RELAZIONE DI PUBBLICAZIONE

Il sottoscritto dichiara che la presente deliberazione viene affissa all'Albo Pretorio di questa Azienda per quindici giorni consecutivi, dal 19/6/18 al 3/5/18 ai sensi dell'art.124, comma 1, del D.Lgs. 267/00.

Lì _____ IL FUNZIONARIO

La presente deliberazione è stata-trasmessa al Comitato di Rappresentanza della Conferenza dei Sindaci con nota prot. n. _____del _____

lì _____ IL FUNZIONARIO

La presente deliberazione è stata trasmessa al Collegio Sindacale con nota prot. n. _____del _____

lì _____ IL FUNZIONARIO

La presente deliberazione, decorso il termine di 10 giorni dalla pubblicazione all'Albo Pretorio dell'Azienda, è divenuta esecutiva ai sensi dell'art.134, comma 3 e 4 del D.Lgs. 267/00.

Lì_____ IL FUNZIONARIO

La presente deliberazione viene resa immediatamente eseguibile per l'urgenza.

Lì, _____ IL FUNZIONARIO

REGIONE CAMPANIA

AZIENDA SANITARIA LOCALE NAPOLI 2 NORD

VIA LUPOLI , 27

80027 FRATTAMAGGIORE

Deliberazione n.ro 499 **del** 18/luglio

L'anno 2018, il giorno 18 del mese Aprile,

OGGETTO: Documento Programmatico sulla Sicurezza. Aggiornamento 2018

IL DIRETTORE GENERALE

Nominato con Decreto del Presidente della Giunta Regionale della Campania n. 164 del 19/7/2016, in esecuzione della DGRC n. 373 del 13/07/2016

LA COORDINATRICE DEL GRUPPO PRIVACY

Premesso

Che con deliberazione n. 199 del 22/02/2018 l'Azienda, ai sensi dell'art. 29 del D.lgs. n. 196/2003, ha già provveduto ad individuare i responsabili del trattamento dati tra quei soggetti che forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati, ivi compreso il profilo relativo alla sicurezza, con obbligo del Titolare medesimo di impartire le relative istruzioni per l'esecuzione dell'incarico conferito;

Che con deliberazione n. 108/2010 l'Azienda ha già provveduto a regolamentare il trattamento dei dati personali ai sensi dell'art. 20 del d.lgs. 196/ 03, costituendo, di seguito il Gruppo Aziendale Privacy con provvedimento 712/10 e ss.mm.ii. ai sensi dell'art 17 del succitato regolamento;

Che con deliberazione n. 195 del 03/02/2017 è stato approvato il regolamento aziendale relativo alla tutela dei diritti di soggetti coinvolti dalla utilizzazione o dalla diffusione di immagini relative a comportamenti personali raccolte all'interno di luoghi dell'Azienda aperti al pubblico, all'insaputa degli interessati e, comunque, senza il loro consenso;

Che l'ASL Napoli 2 nord ha già approvato il Documento Programmatico sulla Sicurezza con deliberazione n. 309 del 31/03/2011 per il periodo 01/04/2011-31/03/2012 e con deliberazione n. 262 del 29/03/2012 per il periodo 01/04/2012-31/03/2013, e deliberazione n. 369 del31/03/2014 per il periodo 01/04/2014-31/03/2015, in conformità alle disposizioni contenute nel D.lgs. 196/2003 e ss.mm.ii.

Che il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 26 aprile 2016, ha disciplinato i trattamenti di dati personali relativi per la protezione delle persone fisiche con una maggiore attenzione alla libera circolazione di dati ed un più elevato livello di protezione, abrogando la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

Rilevato

Che, ai sensi del Decreto Legge n. 5/2012, convertito in Legge n. 35/2012, era stato abrogato l'obbligo di redazione ed aggiornamento del Documento in questione e che, pertanto, rimaneva in vigenza il documento approvato con delibera n. 369 di cui sopra;

Che rimane inalterato l'obbligo di adottare misure minime di sicurezza dei dati e dei sistemi secondo le prescrizioni dell'art. 34 del Codice della privacy e dell'allegato B, tenendo conto, in particolare, che "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;

Ritenuta

alla luce di quanto sopra, vi sia l'esigenza di aggiornare 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 ed addetti alla gestione e 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) Adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rilevare lo stato di salute o la vita sessuale effettuati da organismi sanitari

Inoltre, la necessità di aggiornare l'elenco degli incaricati del trattamento dati, le relative informative e formazione e l'adozione di un nuovo Documento Programmatico sulla Sicurezza, contenente tutte le modifiche apportate al precedente Documento.

Visti:

1. Il d.lgs. 502/92 e il d.lgs 229/99;
2. la L.R. 16/08;

per i motivi di cui alla narrativa, che qui si intendono integralmente riportati, e attestato che il presente provvedimento, alla stregua dell'istruttoria compiuta e delle risultanze e degli atti tutti richiamati nella premessa, costituenti istruttoria a tutti gli effetti di legge, è regolare e legittimo, nella forma e nella sostanza, ai sensi della vigente normativa e utile per il servizio pubblico, e per gli effetti di quanto disposto dall'art. 1 della legge 20/94 e successive modifiche

PROPONE

Al sig. Direttore generale

Per i motivi espressi in narrativa che qui s'intendono integralmente riportati e trascritti:

Di approvare, in ossequio alle disposizioni di cui al D.Lgs 196/2003, il Documento Programmatico sulla Sicurezza dei dati personali dell'Azienda Sanitaria Locale Napoli 2 Nord che, allegato al presente provvedimento, ne forma parte integrante e sostanziale;

La Coordinatrice Gruppo Aziendale Privacy
Dr.ssa Angela Cocca

Il Direttore Generale

Alla stregua dell'istruttoria compiuta dalla Coordinatrice del Gruppo aziendale Privacy e delle risultanze degli atti tutti richiamati nella premessa, costituenti istruttoria a tutti gli effetti di legge, nonché di espressa dichiarazione, mediante la sottoscrizione dello stesso da parte del dirigente proponente, della regolarità e legittimità del presente atto nella forma e nella sostanza, ai sensi della vigente normativa e utilità per il Servizio pubblico, ai sensi e per gli effetti di quanto disposto dall'art.1 della legge 20/94 e successive modifiche;

Sentiti i pareri favorevoli del Direttore Sanitario e del Direttore Amministrativo

D E L I B E R A

Di approvare, in ossequio alle disposizioni di cui al D.lgs. 196/2003, il Documento Programmatico sulla Sicurezza dei dati personali dell'Azienda Sanitaria Locale Napoli 2 Nord che, allegato al presente provvedimento, ne forma parte integrante e sostanziale;

Di precisare che il suddetto provvedimento venga trasmesso

Di rendere la presente deliberazione immediatamente eseguibile, trasmettendone copia a:

- Collegio Sindacale;
- UOC AAGG perché provveda ad inserire tale deliberazione tra gli atti di interesse generale.

IL DIRETTORE SANITARIO

Dott.ssa M. Virginia Scafarto

IL DIRETTORE AMMINISTRATIVO

dott. Francesco Balivo

IL DIRETTORE GENERALE

Dott. Antonio d'Amore

CODICE DELLA PRIVACY

(D.L.vo N. 196/2003)

DISPOSIZIONI MINIME SULLA SICUREZZA

E

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Il presente documento si compone di n. 54 pagine (inclusa la presente)

Data di emissione: 31/09/2018

Il responsabile della sicurezza

U.O.C. Tecnologie Informatiche e Ing. Clinica

ing. Salvatore Flaminio

Azienda Sanitaria Locale Napoli 2 Nord

Via Lupoli n.27

80027 Frattamaggiore NA

Sommario

Premessa

Scopo di questo documento è stabilire le misure di sicurezza organizzative, fisiche e logiche da adottare affinché siano rispettati gli obblighi, in materia di sicurezza del trattamento dei dati effettuato da Azienda Sanitaria Locale Napoli 2 Nord, previsti dal D.L.vo 30/06/2003 Num. 196 "Codice in materia di protezione dei dati personali".

Il presente documento è stato redatto da ing. Salvatore Flaminio in qualità di Direttore U.O.C. Tecnologie Informatiche e Ingegneria Clinica, che provvede a firmarlo in calce.

Eventuali situazioni di deviazione accertate rispetto a quanto precisato nel presente documento dovranno essere rimosse nel più breve tempo possibile.

Normativa di riferimento

D.L.vo n. 196 del 30/06/2003;

Regolamento per l'utilizzo della rete.

Definizioni e responsabilità

AMMINISTRATORE DI SISTEMA: il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione. In questo contesto l'amministratore di sistema assume anche le funzioni di amministratore di rete, ovvero del soggetto che deve sovrintendere alle risorse di rete e di consentirne l'utilizzazione. L'amministratore deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali.

Ai fini della sicurezza l'amministratore di sistema ha le responsabilità indicate nella lettera di incarico.

CUSTODE DELLE PASSWORD: il soggetto cui è conferito la gestione delle password degli incaricati del trattamento dei dati in conformità ai compiti indicati nella lettera di incarico.

DATI ANONIMI: i dati che in origine, o a seguito di trattamento, non possono essere associati a un interessato identificato o identificabile.

DATI PERSONALI: qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

DATI IDENTIFICATIVI: i dati personali che permettono l'identificazione diretta dell'interessato.

DATI SENSIBILI: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

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

INCARICATO: il soggetto, nominato dal titolare o dal responsabile del trattamento, che tratta i dati. L'incaricato del trattamento dei dati, con specifico riferimento alla sicurezza, ha le responsabilità indicate nella lettera di incarico.

INTERESSATO: il soggetto al quale si riferiscono i dati personali.

RESPONSABILE DEL TRATTAMENTO: il soggetto preposto dal titolare al trattamento dei dati personali. La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto che fornisce, per esperienza, capacità e affidabilità, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il

profilo relativo alla sicurezza. Il responsabile del trattamento dei dati personali, ai fini della sicurezza, ha le responsabilità indicate nella lettera di incarico.

RESPONSABILE DELLA SICUREZZA INFORMATICA: il soggetto preposto dal titolare alla gestione della sicurezza informatica. La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali. Ai fini della sicurezza il responsabile del sistema informativo ha le responsabilità indicate nella lettera di incarico.

TITOLARE: il titolare del trattamento è Direttore Generale dott. Antonio D'Amore e la titolarità è esercitata dal rappresentante legale, tra i compiti che la legge gli assegna e che non sono delegabili, è prevista la vigilanza sul rispetto da parte dei Responsabili delle proprie istruzioni, nonché sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il titolare è il soggetto che assume le decisioni sulle modalità e le finalità del trattamento.

Titolare, responsabili, incaricati

Titolare del trattamento: Direttore Generale dott. Antonio D'Amore

Responsabile del trattamento dei dati: in allegato elenco Responsabili Trattamento e disposizione D.G. n. _____ del _____

Responsabile della sicurezza informatica: ing. Salvatore Flaminio

Amministratore della rete: vedi tabella _____

Custode delle password: vedi elenco

Incaricati del trattamento dei dati: vedi elenchi agli atti delle rispettive UOC

Incaricato dell'assistenza e della manutenzione degli strumenti elettronici: –vedi elenco custodito presso la UOC Tecnologie Informatiche

Analisi dei rischi

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

L'analisi dei rischi consiste nella:

A. *individuazione di tutte le risorse del patrimonio informativo*
B. *identificazione delle minacce a cui tali risorse sono sottoposte*
C. *identificazione delle vulnerabilità*
D. *definizione delle relative contromisure*

La classificazione dei dati in funzione dell'analisi dei rischi risulta la seguente:

- DATI ANONIMI, ovvero la classe di dati a minore rischio, per la quale non sono previste particolari misure di sicurezza;
- DATI PERSONALI,
  - DATI PERSONALI SEMPLICI, ovvero la classe di dati a rischio intermedio
  - DATI PERSONALI SENSIBILI/GIUDIZIARI, ovvero la classe di dati ad alto rischio;
  - DATI PERSONALI SANITARI, ovvero la classe di dati a rischio altissimo.

Individuazione delle risorse da proteggere

Le risorse da proteggere sono:

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

Per ulteriori dettagli vedere gli Allegati 1 e 3.

Individuazione delle minacce

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

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

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

Per ulteriori dettagli delle minacce relative all'aspetto informatico vedere l'Allegato 2

Individuazione delle vulnerabilità

Nelle tabelle seguenti sono elencate le vulnerabilità del sistema informativo che possono essere potenzialmente sfruttate qualora si realizzasse una delle minacce indicate nell'articolo 6.

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

Documenti cartacei	Software	Personale
Locali documenti non protetti	Interfaccia uomo-macchina complicata	Mancanza di personale
Carenza di precauzioni nell'eliminazione	Mancanza di identificazione / autenticazione	Mancanza di supervisione degli esterni
Non controllo delle copie	Mancanza del registro delle attività (log)	Formazione insufficiente sulla sicurezza
	Errori noti del software	Mancanza di consapevolezza
	Tabelle di password non protette	Uso scorretto di hardware/software
	Carenza/Assenza di password management	Carenza di monitoraggio
	Scorretta allocazione dei diritti di accesso	Mancanza di politiche per i mezzi di comunicazione
	Carenza di controllo nel caricamento e uso di software	Procedure di reclutamento inadeguate
	Permanenza di sessioni aperte senza utente	
	Carenza di controllo di configurazione	
	Carenza di documentazione	
	Mancanza di copie di backup	
	Incuria nella dismissione di supporti riscrivibili	

Individuazione delle contromisure

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

- *contromisure di carattere fisico*
- *contromisure di carattere procedurale*
- *contromisure di carattere elettronico/informatico*

Contromisure di carattere fisico

- Le apparecchiature informatiche critiche (server di rete, computer utilizzati per il trattamento dei dati personali o sensibili/giudiziari e apparecchiature di telecomunicazione, dispositivi di copia) e gli archivi cartacei contenenti dati personali o sensibili/giudiziari sono situati in locali ad accesso controllato che è regolamentato mediante ritiro di chiavi e con annotazione dei dati dell'accedente in un apposito registro custodito dal responsabile
- i locali ad accesso controllato sono all'interno di aree sotto la responsabilità del Direttore di Struttura
- i responsabili dei trattamenti indicati nell'allegato 1 sono anche responsabili dell'area in cui si trovano i trattamenti
- i locali ad accesso controllato sono chiusi anche se presidiati, le chiavi sono custodite a cura del personale dipendente (elenco presso le UOC di competenza)
- l'ingresso ai locali ad accesso controllato è possibile solo dall'interno dell'area sotto la responsabilità dell'ENTE
- le aree di accesso ai locali ad accesso controllato sono provvisti di sistema di allarme e di estintore
- sono programmati interventi atti a dotare detti locali ad accesso controllato, di controllo automatizzato con porte blindate e impianti elettrici dedicati, mentre già sono attivi i sistemi di condizionamento e di continuità elettrica che è garantita da appositi gruppi di continuità ed elettrogeni

Contromisure di carattere procedurale

- l'ingresso nei locali ad accesso controllato è consentito solo alle persone autorizzate
- il responsabile dell'area ad accesso controllato deve mantenere un effettivo controllo sull'area di sua responsabilità

- nei locali ad accesso controllato è esposta una lista delle persone autorizzate ad accedere, che è periodicamente controllata dal responsabile del trattamento o da un suo delegato
- i visitatori occasionali delle aree ad accesso controllato sono accompagnati da un incaricato
- per l'ingresso ai locali ad accesso controllato è necessaria preventiva autorizzazione da parte del Responsabile del trattamento e successiva registrazione su apposito registro
- è controllata l'attuazione del piano di verifica periodica sull'efficacia degli allarmi e degli estintori
- l'ingresso in locali ad accesso controllato da parte di dipendenti o estranei per operazioni di pulizia o di manutenzione avviene solo se i contenitori dei dati sono chiusi a chiave e i computer sono spenti oppure se le operazioni si svolgono alla presenza dell'Incaricato del trattamento di tali dati
- i registri, contenenti dati comuni e particolari, durante l'orario di lavoro devono essere tenuti in e affidati al responsabile di turno. Al termine dell'orario di lavoro vengono depositati e successivamente raccolti da un incaricato del trattamento e conservati in luogo sicuro per essere riconsegnati da un incaricato del trattamento all'inizio dell'orario di lavoro
- il responsabile del trattamento dei dati è responsabile della riservatezza del registro personale in cui sono annotati dati comuni e particolari. Fuori dall'orario di servizio il registro viene conservato nell'armadietto del responsabile del trattamento dei dati che è chiuso a chiave, una chiave di riserva è mantenuta con le dovute cautele dalla ditta
- il protocollo riservato, accessibile solo al Titolare e al Responsabile del trattamento, è conservato in luogo sicuro

Contromisure di carattere elettronico/informatico

- Vedere l'Allegato 3

Norme per il personale

Tutti i dipendenti concorrono alla realizzazione della sicurezza, pertanto devono proteggere le risorse loro assegnate per lo svolgimento dell'attività lavorativa, nel rispetto di quanto stabilito nel presente documento e dal regolamento di utilizzo della rete (Allegato 4).

Incident response e ripristino

Vedere l'Allegato 3

Piano di formazione

La formazione degli incaricati viene effettuata all'ingresso in servizio, all'installazione di nuovi strumenti per il trattamento dei dati, e comunque con frequenza annuale. Le finalità della formazione sono:

- sensibilizzare gli incaricati sulle tematiche di sicurezza, in particolar modo sui rischi e sulle responsabilità che riguardano il trattamento dei dati personali
- proporre buone pratiche di utilizzo sicuro della rete
- riconoscere eventuali anomalie di funzionamento dei sistemi (hardware e software) correlate a problemi di sicurezza

Aggiornamento del piano

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

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

Elenco Allegati costituenti parte integrante di questo documento

- Allegato 1 - elenco trattamenti dei dati
- Allegato 2 - minacce hardware, minacce rete, minacce dati trattati, minacce supporti
- Allegato 3 - misure di carattere elettronico/informatico, politiche di sicurezza, incident response e ripristino
- Allegato 4 - regolamento per l'utilizzo della rete
- Allegato 5 – uso del proxy
- Lettere di incarico per il trattamento dei dati
- Lettera di incarico per il responsabile del trattamento
- Lettera di incarico per il custode delle password
- Lettera di incarico per l'amministratore di sistema

Il presente Documento Programmatico sulla Sicurezza deve essere divulgato e illustrato a tutti gli incaricati.

Il redattore del documento

Direttore UOC Tecnologie Informatiche e Ingegneria Clinica

ing. Salvatore Flaminio

Nota: Fonti di documentazione

Il modello di documento programmatico sulla sicurezza è stato predisposto consultando le seguenti fonti:

- http://www.garanteprivacy.it
- "Sicurezza informatica" ECDL IT Administrator – Modulo 5 Testo di riferimento per la certificazione EUCIP - McGraw Hill ISBN 88-3864333-4 Tabelle Minacce e vulnerabilità Cap. 1
- Il regolamento per l'utilizzo della rete è stato derivato dal documento CISEL 0203G286 – CISEL Centro Studi per gli Enti Locali – Maggioli

ALLEGATO 1 – Elenco trattamenti dei dati

Tabella 1 - Elenco dei trattamenti dei dati

Descrizione sintetica:

La ASL NA2 NORD tratta essenzialmente i seguenti dati:

- **amministrativi e contabili**: offerte tecniche, offerte economiche, documenti di gara, documenti della stazione appaltante, fatture (fornitori e clienti), bolle (fornitori e clienti), estratti conto, informazioni economiche e finanziarie sui clienti e fornitori, solleciti di pagamento; corrispondenza clienti e fornitori
- **curriculari e stipendiali**: curricula professionali, dati anagrafici di base, dati relativi alla composizione del cedolino, dati sui corsi di formazione
- **sanitari**: legati alle prestazioni sanitarie, ai ricoveri, alle prescrizioni sanitarie erogate per diversi motivi agli assistiti della ASL NA2 NORD
- **legali**: relativi ad atti di giustizia amministrativa da fornitori e verso clienti
- **tecnici**: documenti di analisi, manuali, struttura di data base, documenti di progetto e di qualità, informazioni su siti web

Natura dei dati trattati: di seguito è indicato, in forma tabellare, la relazione esistente tra il tipo di trattamento e la natura dei dati con evidenziazione della classe di rischio (SENSIBILE, COMUNE) tenendo presente la seguente classificazione:

- DATI ANONIMI (TIPO COMUNE), ovvero la classe di dati a minore rischio, per la quale non sono previste particolari misure di sicurezza
- DATI PERSONALI (TIPO SENSIBILE)
  - DATI PERSONALI SEMPLICI, ovvero la classe di dati a rischio intermedio
  - DATI PERSONALI SENSIBILI/GIUDIZIARI, ovvero la classe di dati ad alto rischio
  - DATI PERSONALI SANITARI, ovvero la classe di dati a rischio altissimo

Tabella A1 – Elenco dei trattamenti dei dati

codice	trattamento	natura dei dati
d01	stipendi al personale dipendente	sensibile
d02	stipendi al personale convenzionato	sensibile
d03	gestione giuridica del personale dipendente	comune
d04	rilevazione elettronica presenze del personale	comune

codice	trattamento	natura dei dati
d05	contabilità generale	comune
d06	libera professione (intramoenia)	comune
d07	magazzini farmacia	comune
d08	protocollo informatico	comune
d09	schede dimissioni ospedaliere	sensibile
d10	prenotazione ambulatoriali (cup aziendale)	sensibile
d11	anagrafe assistiti	sensibile
d12	vaccinazioni	sensibile
d13	screening patologie femminili	sensibile
d14	invalidi civili	sensibile
d15	convenzionamento esterno	sensibile
d16	termalismo	sensibile
d17	riabilitazione	sensibile
d18	laboratori di analisi chimico-cliniche	sensibile
d19	diagnostica per immagini	sensibile
d20	sito web aziendale	comune
d21	diabetologia (piani terapeutici)	sensibile
d22	diabetologia (cartella clinica)	sensibile
d23	tea	sensibile
d24	adt	sensibile
d25	farmaceutica convenzionata esterna	sensibile
d26	assistenza domiciliare	sensibile
d27	cartelle cliniche gestione documentale	sensibile
d28	cartelle cliniche diendenze patologiche	sensibile
d29	prenotazione ambulatoriali (cup regionale)	sensibile
d30	credenziali	comune
d31	lab. analisi chimico-cliniche ex na2-na3 osped.	sensibile
d32	lab. analisi chimico-cliniche ex na2-na3 territ.	sensibile
d33	diagnostica per immagini pacs e ris ex na2-na3	sensibile

Struttura di riferimento: di seguito sono indicate le strutture all'interno delle quali vengono effettuati i trattamenti. Nell'ultima colonna della tabella, sono riportate altre strutture che concorrono al trattamento.

Tabella A2 – Elenco strutture che effettuano i trattamenti

codice	dato	struttura riferimento	altre strutture trattanti
D01	stipendi al personale dipendente	servizio personale	strutture sanitarie distribuite sul territorio.
D02	stipendi al personale convenzionato	servizio personale	strutture sanitarie distribuite sul territorio.
D03	gestione giuridica del personale dipendente	servizio personale	strutture sanitarie distribuite sul territorio.
D04	rilevazione elettronica presenze del personale	servizio personale	strutture sanitarie distribuite sul territorio.
D05	contabilità generale	servizio economico finanziario	strutture economali distrettuali e di presidio ospedaliero
D06	libera professione (intramoenia)	servizio economico finanziario	strutture economali distrettuali
D07	magazzini farmacia	servizio farmaceutico	farmacie ospedaliere
D08	protocollo informatico	servizio aa. gg.	
D09	schede dimissioni ospedaliere	direzioni sanitarie p.o.	reparti p.o.
D10	prenotazione ambulatoriali (cup)	direzione distretti e presidi ospedalieri;	ambulatori distrettuali ed ospedalieri
D11	anagrafe assistiti	direzione distretti;	presidi ospedalieri, dipartimenti strutturali
D12	vaccinazioni	servizio di epidemiologia	uo materno infantile dei distretti
D13	screening patologie femminili	dipartimento materno infantile	uo materno infantile dei distretti
D14	invalidi civili	coordinamento medicina legale	uo medicina legale dei singoli distretti
D15	convenzionamento esterno	direzione distretti	staff direzione

codice	dato	struttura riferimento	altre strutture trattanti
D16	termalismo	direzione distretti	staff direzione
D17	riabilitazione	direzione distretto 57	staff direzione
D18	laboratori di analisi chimico-cliniche ex na3	uoc di pertinenza	distretti territoriali, reparti degenza
D19	diagnostica per immagini ex na2	uoc di pertinenza	reparti degenza
D20	sito web aziendale	comunicazione	
D21	diabetologia (piani terapeutici)	coordinamento diabetologia	ambulatori territoriali dei distretti
D22	diabetologia (cartella clinica)	coordinamento diabetologia	ambulatori territoriali dei distretti
D23	lea	coordinamento socio sanitario	distretti e dipartimenti strutturali
D24	adt	direzione p.o.	reparti p.o.
D25	farmaceutica convenzionata esterna	dipartimento di farmacia	ditta esterna di gestione
D26	assistenza domiciliare	coordinamento assistenza domiciliare	ditta esterna di gestione
D27	cartelle cliniche gestione documentale	direzioni sanitarie p.o.	ditta esterna di gestione
D28	cartelle cliniche dipendenze patologiche	dipartimento di dipendenze patologiche	ditta esterna di gestione
D29	cup regionale / aziendale	direzione distretti e presidi ospedalieri;	ambulatori distrettuali ed ospedalieri
D30	credenziali	uoc tecnologie informatiche	
D31	lab. analisi chimico-cliniche ex na3 osped.	uoc di pertinenza	reparti degenza
D32	lab. analisi chimico-cliniche ex na3 TERRIT.	uoc di pertinenza	distretti territoriali
D33	diagnostica per immagini pacs e ris ex na3	uoc di pertinenza	reparti degenza

Descrizione degli strumenti utilizzati:

Le attività informatiche dell'Ente vengono gestite dall'Unità Operativa Complessa "Tecnologie Informatiche e Ingegneria Clinica", attualmente strutturata in:

- Direttore del Servizio
- Dirigenti Amministrativo e Analista informatico
- Collaboratori tecnici
- Assistenti tecnici
- Operatori tecnici-software, forniti da ditte private convenzionate, stabilmente assegnati alla struttura

Gli Uffici di tale UOC e le annesse Sala Macchine costituite da sistemi servers e p.c., sono ubicate:

- al Piano Terra della ex sede Amministrativa ASL NA2 in Via Corrado Alvaro 8, Monteruscello – Pozzuoli(Na)
- al Piano Terra della palazzina sede Direzione Strategica di via Padre Mario Vergara – Frattamaggiore (Na)

Con disposizione del Commissario Straordinario, in data 24 Luglio 2010 è stato istituito il servizio di staff alla Direzione Generale di Management dell'Innovazione Tecnologica nelle cui competenze è stata trasferito il servizio di Gestione della Rete Dati e Fonia Aziendale; tale servizio è strutturato con:

- Collaboratore tecnico
- Operatori tecnici-software, forniti da ditte private convenzionate, stabilmente assegnati alla struttura

Il **Sistema Informativo della ASL Napoli 2 NORD**, oltre che dal Sistema generale, è costituito anche da Gestioni affidate all'esterno, nonché da numerose autonome Gestioni su PC di alcuni Uffici amministrativi e di varie Strutture sanitarie.

Il **Sistema Informativo generale aziendale**, è strutturato in 4 distinte macro-aree applicative:

- **SIA** - Sistema Informativo Amministrativo
- **SIS** - Sistema Informativo Sanitario
- **SID** - Sistema Informativo Direzionale
- **SIT** - Sistema Informativo Telematico

Le quali a loro volta possono essere così suddivise:

SIA

- SottoSistema Economico-Finanziario
- SottoSistema Personale

- SottoSistema Ordini e Magazzini
- SottoSistema Protocollo

SIS

- SottoSistema Anagrafe Assistiti
- SottoSistema Centro Unico Prenotazione ambulatoriali
- SottoSistema Centri Convenzionati (Specialisti – Laboratori – Termalismo)
- SottoSistema Accettazione Dimissione Trasferimenti ospedalieri
- SottoSistema Diagnostica per Immagini
- SottoSistema Laboratori di Analisi
- SottoSistema Farmacie ospedaliere
- SottoSistema Riabilitazione
- SottoSistema Vaccinazioni
- SottoSistema Screening patologie femminili
- SottoSistema Invalidi Civili

SID

- SottoSistema Contabilità analitica e Controllo di Gestione

SIT

- Intranet
- Sito Web
- Accesso ad Internet
- Posta elettronica

Gestioni affidate all'esterno

- SottoSistema Assistenza Domiciliare
- SottoSistema Farmaceutica convenzionata
- Cartelle Cliniche Documentale
- Cartella Cliniche Dipendenze Patologiche
- CUP Regionale

Gestioni autonome su PC

Vari Uffici amministrativi e numerose Strutture sanitarie, trattano dati personali in maniera autonoma al di fuori del Sistema Informativo aziendale istituzionale afferente alla UOC Tecnologie Informatiche.

Infrastruttura di comunicazione

Tutti i Sistemi Informativi sopracitati si poggiano su una Rete Dati costituita da una VPN Virtual Private Network, con protocollo MPLS, gestita attualmente direttamente dalla FASTWEB e dalla TELECOM.

L'Azienda Sanitaria Locale Napoli 2 Nord sta ultimando un cambio "provider" di rete (da Fastweb a Telecom) pertanto vi sono alcune sedi periferiche connesse con la sede di Monteruscello su Fastweb, sulla quale è presente un collegamento in fibra da 50Mb che consente l'accesso centralizzato ad Internet ed al Servizio di Posta Elettronica e che collega anche i Centri convenzionati sul territorio della ex ASL Napoli 2. Le altre sedi periferiche sono connesse con la sede di Frattamaggiore su Telecom la quale è dotata di un sistema avanzato di elaborazione dati (sistema "blade") ed attualmente già centralizza numerose applicazioni e data base, nonché la navigazione internet e il servizio unificato della posta elettronica aziendale. Quando l'attività di cambio "provider" sarà ultimato si centralizzeranno tutti i servizi sulla sede di Frattamaggiore.

Attualmente, una Piattaforma di Sicurezza perimetrale, è preposta al controllo ed al monitoraggio dei collegamenti con l'esterno in entrambi i CED. E' in corso la gestione della sicurezza tramite adesione alla convenzione CONSIP SPC 2 Lotto 2.

Il Sistema Informativo della ASL Napoli 2 NORD è costituito da diverse banche dati localizzate, come indicato in tabella seguente, sul territorio di Pozzuoli e Frattamaggiore. E' in corso la migrazione su cloud per alcuni sotto-sistemi informativi secondo convenzione CONSIP SPC 2 Lotto 1.

Tabella A3 – Descrizione del tipo di trattamento e denominazione / localizzazione banca dati.

Codice	trattamento	denominazione banca dati	ubicazione	nome server
D01	stipendi al personale dipendente	jsipe-jsipedipe-jsec-jsecdipe	sala ced Frattamagg.	SERVER BLADE FUJITSU

Codice	Trattamento	denominazione banca dati	ubicazione	nome server
D02	stipendi al personale convenzionato	jsipeconv-jsipegen, jsecconv-jsecgen	sala ced Frattamagg.	SERVER BLADE FUJITSU
D03	gestione giuridica del personale dipendente	jsipe-jsipedipe-jsec-jsecdipe	sala ced Frattamagg.	SERVER BLADE FUJITSU
D04	rilevazione elettronica presenze del personale	Jobtime e time manager	sala ced Pozzuoli e sala ced Frattam.	p5701 SERVER BLADE FUJITSU
D05	contabilità generale	jsiac2-jsecjsiac	sala ced Frattam.	SERVER BLADE FUJITSU
D06	libera professione (intramoenia)	confina	sala ced Frattam.	SERVER BLADE FUJITSU
D07	magazzini farmacia	Pharmaweb	sala ced Frattam.	SERVER BLADE FUJITSU
D08	protocollo informatico	protocollo	sala ced Frattam.	SERVER BLADE FUJITSU
D09	schede dimissioni ospedaliere	ssi	sala ced Frattam.	SERVER BLADE FUJITSU
D10	database prenotazione ambulatoriali (cup aziendale e cup regionale)	cup	sala ced Frattam.	SERVER BLADE FUJITSU
D11	anagrafe assistiti	anag	sala ced Frattam.	SERVER BLADE FUJITSU
D12	vaccinazioni	geva	sala ced Frattam.	SERVER BLADE FUJITSU
D13	screening patologie femminili	plinius	sala ced Frattam.	SERVER BLADE FUJITSU
D14	invalidi civili	invciv	sala ced Frattam.	SERVER BLADE FUJITSU

Codice	Trattamento	denominazione banca dati	ubicazione	nome server
D15	convenzionamento esterno	cacomm	sala ced Frattam.	SERVER BLADE FUJITSU
D16	termalismo	tecomm	sala ced Frattam.	SERVER BLADE FUJITSU
D17	riabilitazione	gepres	sala ced pozzuoli	p5701 p5702
D18	laboratori di analisi chimico-cliniche ex NA2	Superlab	sala ced Frattam.	SERVER BLADE FUJITSU
D19	diagnostica per immagini ex NA 2	ra2000	sala ced pozzuoli	ra2000 princ ra2000 backup
D20	sito web aziendale	server	server farm aruba spa	
D21	diabetologia (piani terapeutici)	diab	sala ced Frattam.	SERVER BLADE FUJITSU
D22	diabetologia (cartella clinica)	diab	sala ced Frattam.	SERVER BLADE FUJITSU
D23	lea		sala ced Frattam.	SERVER BLADE FUJITSU
D24	adt	ssi	sala ced Frattam.	SERVER BLADE FUJITSU
D25	farmaceutica convenzionata esterna	servizio acquisizione ricette mediche	esterno	
D26	assistenza domiciliare		esterno	
D27	cartelle cliniche gestione documentale		esterno	
D28	cartelle cliniche dipendenze patologiche		esterno	
D29	application prenotazione ambulatoriali (cup aziendale e cup regionale)		sala ced frattamaggiore	SERVER BLADE FUJITSU

Codice	trattamento	denominazione banca dati	ubicazione	nome server
D30	credenziali			SERVER BLADE FUJITSU
D31	laboratori di analisi chimico-cliniche EX NA 3	open lis - omnilab	p.o. san giovanni di dio	hp proliant
D32	laboratori di analisi chimico-cliniche EX NA 3	open lis - omnilab	distretto 41	SERVER BLADE FUJITSU
D33	DIAGNOSTICA PER IMMAGINI ex NA 3	pacs e ris	p.o. san giovanni di dio	Dell
d04	rilevazione elettronica presenze del personale	tmgs	sala ced frattamaggiore	SERVER BLADE FUJITSU
d23	lea		sala ced frattamaggiore	SERVER BLADE FUJITSU
d24	adt		sala ced frattamaggiore	SERVER BLADE FUJITSU
d26	assistenza domiciliare		esterno	
d27	cartelle cliniche gestione documentale		esterno	
d28	cartelle cliniche dipendenze patologiche		esterno	

Tabella A4 - Elenco del personale incaricato del trattamento con accesso alle banche dati.

Nome e Cognome	Profilo	Azienda di Appartenenza
Paolo Quintavalle	Specialista di Sistema Specialista RDBMS	CID Software spa
Paolo Quintavalle	Gestore RDBMS	CID Software spa
<designati>	Specialisti Applicativi	RTI Convenz. CONSIP Lotto 1
<designati>	Specialista Sistema	RTI Convenz. CONSIP Lotto 1
<designati>	Amministratore di Centrale Telefonica e Rete Dati	RTI Convenz. CONSIP SGM e SPC 2 Connettività
Michele Sol	Specialista di Sistema Specialista Piattaforma di Sicurezza	ASL NA2 NORD
Gennaro Buono	Specialista Piattaforma di Sicurezza	ASL NA2 NORD

Per il "Mapping" dei sistemi amministrati e per l'ambito di operatività degli amministratori di sistema, fare riferimento all'allegato "Elenco degli amministratori di sistema ed ambiti di operatività" custoditi presso la UOC Tecnologie Informatiche.

Nota: parte delle indicazioni sono tratte dalla "Guida operativa per redigere il documento programmatico sulla sicurezza (DPS)" pubblicate dal garante

ALLEGATO 2 – Minacce

Minacce a cui sono sottoposte le risorse hardware

Le principali minacce alle risorse hardware sono:

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

Minacce a cui sono sottoposte le risorse connesse in rete

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

- all'utilizzo della LAN/Intranet (interne)
- ai punti di contatto con il mondo esterno attraverso Internet (esterne)
- allo scaricamento di virus e/o trojan per mezzo di posta elettronica e/o alle operazioni di download eseguite tramite il browser (interne/esterne)

In dettaglio si evidenziano le seguenti tecniche:

IP spoofing

L'autore dell'attacco sostituisce la propria identità a quella di un utente legittimo del sistema. Viene fatto non per generare intrusione in senso stretto, ma per effettuare altri attacchi. Lo spoofing si manifesta come attività di "falsificazione" di alcuni dati telematici, come ad esempio di un indirizzo IP o dell'indirizzo di partenza dei messaggi di posta elettronica.

Packet sniffing

Apprendimento di informazioni e dati presenti sulla Rete o su un sistema, tramite appositi programmi. Consiste in un'operazione di intercettazione passiva delle comunicazioni di dati ed informazioni che transitano tra sistemi informatici. In particolare, un aggressore (attacker) può essere in grado di intercettare transazioni di varia natura (password, messaggi di posta elettronica etc.). L'intercettazione illecita avviene con l'ausilio degli sniffer, strumenti che catturano le informazioni in transito per il punto in cui sono installati. Gli sniffer possono anche essere installati su di un computer di un soggetto inconsapevole, in questo caso é possibile che prima dell'installazione dello sniffer, la macchina "obiettivo" sia stata oggetto di un precedente attacco e sia di fatto controllata dall'hacker.

Port scanning

Serie programmata di tentativi di accesso diretti a evidenziare, in base alle "risposte" fornite dallo stesso sistema attaccato, le caratteristiche tecniche del medesimo (e le eventuali vulnerabilità), al fine di acquisire gli elementi per una "intrusione". Trattasi di un vero e proprio studio delle vulnerabilità di un sistema; gli amministratori dei sistemi eseguono spesso questa funzione allo scopo di verificare la funzionalità del medesimo.

Highjacking

Intrusione in una connessione di Rete in corso. In questo modo si colpiscono principalmente i flussi di dati che transitano nelle connessioni point to point. In sostanza l'hacker, simulando di essere un'altra macchina al fine di ottenere un accesso, si inserisce materialmente nella transazione, dopo averne osservato attentamente il flusso. L'operazione é complessa e richiede elevate capacità e rapidità d'azione.

Social engineering

Apprendimento fraudolento da parte degli utenti di sistemi di informazioni riservate sulle modalità di accesso a quest'ultimo.

Buffer overflow

Azioni che tendono a sfruttare eventuali anomalie e difetti di applicazioni che installate in alcuni sistemi operativi, forniscono le funzionalità di "amministratore del sistema", consentendo il controllo totale della macchina. L'hacker, dunque, con tale azione va a sconvolgere la funzionalità di tali programmi, prendendo il controllo della macchina vittima;

Spamming

Saturazione di risorse informatiche a seguito dell'invio di un elevato numero di comunicazioni tali da determinare l'interruzione del servizio. Ad esempio l'invio di molti messaggi di posta elettronica con allegati provoca, come minimo, la saturazione della casella e la conseguente non disponibilità a ricevere ulteriori (veri) messaggi.

Password cracking

Sono programmi che servono per decodificare le password, una volta entrati in possesso del/dei file delle parole d'ordine.

Trojan

Appartengono alla categoria dei virus, di solito sono nascosti in file apparentemente innocui che vengono inconsciamente attivati dall'utente. Permettono, una volta attivati, di accedere incondizionatamente al sistema.

Worm

Appartengono alla categoria dei virus e sono programmi che si replicano attraverso i computer connessi alla rete. In genere consumano una gran quantità di risorse di rete (banda) e di conseguenza possono essere utilizzati per gli attacchi DOS (denial of service) in cui si saturano le risorse di un server o di una rete producendo una condizione di non disponibilità (non funzionamento).

Logic bomb

Appartengono alla categoria dei virus e sono programmi che contengono al proprio interno una funzione diretta a danneggiare o impedire il funzionamento del sistema, in grado di attivarsi autonomamente a distanza di tempo dall'attivazione.

Malware e MMC (Malicious Mobile Code)

Costituiscono la macrocategoria di codici avente come effetto il danneggiamento e l'alterazione del funzionamento di un sistema informativo e/o telematico. In tale categoria sono incluse anche alcune forme di codice ad alta diffusione, quali i virus, i worms ed i trojan horses.

DOS (Denial of Service)

Attacco che mira a saturare le risorse di un servizio, di un server o di una rete.

DDOS (Distributed Denial of Service)

Attacco ripetuto e distribuito che mira a saturare le risorse di un servizio, di un server o di una rete

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

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

Minacce a cui sono sottoposti i dati trattati

Le principali minacce ai dati trattati sono:

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

Minacce a cui sono sottoposti i supporti di memorizzazione

Le principali minacce ai supporti di memorizzazione sono:

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

ALLEGATO 3 – Misure, incident response, ripristino

Le misure logiche di sicurezza (componente logica della sicurezza)

L'aspetto riguardante la componente logica della sicurezza è importante perché garantisce i requisiti di integrità, confidenzialità, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi.

Tale componente è realizzata sia con la prevista ridondanza dei sistemi di esercizio che con l'attivazione di servizi di sicurezza che prevengono l'effetto "dannoso" delle minacce sulle vulnerabilità del sistema informatico ed in particolare con riguardo a:

- identificazione e autenticazione
- autorizzazione
- confidenzialità dei dati
- integrità dei dati
- integrità del flusso dei messaggi
- non ripudio dell'origine (da parte del mittente)
- non ripudio della ricezione (da parte del destinatario)
- audit di sicurezza.

In base alle esigenze rilevate dall'analisi delle minacce e delle vulnerabilità è definita l'architettura informatica di sicurezza che è costituita dall'implementazione di sistemi di firewalling, proxy, antivirus perimetrali e desktop.

Il primo aspetto riguarda la protezione dei dati personali dal rischio di intrusione e dall'azione di programmi di cui all'articolo 615-quinquies del codice penale, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento (comunemente conosciuti come virus).

A tale fine, si sono già installati idonei strumenti elettronici e programmi, che il Dlgs 196/2003 imporrebbe di aggiornare con cadenza almeno semestrale, ma che, in relazione al continuo evolversi dei virus, si è ritenuto opportuno di sottoporre ad aggiornamento continuo al momento stesso della nuova versione di impronte virali.

Tutti gli incaricati saranno istruiti, in merito all'utilizzo dei programmi antivirus e, più in generale, sulle norme di comportamento da tenere, per minimizzare il rischio di essere contagiati: a tale fine, già durante lo scorso anno solare, è stato loro distribuito un codice dei comportamenti da tenere, e di quelli da evitare.

PIATTAFORMA DI SICUREZZA (CED POZZUOLI)

Presso il CED di Pozzuoli è presente un'infrastruttura informatica, denominata "piattaforma di sicurezza", costituita da un sistema hardware e software per la difesa del patrimonio informativo aziendale. La parte software è costituita principalmente da prodotti antivirali per la difesa perimetrale (attacchi virali provenienti dal mondo esterno) e desktop (attacchi virali provenienti dall'interno della rete aziendale).

Gli aggiornamenti delle impronte virali avvengono "on line" e sono disponibili appena il fornitore del software rilascia la nuove release di impronte.

In caso di mancato funzionamento degli antivirus e, quindi, di contagio del sistema si provvederà a:

- isolare il sistema;
- identificare e bonificare il sistema infetto;
- verificare il contagio su altri elaboratori in rete;
- compilare un rapporto di contagio identificando, se possibile, anche la fonte dello stesso.

Il secondo aspetto riguarda la protezione degli elaboratori in rete dall'accesso abusivo, di cui all'articolo 615-ter del codice penale, ai sensi del quale compie tale reato chi si introduce abusivamente in un sistema informatico o telematico, protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo. La protezione da tali accessi avviene mediante l'impiego di idonei strumenti elettronici, comunemente conosciuti come firewall, che il nuovo codice privacy ha reso obbligatoria per i casi in cui si trattino dati sensibili o giudiziari.

La piattaforma di sicurezza oltre agli apparati firewall e sistemi antivirali, include:

- Sistema composto da servers proxy ("url filtering") e software di "content filtering" per l'applicazione delle politiche di sicurezza in osservanza alla normativa vigente in termini di controllo per eventuali abusi della navigazione internet e servizi annessi;
- Sistema composto da servers di "domain controller" basati su "Active Directory" per la centralizzazione degli accessi ai sistemi e per le politiche di assegnazione di credenziali, profilatura delle autenticazioni-autorizzazioni degli utenti aventi diritto, gestione centralizzata dei sistemi client.

L'architettura di autenticazione ed autorizzazione degli utenti del sistema, è basata su caratteristiche tipo:

- unico Login Server per la gestione dei diritti di accesso ai servizi applicativi;
- unico sistema di repository delle credenziali di accesso degli utenti;
- unico database delle anagrafiche contenente tutti i profili di utenza.

PIATTAFORMA DI SICUREZZA (CED FRATTAMAGGIORE)

Per il CED di Frattamaggiore si é adottato un sistema centralizzato antivirale per la difesa interna ed un sistema integrato di antivirus perimetrale, proxy (url filtering) e firewalling per la protezione dagli accessi abusivi di cui all'articolo 615-ter del codice penale.

Gli aggiornamenti delle impronte virali avvengono "on line" e sono disponibili appena il fornitore del software rilascia la nuove release di impronte.

In caso di mancato funzionamento degli antivirus e, quindi, di contagio del sistema si provvederà a:

- isolare il sistema;
- identificare e bonificare il sistema infetto;
- verificare il contagio su altri elaboratori in rete;
- compilare un rapporto di contagio identificando, se possibile, anche la fonte dello stesso.

PROCESSO DI AUTENTICAZIONE ED AUTORIZZAZIONE ALL'ACCESSO

Il processo che si va a descrivere nel seguente paragrafo è quello che interessa tutte le strutture sanitarie integrate in un disegno complessivo ed unitario.

Operativamente per i trattamenti effettuati con strumenti elettronici (elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato), si sono adottate le seguenti misure:

- realizzazione e gestione di un sistema di autenticazione informatica, con tecniche di cifratura, che ha il fine di accertare l'identità delle persone affinché ad ogni strumento elettronico possa accedere solo chi è autorizzato

- realizzazione e gestione di un sistema di autorizzazione, anche con tecniche di cifratura, che ha il fine di circoscrivere le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare a quelli strettamente necessari per lo svolgimento delle proprie mansioni lavorative

Il sistema di autenticazione informatica è adottato per disciplinare gli accessi a tutti gli strumenti elettronici, presenti nell'organizzazione fatta unicamente salva l'eventuale eccezione per quelli che:

- non contengono dati personali
- contengono solo dati personali destinati alla diffusione, che sono quindi per definizione conoscibili da chiunque.

L'eccezione vale, ovviamente, solo per gli strumenti elettronici che non siano in rete, o che siano in rete esclusivamente non contenendo dati personali, o contenenti solo dati personali destinati alla diffusione.

Per tutti gli altri casi, è impostata e gestita una procedura di autenticazione, che permette di verificare l'identità della persona, e quindi di accertare che la stessa è in possesso delle credenziali di autenticazione per accedere ad un determinato strumento elettronico.

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

- si associa un codice per l'identificazione dell'incaricato (username), attribuito da chi amministra il sistema, ad una parola chiave riservata (password), conosciuta solamente dall'incaricato, che provvederà ad elaborarla, mantenerla riservata e modificarla periodicamente, in modo obbligatorio, entro 90 giorni.

Per l'attribuzione e la gestione delle credenziali per l'autenticazione si utilizzano i seguenti criteri:

- ad ogni incaricato vengono assegnate o associate individualmente, per cui non è ammesso che due o più incaricati possano accedere agli strumenti elettronici utilizzando la medesima credenziale.
- nei casi in cui una componente della credenziale di autenticazione è costituita dal codice per l'identificazione (username), attribuito all'incaricato da chi amministra il sistema, tale codice deve essere univoco: esso non può essere assegnato ad altri incaricati, neppure in tempi diversi.

- sarà ammesso che, qualora sia necessario o comunque opportuno, che ad una persona venga assegnata più di una credenziale di autenticazione.

Al verificarsi dei seguenti casi, è prevista la disattivazione delle credenziali di autenticazione:

- immediatamente, nel caso in cui l'incaricato perda la qualità (funzione), che gli consentiva di accedere allo strumento
- in ogni caso, entro sei mesi di mancato utilizzo, con l'unica eccezione delle credenziali che sono state preventivamente autorizzate per soli scopi di gestione tecnica, il cui utilizzo è quindi sporadico.

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

- dovere di custodire i dispositivi, attribuiti agli incaricati a titolo di possesso ed uso esclusivo, con i quali si può accedere agli strumenti informatici (ad esempio, il tesserino magnetico o la smart card): la custodia deve avvenire in modo diligente, sia nell'ipotesi in cui tali dispositivi siano riposti negli uffici (viene prescritto l'obbligo di utilizzare cassetti con serratura), che in quella in cui l'incaricato provveda a portare il dispositivo con sé (viene prescritto l'obbligo di custodirlo come se fosse una carta di credito). In ipotesi di smarrimento, l'incaricato deve provvedere immediatamente a segnalare la circostanza all'amministratore di sistema, o alle altre persone che sono state a tale fine indicate, al momento dell'attribuzione del dispositivo
- obbligo di non lasciare incustodito e accessibile lo strumento elettronico, durante una sessione di trattamento, neppure in ipotesi di breve assenza
- dovere di elaborare in modo appropriato la password, e di conservare la segretezza sulla stessa, nonché sulle altre componenti riservate della credenziale di autenticazione (username), attribuite dall'amministratore di sistema. Agli incaricati è imposto l'obbligo di provvedere a modificare la password, con la seguente tempistica:
  - immediatamente, non appena viene consegnata loro da chi amministra il sistema
  - successivamente, almeno ogni sei mesi. Tale termine scende a tre mesi, se la password dà accesso ad aree in cui sono contenuti dati sensibili o giudiziari.

Le password saranno composte da almeno otto caratteri.

Agli incaricati sarà prescritto di utilizzare alcuni accorgimenti, nell'elaborazione delle password quali:

- non devono contenere riferimenti agevolmente riconducibili all'interessato (non solo nomi, cognomi, soprannomi, ma neppure date di nascita proprie, dei figli o degli amici), né consistere in nomi noti, anche di fantasia (pippo, pluto, paperino,....)
- buona norma è che, dei caratteri che costituiscono la password, da un quarto alla metà siano di natura numerica.
- la password non deve essere comunicata a nessuno (non solo a soggetti esterni, ma neppure a persone appartenenti all'organizzazione, siano esse colleghi, responsabili del trattamento, amministratore del sistema o titolare).

Per quanto concerne le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, si è impostato un sistema di autorizzazione, al fine di circoscrivere le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, a quelli strettamente necessari per lo svolgimento delle proprie mansioni lavorative. L'unica eccezione si ha nei casi in cui il trattamento riguardi solo dati personali destinati alla diffusione: in questo caso non è necessario predisporre alcun sistema di autorizzazione, poiché i dati trattati sono, per definizione, conoscibili da chiunque.

Al di fuori di questi casi, le autorizzazioni all'accesso verranno rilasciate e revocate dal titolare e, se designato, dal responsabile, ovvero da soggetti da questi appositamente incaricati.

Il profilo di autorizzazione è studiato per classi omogenee di incaricati (ad esempio, attribuendo un determinato profilo di autorizzazione a tutti gli impiegati della contabilità, ed attribuendone un altro a coloro che lavorano nell'ufficio personale). L'obiettivo di fondo, in ogni caso, è di limitare preventivamente l'accesso, di ciascun incaricato o di ciascuna classe omogenea di incaricati, ai soli dati necessari per effettuare le operazioni di trattamento, che sono indispensabili per svolgere le mansioni lavorative.

Periodicamente, e comunque almeno semestralmente, dovrà essere verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione: ciò per quanto riguarda l'ambito di trattamento consentito sia ai singoli incaricati, che agli addetti alla manutenzione e gestione degli strumenti elettronici.

Per quanto concerne i supporti rimovibili (es. floppy disk, dischi ZIP, CD....), contenenti dati personali, la norma impone particolari cautele solo nell'ipotesi in cui essi contengano dati sensibili o giudiziari e pertanto la nostra proposta ha

ritenuto di estendere tali precetti ai supporti contenenti dati personali di qualsiasi natura, anche comune, prescrivendo agli incaricati del trattamento quanto segue:

- i supporti dovranno essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: in particolare, essi saranno conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi
- una volta cessate le ragioni per la conservazione dei dati, si devono in ogni caso porre in essere gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati contenuti nei supporti. Tali dati devono quindi essere cancellati, se possibile, e si deve arrivare addirittura a distruggere il supporto, se necessario per i fini in esame.

Le misure logiche di sicurezza, di cui si doterà il Titolare per la protezione dei trattamenti che avvengono con strumenti elettronici saranno pertanto nel loro complesso soddisfacenti, al fine di garantire la necessaria sicurezza ai dati personali trattati.

LA PROTEZIONE DEL CENTRO SERVIZI (COMPONENTE INFRASTRUTTURALI DELLA SICUREZZA)

Per riportare la completezza delle misure che sono state adottate si ricorda che il Centro Elaborazione Dati è dotato dei seguenti impianti:

- Antincendio (mediante estintori)
- luci di emergenza,
- di continuità elettrica (con gruppi di continuità e gruppo elettrogeno)
- controlli accessi e varchi fisici (il SED è in locale chiuso con porte in ferro).

Che completano le misure che rappresentano la componente infrastrutturale della sicurezza.

RIEPILOGO DELLE CONTROMISURE ADOTTATE.

Vigilanza armata, gruppo elettrogeno, armado ignifugo,	Eventi relativi al contesto	Tutti quelli presenti in sala server	Piano di Disaster Recovery, vigilanza, gruppo		RTI in gestione, Direzione Generale, ufficio tecnico

porte blindate			elettrogeno , Armadio ignifugo, porte blindate		
Formazione operatori	Comportamento errato degli operatori	Tutti quelli gestiti da operatori interni ed esterni alla ASL	Formazione	Formazione	SED Pozzuoli
Determinazione ed aggiornamento delle policy di sicurezza	Eventi relativi agli strumenti	Tutti quelli presenti sui server	Politica sui firewall,		SED Pozzuoli

SALVATAGGIO E RIPRISTINO DEI DATI.

Per fronteggiare le ipotesi in cui i dati siano colpiti da eventi che possano danneggiarli, o addirittura distruggerli, sono previsti criteri e modalità tali, da garantire il loro ripristino in termini ragionevoli, e comunque entro una settimana per i dati sensibili e giudiziari.

Per i dati trattati con strumenti elettronici, sono previste procedure di backup, attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema su sistemi di storage composti da batterie di hard disk.

Il salvataggio dei dati trattati avviene con le seguenti modalità:

- la frequenza sarà giornaliera.
- sarà effettuato un salvataggio mensile che storicizzerà le situazioni
- si utilizzeranno supporti differenti, da quelli in cui sono contenuti i dati dei salvataggi eseguiti la volta precedente
- per ciascun salvataggio, si eseguirà 1 copia.

Le copie sono/saranno custodite:

- presso il locale sala server della Direzione del Servizio Informatico
- su CLOUD del Centro Servizi della società RTI capofila Telecom appartenente alla convenzione CONSIP SPC 2 Lotto 1 che gestisce i sistemi informatici della ASL (in modo da realizzare un Disaster Recovery).

L'accesso ai supporti utilizzati per il back up dei dati è limitato per ogni banca dati a:

- Responsabile del trattamento della sicurezza dei dati;
- Responsabile del trattamento;
- Incaricato;
- Amministratore di sistema.

Tabella B1 – Tipologie di salvataggio – Banche DATI CED FRATTAMAGG./POZZUOLI

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
JSIPE	automatico	RTI	Q	C3	M2	L4	S2	L,F
JSIPEDIPE								
JSIPEGEN	automatico	RTI	Q	C3	M2	L4	S2	L,F
JSIPECONV	automatico	RTI	Q	C3	M2	L4	S2	L,F
JSEC	automatico	RTI	Q	C3	M2	L4	S2	L,F
JSECCONV	automatico	RTI	Q	C3	M2	L4	S2	L,F
JSECDIPE	automatico	RTI	Q	C3	M2	L4	S2	L,F
JSECGENE	automatico	RTI	Q	C3	M2	L4	S2	L,F
JSECJSIAC	automatico	RTI	Q	C3	M2	L4	S2	L,F
JSIAC2	automatico	RTI	Q	C3	M2	L4	S2	L,F
JOBTIME	automatico	RTI	Q	C3	M2	L4	S2	L,F
CONFINA	automatico	RTI	Q	C3	M2	L4	S2	L,F
PROTOCOLLO	automatico	RTI	Q	C3	M2	L4	S2	L,F
ADT	automatico	RTI	Q	C3	M2	L4	S2	L,F

GEVA	automatico	RTI	Q	C3	M2	L4	S2	L,F
PLINIUS	automatico	RTI	Q	C3	M2	L4	S2	L,F
INVCIV	automatico	RTI	Q	C3	M2	L4	S2	L,F
CACOMMM	automatico	RTI	Q	C3	M2	L4	S2	L,F
TECOMM	automatico	RTI	Q	C3	M2	L4	S2	L,F
COSPER	automatico	RTI	Q	C3	M2	L4	S2	L,F
Laboratorio Analisi	automatico	RTI	Q	C3	M1	L4	S2	L,F
RA2000	Automatico	Siemens	Q	C4 C3	M2	L4	S2	L,F
DIAB	Automatico	RTI	Q	C3	M2	L4	S2	L,F
MONLEA	Automatico	RTI	Q	C3	M2	L4	S2	L,F
SANITA *(ANAGRAFE UNIFICATA)*	Automatico	RTI	Q	C3	M2	L4	S2	L,F
SANITA *(ANAGRAFE EX ASL NA2 + CUP)*	Automatico	RTI	Q	C3	M2	L4	S2	L,F
CREDENZIALI DI DOMINIO	Automatico	RTI	Q	C3	M2	L4	S2	L,F

Nella lettura della tabella valgono i seguenti acronimi:

- IS = Incaricato Salvataggio
- IV = Incaricato Verifica
- Po = Periodicità
- Pe = Protezione
- LC = Luogo Custodia
- CS = Criterio Salvataggio

Criterio di salvataggio:

- C1= 2 supporti rimovibili a giorni alterni
- C2= 7 supporti rimovibili dal Lunedì alla Domenica
- C3= FTP su disco remoto
- C4= copia su disco Server di BackUp
- C5= 5 supporti rimovibili dal Lunedì al Venerdì
- C6=1 supporto rimovibile saltuario
- C7 sovrascrittura

Luogo custodia (LC):

- L1 = Armadio Ignifugo SED
- L2 = Studio del primario
- L3 = Armadio
- L4 = Server

Supporto:

- S1 = Nastro magnetico
- S2 = Hard disk

Protezione (Pe)

- M1 = Copia cifrata e dotata di password
- M2 = Copia non protetta

Periodicità (Po)

- Q = quotidiana
- V = variabile

Modalità di Backup

- L = Logico
- F = Fisico

REGISTRAZIONE CENTRALIZZATA DEGLI ACCESSI AI SISTEMI

E' stato implementato una soluzione per la raccolta centralizzata dei LOG dei vari sistemi grazie all'adesione della convenzione CONSIP SPC 2 Lotto 2 Sicurezza al fine di consentire una facile lettura dei dati e la loro ottimale gestione, come prescritto dalla normativa vigente (provvedimento del Garante del 27711/2008). Tale archiviazione avviene tramite collegamento remoto persistente (MPLS) su cloud gestito dalla società capofila Leonardo.

Questa soluzione consente di monitorare gli eventi e chi li ha compiuti ottemperando così agli obblighi derivanti dal Provvedimento del Garante del 27/11/2008 relativamente all'assegnazione individuale delle credenziali di amministratore di sistema.

DATI IN OUTSOURCING.

Per i casi in cui i trattamenti di dati personali sono affidati, in conformità a quanto previsto dal Dlgs 196/2003, all'esterno della struttura del Titolare, si adotteranno i seguenti criteri, atti a garantire che il soggetto destinatario adotti misure di sicurezza conformi a quelle minime, previste dagli articoli da 33 a 35 Dlgs 196/2003 e dal disciplinare tecnico, allegato sub b) al codice.

Per la generalità dei casi, in cui il trattamento di dati personali, di qualsiasi natura, venga affidato all'esterno della struttura del titolare, sono impartite istruzioni per iscritto al terzo destinatario, di rispettare quanto prescritto per il trattamento dei dati personali:

- dal Dlgs 196/2003, se il terzo destinatario è italiano
- dalla direttiva 95/46/CE , se il terzo destinatario non è italiano.

In ogni caso, al soggetto cui le attività sono affidate sarà richiesta la seguente dichiarazione:

- di essere consapevole che i dati che tratterà, nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali, sono soggetti all'applicazione della normativa per la protezione dei dati personali
- di ottemperare agli obblighi previsti dalla normativa per la protezione dei dati personali
- di attenersi alle istruzioni specifiche, eventualmente ricevute per il trattamento dei dati personali, conformando ad esse anche le procedure eventualmente già in essere
- di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate, e di avvertire immediatamente il proprio committente in caso di situazioni anomale o di emergenze

- di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.
- di indicare gli Amministratori di Sistema ai sensi del provvedimento del garante del 27/11/2008
- di registrare gli accessi ai sistemi da parte degli Amministratori di Sistema come previsto dal richiamato provvedimento del Garante e conservarli almeno per mesi 6 consentendo all'amministrazione l'eventuale analisi

Per il trattamento affidato all'esterno dei dati sensibili o giudiziari, si procederà alla stipula di clausole contrattuali, con il destinatario, che disciplinano gli aspetti legati alla gestione dei dati personali.

Nei casi in cui ciò si renda opportuno, per ragioni operative legate anche alla tutela dei dati personali, il destinatario esterno viene nominato dal Titolare come responsabile del trattamento dei dati, mediante apposita lettera scritta.

Per le attività svolte in outsourcing vale la seguente tabella.

Tabella B2 – Soggetti delegati e criteri

Data trattamento	Trattamenti	Soggetto Delegato	Ruolo del Soggetto	Criteri e impegni assunti per l'adozione delle misure
Anno corrente	Assistenza Domiciliare	MEDICASA	Società	Nessuna
Anno corrente	Farmaceutica Convenzionata	CEDOCA	Società	Contrattuale
Anno corrente	Cartelle Cliniche Documentali	Progetto 2000	Società	Nessuna
Anno corrente	Cartella Cliniche Dipendenze Patologiche	CRED Regione Campania	ENTE	Nomina DG
Anno corrente	CUP Regionale	Telecom	Società	Nessuna

ATTIVITÀ DI CONTROLLO E VERIFICA.

Al Responsabile per la sicurezza sarà affidato il compito di aggiornare le misure di sicurezza, al fine di adottare gli strumenti e le conoscenze, resi disponibili dal progresso tecnico, che consentano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito.

A tale fine, sarà previsto che :

- ogni 6 mesi si effettui una riunione del responsabile per la sicurezza con il Titolare o con gli eventuale membri che questi dovesse ritenere di coinvolgere, durante la quale il responsabile renderà conto della situazione
- al fine di verificare l'efficacia delle misure di sicurezza adottate, il responsabile per la sicurezza e le persone da questo appositamente incaricate provvederanno con frequenza bimestrale, anche con controlli a campione, ad effettuare una o più delle seguenti attività:
  - verificare l'accesso fisico ai locali dove si svolge il trattamento
  - verificare la correttezza delle procedure di archiviazione e custodia di atti, documenti e supporti contenenti dati personali
  - monitorare l'efficacia ed il corretto utilizzo delle misure di sicurezza adottate per gli strumenti elettronici, mediante l'analisi dei log file, nei quali i software di sicurezza installati, i sistemi operativi e le applicazioni scrivono le operazioni svolte dagli incaricati per il loro tramite. Attraverso questa analisi, che viene effettuata adottando strumenti automatici di reportistica e di sintesi, è possibile individuare i tentativi, riusciti o meno, di accesso al sistema e l'esecuzione di operazioni non corrette, o sospette
  - verificare l'integrità dei dati e delle loro copie di backup
  - verificare la sicurezza delle trasmissioni in rete
  - verificare che i supporti magnetici, che non possono più essere riutilizzati, vengano distrutti
  - verificare il livello di formazione degli incaricati
- Almeno ogni sei mesi, si procederà ad una sistematica verifica del corretto utilizzo delle parole chiave e dei profili di autorizzazione che consentono l'accesso agli strumenti elettronici da parte degli incaricati, anche al fine di disabilitare quelli che non sono stati mai utilizzati in sei mesi. Dell'attività di verifica svolta sarà redatto un verbale, che viene conservato dal Titolare e allegato al Documento programmatico sulla sicurezza).

ORGANIZZAZIONE PER IL TRATTAMENTO.

L'organizzazione è stata fissata con apposita delibera del D.G. e sarà eventualmente rivista sempre con delibera del Direttore Generale.

Per quanto attiene al Gestore delle Credenziali si è stabilito che lo stesso tenga traccia solo delle credenziali (user-id) identificativi della persona e profili di appartenenza.

Le Password degli amministratori di sistema ai sensi della provvedimento del Garante del 27/11/2008 sono nominative e pertanto come quelle di carattere applicativo sono affidate ai singoli utenti e non possono essere note ad altri utenti in quanto, una volta assegnate, sono modificate dall'utente al primo collegamento.

E' conservato a cura del Responsabile della UOC Tecnologie Informatiche le solo password degli utenti generici di Amministrazione di Sistema e banche dati (Root ed Administrator) al fine di consentire di intervenire in casi di assenza degli Amministratori nominati. Azioni Programmate per il 2018

Le azioni programmate per il contenimento dei rischi e la diffusione della cultura della sicurezza ed il rispetto delle norme e procedure in materia sono:

A. completamento del processo di unificazione delle infrastrutture e dei sistemi informativi delle due ex ASL
B. conseguente unificazione dei processi e delle procedure in materia
    - unica piattaforma di sicurezza
    - completamento dell'inserimento in dominio dei PC aziendali
    - unificazione dei servizi applicativi e di accesso ad Internet/mail
    - migrazione di alcuni sistemi informativi su CLOUD
C. Erogazione dei Corsi di formazione come indicato nel paragrafo successivo

EROGAZIONE CORSI DI FORMAZIONE.

Si reiterano i corsi previsti per lo scorso anno.

CORSO P01

- Docente : Esperto, da designarsi da parte della Direzione Generale
- Destinatari : Direttori UOC, sia amministrativi che sanitari
- Date : da stabilirsi
- Durata : 4 ore complessive, su 1 incontro
- Contenuti : Principi generali
  Diritti delle persone
  Regole generali per il trattamento di tutti i dati personali
  Regole ulteriori per i soggetti pubblici
  Misure minime di sicurezza
  Trattamenti dei dati personali in ambito sanitario
- Obbiettivi : al termine del corso, i partecipanti dovrebbero aver preso conoscenza dei punti principali della vigente normativa

sulla privacy, con particolare riferimento al Sistema delle responsabilità individuali ed al Sistema di gestione aziendale della problematica generale.

CORSO P02

- Docente : Esperto , da designarsi da parte della Direzione Generale
- Destinatari : gli incaricati dei trattamenti dati, sia amministrativi che sanitari
- Date : da stabilirsi
- Durata : 8 ore complessive, su 2 incontri
- Contenuti : Principi generali
  Diritti delle persone
  Regole generali per il trattamento di tutti i dati personali
  Regole ulteriori per i soggetti pubblici
  Misure minime di sicurezza
  Trattamenti dei dati personali in ambito sanitario
  Modalità tecniche relative alla gestione di User-id e password, Antivirus, Back- Up
- Obbiettivi : al termine del corso, i partecipanti dovrebbero aver preso conoscenza dei punti principali della vigente normativa sulla privacy, con particolare riferimento al Sistema delle responsabilità individuali ed al Sistema di gestione aziendale della problematica generale, nonché delle modalità operative per garantire livelli minimi di sicurezza.

REGOLE PER LA GESTIONE DI STRUMENTI ELETTRONICO/INFORMATICO

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

- l'accesso agli incaricati ed agli addetti alla manutenzione è possibile solo in seguito ad autorizzazione scritta;

- gli hard disk non sono condivisi in rete se non temporaneamente per operazioni di copia;
- tutte le operazioni di manutenzione che sono effettuate on-site avvengono con la supervisione dell'incaricato del trattamento o di un suo delegato;
- le copie di backup dei data base sono realizzate su HD in storage protetto dall'accesso fisico/logico non autorizzato;
- divieto di utilizzare supporti rimovibili come mezzo per il backup;
- divieto per gli utilizzatori di strumenti elettronici di lasciare incustodito, o accessibile, lo strumento elettronico stesso. A tale riguardo, per evitare errori e dimenticanze, è adottato uno screensaver automatico dopo 10 minuti di non utilizzo, con ulteriore password segreta per la prosecuzione del lavoro.
- divieto di memorizzazione di archivi con dati sensibili di carattere personale dell'utente sulla propria postazione di lavoro non inerenti alla funzione svolta;
- divieto di installazione di software di qualsiasi tipo sui personal computer che contengono archivi con dati sensibili senza apposita autorizzazione scritta da parte del responsabile del trattamento dati;
- divieto di installazione sui personal computer di accessi remoti di qualsiasi tipo mediante modem e linee telefoniche.

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

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

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

REGOLE DI COMPORTAMENTO PER MINIMIZZARE I RISCHI DA VIRUS

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

- divieto di lavorare con diritti di amministratore o superutente sui sistemi operativi che supportano la multiutenza;
- limitare lo scambio fra computer di supporti rimovibili (cd, zip) contenenti file con estensione EXE, COM, OVR, OVL, SYS, DOC , XLS;

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

- conservare i driver delle periferiche (stampanti, schede di rete, monitor ecc. fornite dal costruttore).

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

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

INCIDENT RESPONSE E RIPRISTINO

Tutti gli incaricati del trattamento dei dati devono avvisare tempestivamente il responsabile della sicurezza informatica o l'amministratore di sistema o il responsabile del trattamento dei dati, nel caso in cui constatino le seguenti anomalie:

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

In caso di incidente sono considerate le seguenti priorità:

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

Garantita l'incolumità fisica alle persone si procedere a:

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

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

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

- eseguire una copia bit to bit degli hard disk del sistema compromesso;
- se l'incidente riguarda i dati il restore dei dati può avvenire sulla copia di cui al punto 1 precedente a partire dalle ultime copie di backup ritenute valide;
- se l'incidente riguarda il sistema operativo o esiste la possibilità che sia stato installato software di tipo MMC (vedere Allegato 2) il ripristino deve essere effettuato reinstallando il sistema operativo su nuovo supporto.

ALLEGATO 4 - Regolamento per l'utilizzo della rete

OGGETTO E AMBITO DI APPLICAZIONE

Il presente regolamento disciplina le modalità di accesso e di uso della rete informatica e telematica e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire.

PRINCIPI GENERALI – DIRITTI E RESPONSABILITÀ

Azienda Sanitaria Locale Napoli 2 Nord promuove l'utilizzo della rete quale strumento utile per perseguire le proprie finalità.

Gli utenti manifestano liberamente il proprio pensiero nel rispetto dei diritti degli altri utenti e di terzi, nel rispetto dell'integrità dei sistemi e delle relative risorse fisiche, in osservanza delle leggi, norme e obblighi contrattuali.

Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina.

Il posto di lavoro costituito da personal computer viene consegnato completo di quanto necessario per svolgere le proprie funzioni, pertanto è vietato modificarne la configurazione.

Il software installato sui personal computer è quello richiesto dalle specifiche attività lavorative dell'operatore. E' pertanto proibito installare qualsiasi programma da parte dell'utente o di altri operatori, escluso l'amministratore del sistema. L'utente ha l'obbligo di accertarsi che gli applicativi utilizzati siano muniti di regolare licenza.

Ogni utente è responsabile dei dati memorizzati nel proprio personal computer. Per questo motivo è tenuto ad effettuare la copia di questi dati secondo le indicazioni emanate dal titolare del trattamento dei dati o suo delegato.

ABUSI E ATTIVITÀ VIETATE

E' vietato ogni tipo di abuso. In particolare è vietato:

- usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da quanto previsto dal presente regolamento;
- utilizzare la rete per scopi incompatibili con l'attività istituzionale;
- utilizzare una password a cui non si è autorizzati;
- cedere a terzi codici personali (USER ID e PASSWORD) di accesso al sistema;
- conseguire l'accesso non autorizzato a risorse di rete interne o esterne;
- violare la riservatezza di altri utenti o di terzi;

- agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti;
- agire deliberatamente con attività che distraggano risorse (persone, capacità, elaboratori);
- fare o permettere ad altri, trasferimenti non autorizzati di informazioni (software, basi dati, ecc.);
- installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (p.e. virus, cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing - p2p);
- installare o eseguire deliberatamente programmi software non autorizzati e non compatibili con le attività istituzionali;
- cancellare, disinstallare, copiare, o asportare deliberatamente programmi software per scopi personali;
- installare deliberatamente componenti hardware non compatibili con le attività istituzionali;
- rimuovere, danneggiare deliberatamente o asportare componenti hardware.
- utilizzare le risorse hardware e software e i servizi disponibili per scopi personali;
- utilizzare le caselle di posta elettronica per scopi personali e/o non istituzionali;
- utilizzare la posta elettronica con le credenziali di accesso di altri utenti;
- utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi.
- utilizzare l'accesso ad Internet per scopi personali;
- accedere direttamente ad Internet con modem collegato al proprio Personal Computer se non espressamente autorizzati e per particolari motivi tecnici;
- connettersi ad altre reti senza autorizzazione;
- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere copiare o cancellare file e software di altri utenti, senza averne l'autorizzazione esplicita;
- usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete;
- inserire o cambiare la password del bios, se non dopo averla espressamente comunicata all'amministratore di sistema e essere stati espressamente autorizzati;
- abbandonare il posto di lavoro lasciandolo incustodito o accessibile, come specificato nell'allegato 3.

ATTIVITÀ CONSENTITE

E' consentito all'amministratore di sistema:

- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei client e degli applicativi, per copiare o rimuovere file e software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- creare, modificare, rimuovere o utilizzare qualunque password, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori. L'amministratore darà comunicazione dell'avvenuta modifica all'utente che provvederà ad informare il custode delle password come da procedura descritta nell'allegato 3;
- rimuovere programmi software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- rimuovere componenti hardware, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

SOGGETTI CHE POSSONO AVERE ACCESSO ALLA RETE

Hanno diritto ad accedere alla rete tutti i dipendenti, le ditte fornitrici di software per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione.

L'accesso alla rete è assicurato compatibilmente con le potenzialità delle attrezzature.

L'amministratore di sistema può regolamentare l'accesso alla rete di determinate categorie di utenti, quando questo è richiesto da ragioni tecniche.

Per consentire l'obiettivo di assicurare la sicurezza e il miglior funzionamento delle risorse disponibili, l'amministratore di sistema può proporre al titolare del trattamento l'adozione di appositi regolamenti di carattere operativo che gli utenti si impegnano ad osservare.

L'accesso agli applicativi è consentito agli utenti che, per motivi di servizio, ne devono fare uso.

MODALITÀ DI ACCESSO ALLA RETE E AGLI APPLICATIVI

Qualsiasi accesso alla rete e agli applicativi viene associato ad una persona fisica cui collegare le attività svolte utilizzando il codice utente.

L'utente che ottiene l'accesso alla rete e agli applicativi si impegna ad osservare il presente regolamento e le altre norme disciplinanti le attività e i servizi che si svolgono via rete ed si impegna a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi.

L'utente che ottiene l'accesso alla rete e agli applicativi si assume la totale responsabilità delle attività svolte tramite la rete.

L'utente è tenuto a verificare l'aggiornamento periodico del software antivirus.

Al primo collegamento alla rete e agli applicativi, l'utente deve modificare la password (parola chiave) comunicatagli dal custode delle password e rispettare le norme indicate nell'allegato 3.

SANZIONI

In caso di abuso, a seconda della gravità del medesimo, e fatte salve ulteriori conseguenze di natura penale, civile e amministrativa, possono essere comminate le sanzioni disciplinari previste dalla normativa vigente in materia e dai regolamenti interni.

ALLEGATO 5 – Utilizzo del proxy

UTILIZZO DEL PROXY

L'utilizzo del proxy riguarda le misure procedurali relative all'identificazione e all'autenticazione degli utenti, le regole di utilizzo delle risorse hardware e software, le norme comportamentali e le responsabilità di ciascuno. Rientrano in questo aspetto le norme di comportamento interno per limitare l'uso privato di e-mail o Internet, in quanto i controlli sono possibili solo a determinate condizioni e con l'accordo delle rappresentanze sindacali unitarie. Si ricorda che il D.L.vo 196/03 (Codice in materia di protezione dei dati personali) ribadisce quanto dettato dall'art. 4 dello Statuto dei Lavoratori, ovvero il "... divieto di utilizzo da parte del datore di lavoro di apparecchiature atte al controllo a distanza dell'attività del lavoratore, salvo che esigenze organizzative, produttive o di sicurezza non abbiano determinato, previo accordo con le rappresentanze sindacali, la lecita introduzione in azienda". D'altro canto la consultazione di siti web da parte del lavoratore o l'utilizzo di posta elettronica durante il normale orario di lavoro non è consentita quando tale attività non sia pertinente con le mansioni affidate, come l'art. 1024 del codice civile prevede nel principio generale di diligenza del lavoratore. Per trovare un punto di equilibrio dei diritti del lavoratore è opportuno introdurre una policy trasparente e codificata con l'apporto dei lavoratori, dando anche la possibilità al datore di lavoro di prevedere meccanismi sanzionatori, sempre che la policy sia resa accessibile a tutti i lavoratori, come previsto dall'art. 7 dello Statuto dei Lavoratori. Sempre tra le politiche di sicurezza si può fare riferimento alle responsabilità civili e penali per i danni cagionati con il trattamento dei dati personali. A titolo di esempio si possono elencare:

- la responsabilità civile disciplinata dall'art. 2050 del Codice Civile e art. 15 D.Lgs. 196/03 "chi cagiona danno ad altri per effetto del trattamento dei dati personali è tenuto a risarcire il danno, a meno che non provi di aver adottato tutte le misure idonee per evitarlo";
- la sanzione penale che colpisce chi, essendovi tenuto, omette di adottare le misure di sicurezza (art. 169 del D.Lgs. 196/03), pari all'arresto fino a due anni o ad ammenda da 10mila a 50mila euro, ma con estinzione del reato in caso di regolarizzazione entro 6 mesi dall'accertamento del reato e pagamento di somma determinata dal Garante.

Le informazioni e le attività eseguite sulla rete informatica e telematica relative agli utilizzatori, sono registrate e conservate su file (registro elettronico delle attività o file di log).

Tali file possono essere soggetti ad indagini, nel rispetto di quanto sancito dal D.L.vo 30 giugno 2003, n. 196. Inoltre, il responsabile per la sicurezza può accedere ai file degli utilizzatori per proteggere l'integrità dei sistemi informatici.

Per il regolamento d'uso della rete (policy) vedere l'Allegato 4.