installazione o l'esecuzione di programmi non autorizzati sia sulle macchine client che sui server**
6. **per quanto organizzativamente possibile ed appropriato, dovranno essere disabilitate sui server le funzionalità di editor e di file transfer**.

Si invitano inoltre gli utenti:

A) alla massima cautela nella gestione dei supporti magnetici e della posta elettronica: in particolare ogni qualvolta un supporto di memorizzazione - dischetto removibile, nastro magnetico, disco magneto-ottico e ogni altro supporto di memorizzazione removibile - sia stato utilizzato su un computer diverso dal proprio - supponendo che il proprio PC sia immune da infezioni - occorrerà verificare l'assenza di virus mediante un programma antivirale aggiornato. Se non vi è l'assoluta certezza che il proprio computer possieda un antivirus aggiornato non sarà possibile utilizzare il supporto di memorizzazione - in quanto potenzialmente infetto -;

B) in generale sarebbe bene conoscere sempre con precisione quale sia la fonte dei dati, ed essere certi che tale fonte sia affidabile e sicura; è preferibile non utilizzare un supporto di memorizzazione removibile di cui non si conosca la fonte;

C) è bene sempre evitare di leggere o utilizzare allegati di messaggi di posta elettronica che non provengano da fonti certe, riconosciute e sicure; nel caso pervenga un messaggio di tale natura procedere immediatamente alla eliminazione. Nel caso si abbia il sospetto che il proprio sistema di elaborazione sia stato infettato avvertire il personale tecnico competente e non operare per alcun motivo scambio di supporti di memorizzazione o posta elettronica con altri. Nel caso si abbia notizia di un nuovo tipo di virus, comunicare tale informazione all'U.O. Sistemi Informatici e Telecomunicazioni e non inviare indiscriminati messaggi a tutti i propri conoscenti.

Almeno in ragione mensile andrà effettuata una ricognizione sul livello di aggiornamento del software presente sulle attrezzature degli **elenchi T-8-1 e T-8-3** al fine di verificare se sia necessaria l'installazione di eventuali FIX e/o effettuare modifiche di configurazione al fine di aumentare il grado di sicurezza delle stesse: la valutazione se operare o meno delle modifiche alle configurazioni o degli aggiornamenti software andrà fatta ogni volta valutando costi e benefici di dette operazioni.

10.13 Formazione e informazione sulla sicurezza informatica

L'informazione e la formazione in materia di sicurezza informatica sono, accanto alla predisposizione di opportune misure tecniche, i pilastri su cui si fonda la gestione in sicurezza del sistema.

La strategia che l'azienda adotta a fini informativi e formativi in materia di sicurezza si articola in:

A) ***Fase di Analisi e Progettazione****: analisi ed identificazione, tramite*

1. *la somministrazione supervisionata di questionari ai "soggetti apicali" delle Unità Operative dei Dipartimenti*
2. *l'acquisizione di documenti quali: organigramma, funzionigramma, topografia fisica e logistica dell'Azienda, relazione sull'architettura dei sistemi informativi e/o diagnostici*

delle coordinate strategiche ed operative in termini di figure, competenze, responsabilità e specifici indici di rischio.

Documenti in output:

- ✓ *organigramma dell'Azienda Ospedaliera sotto lo specifico profilo degli adempimenti in materia di protezione dei dati personali*
- ✓ *tavola sinottica dei fattori di rischio in relazione alle categorie di rischio descritte dall'art. 31 del D.lgs. 196/2003*
- ✓ *tavola sinottica delle possibili azioni e degli specifici interventi formativi a supporto della riduzione del rischio*

L'esecuzione di tale Fase è funzionale alla corretta pianificazione delle attività formative nonché a rendere le stesse immediatamente fruibili (I) per garantire comportamenti conformi alle norme vigenti, (II) per i'impostazione e l'avvio degli specifici adempimenti previsti dalle norme stesse.

B) ***Fase Formativa "on the job"**: identificate le figure da sottoporre ad intervento formativo (da selezionare tra i Responsabili del Trattamento presso i singoli Dipartimenti ed Unità Operative o loro raccordi operativi) si procederà ad un ciclo di interventi in aula con lezioni frontali in classi di circa venti utenti (6 classi totali) per circa venti ore ad aula (suddivise in cinque incontri).*

Gli interventi si svolgeranno con organizzazione a Vostro carico in termini di aule e strumenti (personal computer e videoproiettore) e con materiale didattico a nostro carico.

A prescindere dalle personalizzazioni derivanti dagli esiti delle attività di cui alla precedente Fase A, gli interventi formativi avranno ad oggetto almeno:

- ✓ *Excursus normativo: il Codice in materia di protezione dei dati personali e sue successive modifiche e integrazioni*
- ✓ *Definizioni di legge, individuazione delle figure rilevanti*
- ✓ *Predisposizione ed utilizzo dei moduli di informativa e consenso*
- ✓ *I diritti dell'interessato*
- ✓ *Il ruolo del Garante per la protezione dei dati personali ed i controlli*
- ✓ *Portata dell'obbligo di notifica*
- ✓ *Regime di responsabilità delle figure rilevanti*
- ✓ *Concetto di sicurezza e misure di sicurezza minime e idonee*
- ✓ *Individuazione dei ruoli all'interno del Sistema di trattamento dei dati personali*
- ✓ *Il Documento Programmatico sulla Sicurezza*
- ✓ *Provvedimenti Generali del Garante rilevanti e Provvedimenti specifici per gli organismi sanitari*
- ✓ *Affidamento a terzi esterni del trattamento dei dati personali*

Documenti in output:

- ✓ *Attestati di partecipazione alla fase formativa con assolvimento degli obblighi di formazione previsti dal D.lgs. 196/2003 relativamente alle persone fisiche coinvolte*

C) ***Fase di Project Work**: all'esito delle attività formative di cui alla Fase precedente, si procederà all'assegnazione di Project Work aventi ad oggetto la gestione di problematiche specifiche (a titolo di esempio, "protezione dei dati personali nel Dipartimento X") o "trasversali" (ad esempio, "gestione dei dati genetici").*

Anche tale fase permetterà di contribuire all'avvio ed alla gestione degli specifici adempimenti previsti dalle norme vigenti, con particolare riferimento alle attività di costruzione del Documento Programmatico sulla Sicurezza.

Documenti in output:

1. *Documenti di "Progetto"*
2. *"Criteri e linee guida per la redazione del Documento Programmatico sulla Sicurezza dell'Azienda"*

D) ***Condivisione dei risultati**: all'esito delle attività di cui alla fase precedente, si procederà alla condivisione degli esiti del Project Work.*

10.14 Sicurezza degli archivi cartacei

Gli archivi cartacei si distinguono in:

- archivi di lavoro: mantenuti a cura dei singoli incaricati negli uffici e nelle aree operative;
- archivi mobili: mantenuti a cura del personale incaricato presso i reparti di cura;
- archivi operativi: archivi ufficiali mantenuti a cura di un Incaricato in locali riservati;
- archivi di deposito: archivi mantenuti per motivi storici o per esigenze di legge, mantenuti a cura di un Incaricato in locali di sicurezza.

10.14.1 ARCHIVI DI LAVORO

Il personale incaricato segue le procedure descritte nella lettera di Incarico. In particolare:

- gli armadi, o altre strutture di conservazione, sono tenuti chiusi a chiave;
- nel corso del trattamento i documenti sono custoditi dal personale incaricato chiusi in appositi contenitori di lavoro durante le pause di lavoro e quando il personale incaricato deve assentarsi dall'ufficio o dal posto di lavoro;
- eventuali fotocopie o copie di documenti in pellicola devono essere autorizzate e custodite con le stesse modalità dei documenti originali. La loro distruzione deve avvenire in modo controllato ed in modalità tale da assicurare il non riutilizzo dei dati.

10.14.2 ARCHIVI OPERATIVI

Nell'accedere ai documenti cartacei o in pellicola, l'Incaricato segue le procedure descritte nella lettera di Incarico. In particolare:

- gli armadi, o altre strutture di conservazione, sono tenuti chiusi a chiave;
- nel corso del trattamento i documenti sono custoditi dal personale incaricato chiusi in appositi contenitori di lavoro durante le pause di lavoro e quando il personale incaricato deve assentarsi dall'ufficio o dallo sportello accettazione;
- i documenti sono prelevati dagli archivi per il tempo strettamente necessario allo svolgimento della mansione;
- eventuali fotocopie o copie di documenti in pellicola devono essere autorizzate e custodite con le stesse modalità dei documenti originali.

10.14.3 ARCHIVI MOBILI

Nell'accedere alle cartelle cliniche, l'Incaricato segue le procedure descritte nella lettera di Incarico. In particolare:

- le strutture di conservazione sono normalmente tenute chiuse a chiave;
- i documenti sono prelevati dagli archivi per il tempo strettamente necessario allo svolgimento della mansione;
- eventuali fotocopie devono essere autorizzate e custodite con le stesse modalità dei documenti originali.

10.14.4 ARCHIVI DI DEPOSITO

L'accesso agli archivi di deposito segue le norme previste per le aree di sicurezza ed è consentito esclusivamente agli Incaricati specificatamente autorizzati nella lettera di Incarico.
Il prelievo dei documenti va registrato riportando i dati relativi al soggetto richiedente, data di uscita, data di restituzione.

10.14.5 DISTRUZIONE DEI DOCUMENTI

La distruzione definitiva dei documenti cartacei deve avvenire in modo controllato ed in modalità tale da assicurare il non riutilizzo dei dati.

11 Appendice 1 - Adempimenti delle varie articolazioni aziendali

La messa in sicurezza di un sistema informativo automatizzato richiede lo svolgimento di una serie di attività a diversi livelli.

Le procedure organizzative relative ad uno specifico aspetto di sicurezza si articolano almeno nelle seguenti fasi:
1. **definizione delle politiche** relative all'aspetto specifico
2. **progettazione, implementazione e gestione delle misure di sicurezza** in attuazione delle Politiche di cui al punto precedente
3. **verifica e controllo** della corretta attuazione e dell'efficienza delle misure di sicurezza adottate (Audit di sicurezza).

Al fine di facilitare l'individuazione delle diverse responsabilità rispetto a tematiche specifiche si riassumono di seguito i ruoli dei principali attori aziendali.

Titolare del trattamento dei dati personali	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza
Responsabili del trattamento	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
Incaricato del trattamento	le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile

Nota bene: per **trattamento**, ai sensi del D.L. 196/2003, si intende "**qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati**".

Compiti

Titolare del trattamento dei dati personali	Decide in ordine alle finalità ed alle modalità di trattamento dei dati personali e sul profilo di sicurezza. Il titolare nomina i responsabili del trattamento dei dati e i preposti alla custodia delle chiavi.
Responsabili del trattamento	Sono responsabili con il titolare del profilo di sicurezza del sistema. Individuano gli incaricati del trattamento dei dati e ne definiscono il profilo abilitativo in maniera formale mediante firma degli appositi moduli di autorizzazione (qualora tale individuazione dovesse essere rettificata o revocata andrà fatto ugualmente per iscritto mediante il medesimo modulo). Nel caso informazioni di tipo personale siano gestite su elaboratori non connessi in rete è necessario che il responsabile del trattamento dia opportune indicazioni organizzative affinché venga garantito il rispetto degli adempimenti di cui al **D.L. 196/2003** sulla gestione delle parole chiave. Redazione e successiva manutenzione dei piani di continuità ed emergenza. Redazione e successiva manutenzione dei piani di recupero da disastro. Reazione ed attuazione di progetti informativi e formativi sugli aspetti di sicurezza.
Incaricato del trattamento	Svolgono le mansioni loro assegnate relativamente ai trattamenti di loro competenza.
Servizi tecnici a cui è demandata la gestione tecnica della infrastruttura informatica	Sovrintendono alle risorse dei sistemi e ne gestiscono gli aspetti tecnici in maniera tale da consentirne l'uso ai responsabili del trattamento - e agli incaricati di trattamento qualora individuati -. Individuano i meccanismi di sicurezza che meglio implementano, in una

	logica costo beneficio, le politiche di sicurezza individuate dal titolare del trattamento - e dai responsabili del trattamento qualora nominati -. Sono responsabili della predisposizione dell'elenco completo di funzionalità applicative da concedere in abilitazione agli incaricati del trattamento - a cura del titolare o, qualora nominati, dai responsabili del trattamento Secondo la periodicità definita elaborano i riepiloghi di abilitazioni applicative da sottoporre a verifica periodica da parte del titolare - o qualora nominati dai responsabili del trattamento -. Predispongono e mantengono aggiornati i seguenti elenchi: • **T-6.2-1** - Elenco Server; • **T-6.2-2** - Elenco Apparati Attivi di Rete; Sono responsabili della corretta collocazione degli apparati di elaborazione dati e degli apparati attivi di rete. Sono responsabili della corretta configurazione e gestione delle caratteristiche fisiche dei server - ai fini della sicurezza -. Sono responsabili della formulazione delle politiche di backup dei server. Sono responsabili della formulazione di opportune politiche di gestione dei sistemi di elaborazione che garantiscano il rispetto delle misure minime di sicurezza - e della attuazione delle misure attuative, per la parte di competenza -**.** Se l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, impartisce idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali è possibile assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali deve essere organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato. Sono responsabili della messa in atto delle misure tecniche per il raggiungimento di livelli di sicurezza superiori a quello minimo. Sono responsabili delle misure sistemistiche per il contrasto dei virus informatici e della manutenzione degli elenchi **T-8-1**, **T-8-2**, **T-8-3**. Predispongono l'elenco degli aspetti di sicurezza da monitorare e delle caratteristiche dell'azione di monitoraggio. Conservano le evidenze e dei risultati degli auditing periodici a cui viene sottoposto il sistema.

Crimine informatico:

Definizioni

Direzione Aziendale	La Direzione Generale, Sanitaria e Amministrativa dell'azienda
Responsabili delle macro articolazioni aziendali	Dirigenti a cui è demandata la direzione delle principali articolazioni organizzative aziendali - direzioni di servizi centrali, direzioni di distretto, direzione di presidio, direzioni di dipartimento, ecc… -
Servizi tecnici a cui è demandata la gestione tecnica della infrastruttura informatica	Vedi il punto sulla Privacy

Compiti

Direzione aziendale	Definisce, con l'ausilio tecnico dell'U.O. Sistemi Informatici e Telecomunicazioni, una serie di linee di indirizzo in tema di prevenzione e repressione del crimine informatico.

Responsabili delle macro articolazioni aziendali	Informano gli utilizzatori sulla normativa vigente. Segnalano i comportamenti criminali.
Servizi tecnici a cui è demandata la gestione tecnica della infrastruttura informatica	Sovrintendono alla gestione tecnica dei programmi per il controllo delle intrusioni ai sensi dell'articolo 615-quinquies del Codice Penale

Buon uso delle attrezzature informatiche:

Definizioni

Vedi il punto precedente

Compiti

Direzione Aziendale	Definisce, con l'ausilio dell'U.O. Sistemi Informatici e Telecomunicazioni, una serie di linee di indirizzo in tema di buon uso delle attrezzature informatiche.
Responsabili delle macro articolazioni aziendali	Vigilano sul buon uso delle attrezzature informatiche. Informano e formano gli utilizzatori sulle linee guida aziendali in materia. Censurano e sanzionano i comportamenti non corretti.
Servizi tecnici a cui è demandata la gestione tecnica della infrastruttura informatica	Individuano le misure di natura tecnica in grado di minimizzare l'onere di gestione degli apparati informatici. Definiscono una serie di misure tecniche e di modalità organizzative volte alla ottimizzazione dell'uso dei sistemi di elaborazione - sia di tipo personale che multiutente - . Individuano inoltre misure tecniche che minimizzino il cattivo uso - o facilitino il controllo da parte delle strutture preposte - dei sistemi di elaborazione.

Gestione sicura degli interventi di manutenzione:

Definizioni

Vedi il punto precedente

Compiti

Direzione aziendale	Definisce, con l'ausilio tecnico dell'U.O. Sistemi Informatici e Telecomunicazioni, una serie di linee di indirizzo in tema di gestione sicura degli interventi di manutenzione.
Servizi tecnici a cui è demandata la gestione tecnica della infrastruttura informatica	Presidiano gli interventi di manutenzione sui sistemi di elaborazione e sugli apparati di rete in maniera tale da prevenire diffusione di informazioni e azioni che diminuiscano il livello di sicurezza del sistema, nella sua globalità.

12 Appendice 2 - Piano di continuità ed emergenza

Vedasi il Piano di continuità ed emergenza interno depositato presso l'U.O. Sistemi Informatici e Telecomunicazioni.

13 Appendice 3 - Regolamento interno per la gestione dei server

Vedasi il Regolamento interno per la gestione dei server depositato presso l'U.O. Sistemi Informatici e Telecomunicazioni.

14 Appendice 4 - Regolamento interno per la gestione della rete di comunicazioni

Vedasi il Regolamento interno per la gestione della rete di comunicazioni depositato presso l'U.O. Sistemi Informatici e Telecomunicazioni.

15 Appendice 5 - Regolamento interno per la gestione dei PC interni

Vedasi il Regolamento interno per la gestione dei Clients depositato presso l'U.O. Sistemi Informatici e Telecomunicazioni.

16 Appendice 6 - Regole tecniche per la sicurezza dei sistemi informatici

1) L'accesso ai personal computer aziendali ed ai sistemi informativi aziendali avviene attraverso una combinazione di utente e password di tipo individuale di seguito chiamata Utenza. Non è consentito condividere l'utenza di accesso con altri dipendenti.
2) Ogni Utenza, con i relativi privilegi, va preventivamente autorizzata dal responsabile della U.O. di appartenenza del dipendente che ne da comunicazione per iscritto al Responsabile della U.O. informatizzazione e Telecomunicazioni di seguito indicato come Amministratore del sistema. I privilegi di ogni utenza sono tali da consentire ad ogni utente di svolgere esclusivamente le attività alle quali lo stesso è preposto.
3) L'Amministratore del sistema, definisce tecnicamente l'utenza ed i privilegi ad essa connessi e ne da comunicazione al dipendente. Il dipendente è il depositario dell'Utenza ed è tenuto a modificare la password al primo accesso e periodicamente con cadenza almeno trimestrale nel rispetto delle regole di definizione.
4) Regole per la definizione della password:
    - password è diversa dal nome utente;
    - password è lunga almeno 8 caratteri;
    - password è diversa da parole comuni, nomi etc;
    - la password deve contenere numeri e lettere.
    - la password deve essere modificata con cadenza almeno trimestrale
5) I Responsabili di ogni U.O. sono tenuti a comunicare tempestivamente all'Amministratore del sistema ogni eventuale modifica delle Utenze dovute a dimissioni, trasferimenti, cambio di mansioni del dipendente. L'amministratore del sistema è tenuto alla disattivazione o modifica dell'utenza conformemente a quanto indicato dal responsabile della U.O.
6) Non è consentita l'installazione di software se non preventivamente autorizzata dall'Amministratore.
7) Non è consentito il collegamento in rete aziendale o lo spostamento di computer se non preventivamente autorizzato dall'Amministratore.
8) Non è consentita la memorizzazione di dati sensibili su computer con sistema operativo Microsoft precedente al windows 2000 (Windows 98, 95, Millenium).
9) La memorizzazione di dati sensibili su computer con sistema operativo Windows 2000, XP o successivi è consentita previa attivazione della crittografia per le cartelle contenenti i dati sensibili (rivolgersi alla U.O. Informatizzazione e Telecomunicazioni per ottenere informazioni su come attivare la crittografia).
10) Quando si memorizzano dati sensibili o comunque importanti per l'azienda sul computer locale preoccuparsi di effettuare il salvataggio degli stessi su supporto magnetico almeno giornalmente. Per effettuare il salvataggio può essere utilizzata il programma backup a corredo delle Utilità del Sistema operativo. Conservare i salvataggi in luogo protetto, accessibile solo al personale autorizzato.

11) Controllare che sul computer sia installato il software Antivirus che l'Azienda ha adottato (Norton Antivirus client) e periodicamente controllare che siano aggiornate le definizioni dei virus. Qualora ciò non si verifichi inviare tempestivamente alla U.O. Informatizzazione e Telecomunicazioni una richiesta di installazione o aggiornamento del software usando gli appositi moduli.
12) L'accesso ad internet dai computer dell'Azienda è consentito solo attraverso la rete aziendale. Non è quindi consentito l'utilizzo di modem per il collegamento ad internet.
13) L'accesso ai siti Web è limitato a quelli i cui contenuti sono strettamente legati alla attività istituzionale svolta.
14) Qualora si utilizzino programmi di posta elettronica, disattivare l'anteprima dei messaggi ed aprire solo la posta il cui mittente sia conosciuto.

17 Appendice 7 - Modulistica

Modulo per la Concessione/Revoca/Modifica delle abilitazioni applicative

MODELLO E

GESTIONE ABILITAZIONI SISTEMI INFORMATICI

(Compilare a stampatello – Non saranno accettate richieste incomplete)

Prot n. _____ **del** _____

Al Responsabile U.O. Informatizzazione e Telecomunicazioni
Dott. Vincenzo Cardinale
Fax N. 091 6664432

AREA o U.O. RICHIEDENTE (Indicare Codice e Nome del Centro di Costo)	
RESPONSABILE U.O. (Cognome e Nom	

SI RICHIEDE DI: CONCEDERE L'ABILITAZIONE ☐
REVOCARE L'ABILITAZIONE A ELENCO FUNZIONI ☐
REVOCARE L'ABILITAZIONE AL SISTEMA INFORMATICO ☐

Persona oggetto dell'abilitazione (Cognome – Nome – Matricola – Qualifica - Interno Telefonico)	
CODICE SISTEMA INFORMATIVO (vedi piè di pagina)	

FUNZIONALITA' (Indicare dettagliatamente a quali operazioni abilitare/disabilitare l'utente)

Timbro e Firma
(del Capo Area o Direttore di U.O.)

_____

18 Appendice 8 – Moduli DPS

I Moduli sono accessibili, in formati elettronico, dall'interno della rete Aziendale, attraverso l'utilizzo di Internet explorer, digitando nel campo indirizzo http://it/Privacy

Unita' Operativa:			**Responsabile**		
Modulo A – Elenco dei trattamenti: informazioni essenziali					
Identificativo del trattamento	**Finalità perseguita o attività svolta**	**Natura dei Dati (P,S,G)**	**Altre UO che concorrono al trattamento**	**Descrizione degli strumenti utilizzati (Informatici o cartacei) Es. PC. Portatile, Elaboratore**	**Tipo di protezione scelta (Obbligatorio per dati di natura S o G l'adozione della Crittografia o della Separazione dei dati**

Unita' Operativa:			**Responsabile**		
Modulo B - Elenco dei trattamenti: descrizione degli strumenti					
Identificativo del trattamento	**Eventuale banca dati (Access, Oracle ….) Software Applicativo e relativo Fornitore**	**Ubicazione fisica della banca dati (Indicare padiglione, piano, stanza) e metodo di protezione dei locali**	**Ubicazione fisica dei supporti utilizzati per le copie di sicurezza metodo di protezione e frequenza dei salvataggi**	**Tipologia dei dispositivi di accesso che concorrono al trattamento**	**Tipologia di connessione (rete locale, geografica, internet)**

Unita' Operativa:		RESPONSABILE:	
Modulo C - Elenco degli Incaricati e relativi compiti			
Identificativo del trattamento	**Cognome e Nome**	**Matricola (Se esterno all'azienda indicare la Ditta)**	**Compiti e responsabilità (Acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, Salvataggio e ripristino dei dati)**

Unita' Operativa:			RESPONSABILE:		
Modulo D - Descrizione della dotazione Hardware e Software					
Tipo apparato (PC, Portatile, Server, Stampante)	**Sistema Operativo (Windows 95, 98, 2000, XP …..)**	**Elenco del Software applicativo installato (Produttore e Nome del Software)**	**Ubicazione fisica (Indicare padiglione, piano, stanza) e metodo di protezione dei locali**	**Elenco del personale che ha accesso all'apparato - Cognome Nome e Matricola o Ditta se esterno**	**Elenco degli Identificativi di trattamento dati e/o scopi di utilizzo dell'apparato**

Unita' Operativa:	RESPONSABILE:

Modulo E - Analisi dei rischi

Rischi		Si/No	Descrizione dell'impatto sulla sicurezza (alto/medio/basso)
comportamento degli operatori	Sottrazione di credenziali di autenticazione		
	carenza di consapevolezza, disattenzione o incuria		
	Comportamenti sleali o fraudolenti		
	errore materiale		
	altro evento		
Eventi relativi agli strumenti	Azione di virus informatici o altri programmi pericolosi		
	spamming o tecniche di sabotaggio		
	malfunzionamento indisponibilità o degrado degli strumenti		
	accessi esterni non autorizzati		
	intercettazione di informazioni in rete		
	altro evento		
Eventi relativi al contesto	Accessi non autorizzati a locari/reparti ad accesso ristretto		
	sottrazione di strumenti contenenti dati		
	Eventi distruttivi, naturalio o artificiali nonché dolosi, accidentali o dovuti ad incuria		
	guasto ai sistemi complementari (impianto elettrico, climatizzazione ecc.)		
	errori umani nella gestione della sicurezza fisica		
	altro evento		

Unita' Operativa:	Responsabile				
Modulo F - Misure adottate o da adottare					
Misura	**Descrizione dei rischi contrastati**	**Trattamenti interessati**	**Misura già in essere**	**Misura da adottare**	**Struttura o persone addette all'adozione**

Unita' Operativa: **Responsabile**

Modulo G - Trattamenti affidati all'esterno			
Descrizione sintetica dell'attività affidata all'esterno	**Trattamenti di dati interessati**	**Soggetto esterno**	**Descrizione dei criteri e degli impegni assunti per l'adozione delle misure**

Allegati

Allegato T-5.2-1 - Elenco trattamenti che è opportuno tutelare da minacce alla disponibilità di servizio
Accettazione/Dimissioni/Trasferimenti
Triage Pronto Soccorso
Gestione SDO
CUP (Centro Unico di Prenotazione delle Prestazioni Ambulatoriali)
Tracciati regionali con dati di Attività
Sistema Contabile
S.I. Casse
S.I. Trattamento del Personale
S.I. Radiologia
S.I. Anatomia Patologica
S.I. Patologia Clinica
S.I. Centro Trasfusionale
S.I. Malattie dell'Apparato Respiratorio
Altri Sistemi Informativi Stand Alone di Reparto

Allegato T-5.2-2 - Elenco trattamenti che è opportuno tutelare da minacce di modifica illecita
Accettazione/Dimissioni/Trasferimenti
Triage Pronto Soccorso
Gestione SDO
CUP (Centro Unico di Prenotazione delle Prestazioni Ambulatoriali)
Tracciati regionali con dati di Attività
Sistema Contabile
S.I. Protocollo
S.I. Casse
S.I. Trattamento del Personale
S.I. Radiologia
S.I. Anatomia Patologica
S.I. Patologia Clinica
S.I. Centro Trasfusionale
Altri Sistemi Informativi Stand Alone di Reparto

Allegato T-5.2-3 - Elenco trattamenti che è opportuno tutelare da minacce di fraudolenta impersonificazione
Sistema Contabile
S.I. Protocollo
S.I. Trattamento del Personale

Allegato T-5.2-4 - Elenco trattamenti che è opportuno tutelare da minacce di intercettazione
Accettazione/Dimissioni/Trasferimenti
Triage Pronto Soccorso
Gestione SDO
CUP (Centro Unico di Prenotazione delle Prestazioni Ambulatoriali)
Tracciati regionali con dati di Attività
Sistema Contabile
S.I. Casse
S.I. Trattamento del Personale
S.I. Radiologia
S.I. Anatomia Patologica
S.I. Patologia Clinica
S.I. Centro Trasfusionale
S.I. Malattie dell'Apparato Respiratorio
Altri Sistemi Informativi Stand Alone di Reparto

Allegato T-6.2-1 - Elenco server
Elenco depositato presso l'U.O. Sistemi Informatici e Telecomunicazioni.

Allegato T-6.2-2 - Elenco apparati attivi di rete
Elenco depositato presso l'U.O. Sistemi Informatici e Telecomunicazioni.

Allegato T-6.2.3 Elenco VLAN
Elenco depositato presso l'U.O. Sistemi Informatici e Telecomunicazioni.

Allegato T-8-1 - Elenco attrezzature di confine su cui mantenere aggiornato il software antivirale
Elenco depositato presso l'U.O. Sistemi Informatici e Telecomunicazioni.

Allegato T-8-2 - Elenco client critici su cui mantenere aggiornato il software antivirale
Tutti i PC Aziendali collegati alla rete interna sono tenuti costantemente aggiornati con un sistema Antivirus centralizzato su un server dedicato all'uopo.

Allegato T-8-3 - Elenco file server su cui mantenere aggiornato il software antivirale
Elenco depositato presso l'U.O. Sistemi Informatici e Telecomunicazioni.