SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Regione Emilia Romagna

AZIENDA UNITA' SANITARIA LOCALE DI PARMA
Strada del Quartiere n. 2/a − Parma

* * * * *

VERBALE DELLE DELIBERAZIONI
DEL DIRETTORE GENERALE

Deliberazione assunta il 28/10/2015 N.697

Proposta n. 19203
Ufficio/Servizio proponente: DIREZIONE AMMINISTRATIVA

OGGETTO

AGGIORNAMENTO DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DI CUI ALL'ALLEGATO B DEL D.L.VO 30/06/03 N. 196 "CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI": ANNO 2015.

Il giorno 28/10/2015 alle ore 09:30 nella sede dell'Azienda Unità Sanitaria Locale di Parma − Strada del Quartiere n.2/a − Parma, il Direttore Generale, sentiti il Direttore Amministrativo e il Direttore Sanitario, ha adottato l'atto in oggetto specificato.

OGGETTO: AGGIORNAMENTO DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DI CUI ALL'ALLEGATO B DEL D.L.VO 30/06/03 N. 196 "CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI": ANNO 2015.

IL DIRETTORE GENERALE

DATO ATTO che, con deliberazione n.° 166 del 31 marzo 2006 è stato approvato il documento programmatico sulla sicurezza, redatto ai sensi degli artt. 33 e seguenti e dell'allegato B del D.Lgs 30.06.2003 n. 196 "Codice in materia di protezione dei dati personali";

RILEVATO che il punto 19 dell'allegato B sopra citato prevede che entro il 31 marzo di ogni anno, il titolare del trattamento di dati sensibili e/o giudiziari rediga un documento programmatico sulla sicurezza contenente idonee informazioni riguardo a:

a) l'elenco dei trattamenti;
b) la distribuzione dei compiti e delle responsabilità;
c) l'analisi dei rischi a cui possono essere soggetti i dati trattati;
d) le misure da adottare per garantire l'integrità e la protezione;
e) i criteri e le modalità di ripristino dei dati in corso di danneggiamento e distribuzione;
f) la formazione per gli incaricati dei trattamenti;
g) i criteri per le misure di sicurezza per i dati il cui trattamento è affidato a soggetti esterni alla struttura del titolare;
h) i criteri adottati per la cifratura e/o la separazione di dati personali dai dati idonei a rivelare lo stato di salute e la vita sessuale;

PRESO ATTO CHE il D.L. n° 5 del 2012, convertito nella legge 4 aprile 2012 n° 35, all'art. 45 dispone la soppressione della lettera g) dell'art. 34, comma 1 del Codice della privacy ossia, per il trattamento dei dati con strumenti elettronici, non è più necessaria la tenuta di un aggiornato documento programmatico sulla sicurezza;

RILEVATO PERO' che la succitata norma (non obbligatorietà dell'adozione del Documento Programmatico sulla Sicurezza) non abroga l'adozione delle misure di sicurezza per cui il Titolare del trattamento deve ridurre i rischi che incombono sui dati; il Titolare mantiene in capo a sé gli obblighi relativi alle misure di sicurezza di cui agli artt. 33 e seguenti ed all'allegato B; non sono state abrogate le sanzioni amministrative e penali nonché l'obbligo del Titolare di dimostrare di aver fatto tutto il necessario per evitare che il danno accadesse;

VISTA la deliberazione n° 240 del 23/04/2014 con la quale è stato approvato l'aggiornamento per l'anno 2014 del Documento programmatico per la sicurezza di cui all'allegato B del D.Lgs 30.06.2003 n° 196 "Codice in materia di protezione dei dati personali";

RITENUTO PERTANTO, alla luce di quanto sopra esposto, di continuare ad approvare l'aggiornamento DPS in modo da dare evidenza alle attività svolte ed alla diligenza posta nella predisposizione delle misure minime di sicurezza e quindi di tutti gli atti possibili ad evitare danni derivanti dal trattamento dei dati personali;

ATTESO che gli articoli da 33 a 35 del D.Lgs 30.06.2003 n° 196 "Codice in materia di protezione dei dati personali" disciplinano l'adozione delle misure minime per il trattamento dei dati sia con l'ausilio che senza l'ausilio di strumenti elettronici;

DATO ATTO che nel provvedimento del 27 novembre 2008, come modificato dal provvedimento del 25 giugno 2009, il Garante ha rimarcato la criticità del ruolo degli amministratori di sistema ed ha diramato indicazioni affinché i titolari dei dati personali adottino cautele volte a prevenire ed accertare eventuali accessi ai dati personali non consentiti, in particolare quelli realizzati con abuso della qualità di amministratore di sistema. In particolare ha disposto che:

1) le funzioni di amministratore di sistema debbano essere affidate con riferimento all'esperienza, alla capacità ed affidabilità del soggetto designato che deve fornire idonea garanzia del rispetto delle norme vigenti;
2) la designazione deve essere individuale e riportare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo autorizzato;
3) gli identificativi degli amministratori di sistema, con le funzioni ad essi attribuite, devono essere riportati nel DPS (Documento Programmatico sulla Sicurezza). Quando l'attività riguarda sistemi che trattano o permettono il trattamento di informazioni di carattere personale dei lavoratori, i Titolari, quali datori di lavoro, devono rendere conoscibile l'identità degli amministratori di sistemi utilizzando i sistemi idonei in atto in Azienda (informativa resa ai sensi dell'art. 13 del Codice oppure l'Intranet aziendale quale strumento di comunicazione). Se detti servizi sono affidati in outsourcing, il Titolare deve conservare specificatamente gli estremi identificativi delle persone fisiche preposte ad amministratore di sistema;
4) annualmente, l'operato degli amministratori di sistema deve essere verificato dal Titolare del trattamento al fine di controllare la rispondenza alle misure organizzative, tecniche e di sicurezza adottate relativamente al trattamento dei dati personali;
5) è stato adottato un sistema di registrazione degli accessi logici ai sistemi di elaborazione ed agli archivi elettronici da parte degli amministratori di sistema. Dette registrazioni hanno la caratteristica di completezza, inalterabilità e possibilità di verifica della loro integrità. Queste registrazioni sono conservate per almeno sei mesi;

RILEVATO che il Direttore del Servizio Risorse Informatiche e Telematiche congiuntamente al Direttore dell'U.O. Affari Legali, ha provveduto, sulla base delle rilevazioni effettuate presso le banche dati aziendali, i nuovi trattamenti e le ultime soluzioni informatiche, ad aggiornare il Documento Programmatico sulla Sicurezza - DPS -, nel testo allegato al presente atto, quale parte integrante e sostanziale;

DATO ATTO che il D.P.S**.** riporta, oltre all'analisi dei rischi, le misure di sicurezza già in atto e quelle da dover adottare, nonché la distribuzione dei compiti e delle responsabilità;

DATO ATTO altresì che nel D.P.S. vengono confermati/indicati i Responsabili dei trattamenti aziendali;

RITENUTO:

- di confermare quale Responsabile della Sicurezza l'Ing. Debora Angeletti, responsabile del Servizio Risorse Informatiche e Telematiche;
- di confermare quale coordinatore del diritto di accesso dell'interessato ai propri dati personali nonché referente aziendale in materia di trattamento dei dati personali, il Direttore dell'U.O."Affari Legali", dott.ssa Albarosa Balestrieri;
- di confermare quale amministratore di sistema, il sig. Domenico Ielo, collaboratore tecnico professionale esperto del Servizio Risorse Informatiche e Telematiche dell'Azienda.

VALUTATO positivamente il documento elaborato che permette, oltre ad un adeguato e costante aggiornamento formativo del personale aziendale, di ottemperare alle disposizioni del Codice

assicurando la protezione dei dati personali, sensibili e giudiziari trattati nell'ambito delle attività aziendali;

RITENUTO quindi di approvare l'aggiornamento del D.P.S. aziendale per l'anno 2015, nel testo allegato, avendo presente che lo stesso sarà costantemente adeguato, nel rispetto delle scadenze previste dal Codice, sia in ordine all'eventuale evoluzione della normativa, che per le innovazioni tecnologiche nonché specifiche azioni volte ad acquisire un maggior livello di sicurezza nella gestione dei dati;

SU PROPOSTA del Direttore Amministrativo;

ACQUISITO il parere favorevole del Direttore Sanitario;

DELIBERA

1) di approvare, nonostante la non obbligatorietà, l'aggiornamento del Documento Programmatico sulla Sicurezza per l'anno 2015 nel testo allegato, quale parte integrante e sostanziale, alla presente deliberazione;

2) di approvare le azioni di seguito indicate al fine di accrescere il livello di sicurezza nella gestione dei dati:

a) avviare la realizzazione della nuova sala server dell'AUSL di Parma e del sito di Disaster Recovery secondo i dettami della DigitPA per garantire maggiore integrità, sicurezza e continuità dei servizi e delle strutture;
b) introdurre strumenti informatici per la formalizzazione delle richieste di creazione nuove utenze, abilitazione ad applicativi aziendali in relazione alle mansioni e modifica delle stesse per cambiamento della collocazione aziendale;
c) procedere alla formalizzazione e raccolta dei documenti relativi all'incarico di Responsabili al trattamento esterno dei dati per tutti i fornitori esterni;
d) completare la messa in dominio delle postazioni client e l'integrazione di tutti gli applicativi con il sistema LDAP aziendale e la distribuzione alle farmacie e ai centri esterni di un certificato di accesso alla rete aziendale;
e) revisionare il contenuto dei seguenti allegati del DPS: T0301 Linee di trasmissione dati, T0302 Elenco strutture aziendali, T0101 Elenco responsabili dei trattamenti, T0102 Elenco responsabili Esterni, T0304 Elenco server aziendali, T0305 Elenco connessioni VPN, P0301 Videosorveglianza,; inserire il seguente allegato: P0401 Linee di indirizzo per la gestione del dossier sanitario nelle aziende sanitarie di AVEN;
f) procedere a una maggiore diffusione all'interno dell'Azienda di software per redazione di testi e fogli elettronici aderenti alle normative Digit PA, ovvero di formati open, secondo le modalità indicate al cap 3.4 del documento allegato P0703;

3) di confermare quale Responsabile della Sicurezza l'Ing. Debora Angeletti, Dirigente Responsabile del Servizio Risorse Informatiche e Telematiche dell'Azienda;

4) di confermare quale Coordinatore del diritto di accesso dell'interessato ai propri dati personali nonché referente aziendale in materia di trattamento dei dati personali, il Direttore dell'U.O."Affari Legali", dott.ssa Albarosa Balestrieri;

5) di confermare quale Amministratore di sistema il dott. Domenico Ielo, collaboratore tecnico professionale esperto del Servizio Risorse Informatiche e Telematiche dell'Azienda.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

ANNO 2015

Sommario

Quadro normativo

Con decreto legislativo 30 giugno 2003, n.196 è stato emanato il "Codice in materia di protezione dei dati personali" (di seguito indicato come Codice) che riforma interamente la materia, abroga e sostituisce undici tra leggi e decreti, e introduce le nuove misure di sicurezza dei dati e dei sistemi. Tali disposizioni sono entrate in vigore dal 1`gennaio 2004, presentando alcuni cambiamenti in singole disposizioni anche a fini di semplificare alcuni adempimenti, ma secondo un'impostazione che prosegue nelle linee già tracciate nella precedente disciplina.
Il Codice, entrato in vigore il 1° gennaio 2004, ha confermato ed aggiornato la disciplina in materia di sicurezza dei dati personali e dei sistemi informatici e telematici introdotta nel 1996 (L.675/96).
Le misure di sicurezza nel loro insieme devono garantire la protezione dei dati personali e dei sistemi. Quindi i programmi informatici, gli strumenti elettronici utilizzati, il sistema informativo nel suo complesso, gli atti e i documenti cartacei, gli ambienti nei quali vengono svolte le operazioni di trattamento e gli archivi devono essere adeguatamente tutelati.

Le prescrizioni sulla sicurezza sviluppano sia i concetti di *integrità, confidenzialità* e *disponibilità* dei dati contenuti nei principali standard di sicurezza condivisi dagli esperti del settore, sia alcuni principi e raccomandazioni della direttiva 2002/58/CE del Parlamento Europeo e del Consiglio del 12 luglio 2002 relativi alla tutela della vita privata nel settore delle comunicazioni elettroniche.

L'adozione di un documento programmatico sulla sicurezza (DPS) era un obbligo previsto dal D.Lgs. n.196/2003 (normativa sulla protezione dei dati personali, che sostituisce e abroga la legge n.675/1996)); l'obbligo esisteva per tutte le imprese, lavoratori autonomi, enti o associazioni che trattano i dati personali, sensibili o giudiziari, ed è venuto meno a seguito del Decreto Legge n. 5 del 9 febbraio 2012, convertito dalla legge n. 35 del 4 aprile 2012.

Il documento, a partire dal 31/03/2006 andava predisposto ed aggiornato annualmente entro il 31 marzo, per attestare la corretta adozione delle previste procedure che riguardano il trattamento dei dati personali e soddisfare anche determinati obblighi di legge, se previsti (p.e. la comunicazione nella relazione allegata al Bilancio di esercizio) per le società.

Il D.L. 9 febbraio 2012 n. 5 ha modificato alcune disposizioni in materia di misure minime di sicurezza sopprimendo in particolare il Documento Programmatico di Sicurezza. La novità introdotta dal cosiddetto "Decreto semplificazioni" del 2012 abolisce anche la precedente possibilità alternativa di rilasciare l'autocertificazione a cura del titolare nonché il "DPS semplificato" del 2011.

L'abolizione dell'obbligo di redazione del DPS, nei casi consentiti dalla normativa aggiornata, non solleva tuttavia dall'attuazione di tutti gli altri adempimenti privacy previsti dalla legislazione. Anzi, ne esce rafforzato proprio l'obbligo di implementazione concreta a discapito di un orpello solo burocratico-formale. D'altra parte, specie per le medio-grandi aziende, un documento analogo al DPS è pressoché scontato per motivi organizzativi e gestionali.

Il DPS ha quindi il compito di definire e descrivere le misure di sicurezza atte a

ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta dei dati personali trattati dall'Azienda (Art. 31).

Nel Codice sono inoltre riportare le seguenti definizioni:

"trattamento": qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

"dato personale": qualunque informazione relativa a persona fisica, identificata o identificabile, 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 con*vinzioni 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.*

Distribuzione di compiti e delle responsabilità

1.1. Le previsioni del Codice

Nel Codice sono individuate all'art. 4 le seguenti figure:

- *titolare*: *La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza*.
  In particolare: esercita il potere decisionale in ordine alle finalità ed alle modalità del trattamento, compreso il profilo della sicurezza.Formalizza per iscritto i compiti affidati ai responsabili di trattamento; impartisce loro le istruzioni e ne verifica periodicamente l'osservanza. Sottoscrive le comunicazioni al Garante per la protezione dei dati personali.

- *responsabile*: *La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.*

In particolare:deve garantire il pieno rispetto delle vigenti disposizioni di legge in materia di trattamento e delle istruzioni impartite dal titolare, anche per quanto riguarda il profilo della sicurezza, verificandone il recepimento e l'attuazione entro la propria area di competenza.

- *incaricati*: *Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.*
  In particolare l'incaricato deve: elaborare i dati per cui è stato autorizzato dal responsabile del trattamento seguendo le regole e le istruzioni impartite; mantenere la comunicazione con il responsabile del trattamento per risolvere ogni problema che si dovesse presentare nel corso del trattamento.

- *interessato*: *la persona fisica cui si riferiscono i dati personali.*

Inoltre devono essere preventivamente individuati per iscritto i *responsabili della custodia* della copia delle credenziali utilizzate dagli incaricati del trattamento, che ne garantiscano la riservatezza, nonché *le misure organizzative con le quali il titolare possa assicurare la disponibilità dei dati*, in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. I custodi devono informare tempestivamente l'incaricato dell'intervento effettuato.

La distribuzione organizzativa dei compiti e delle responsabilità

Il presente atto individua le competenze del titolare, designa i soggetti responsabili del trattamento e definisce i criteri generali da rispettare nell'individuazione dei soggetti incaricati a compiere le operazioni di trattamento.

1.2. Il titolare

Ai sensi dell'art. 4, comma 1, lettera f) e dell'art. 28 del Codice, il titolare dei trattamenti di dati personali è quindi l'Azienda U.S.L. di Parma a cui spetta l'adozione degli atti contenenti le scelte di fondo in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Spetta pertanto in particolare all'Azienda U.S.L, nella persona del Direttore Generale:

*1)*adottare con proprio atto, aggiornandolo periodicamente, il Documento Programmatico per la Sicurezza e riferire della sua adozione nella relazione accompagnatoria del bilancio di esercizio;
*2)*designare il *Responsabile della sicurezza*;
*3)*designare il *Coordinatore del diritto di accesso dell'interessato ai propri dati personali;*
*4)*designare altri soggetti quali *Responsabili del trattamento di dati personali*, oltre ai soggetti già designati con il presente atto;

5) vigilare, anche tramite verifiche periodiche, sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza, e sul rispetto delle proprie istruzioni. Tali verifiche saranno effettuate tramite i *Responsabili dei trattamenti ed il Responsabile della Sicurezza.*

Spetta al Direttore Generale, quale legale rappresentante dell'ente, la sottoscrizione degli atti di notifica, delle comunicazioni e delle richieste al Garante per la protezione dei dati personali (di seguito indicato come Garante). Tale funzione è delegabile ai soggetti designati quali Responsabili del trattamento di dati personali.

La funzione relativa alla sottoscrizione del consenso, richiesto da soggetti privati che trattano i dati dell'Azienda SUL di Parma, è direttamente attribuita ai soggetti designati quali *Responsabili del trattamento di dati personali*.

1.3. I Responsabili del trattamento di dati personali

Ai sensi dell'art. 4, comma 1, lettera g) e dell'art. 29 del Codice, il responsabile del trattamento di dati personali è il soggetto preposto dal Titolare al suddetto trattamento tramite designazione, specificando analiticamente per iscritto i compiti che gli sono affidati.

Nel presente documento sono identificati quali Responsabili del trattamento di dati personali i Responsabili di Struttura Complessa come da allegato Nome Documento : T0101 **Oggetto** : Elenco Responsabili dei Trattamenti

I compiti affidati ai responsabili del trattamento sono i seguenti:

a. verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura di riferimento, con particolare riguardo al principio di necessità di cui all'art. 3 del Codice, sia relativamente ai trattamenti già in essere che ai nuovi trattamenti;
b. disporre, in conseguenza alla verifica di cui alla lettera a), le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;
c. vigilare, per conto del Titolare, anche tramite verifiche periodiche, sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, secondo le modalità del presente regolamento e segnalando eventuali problemi al Responsabile della sicurezza e, in ultima istanza, al Titolare;
d. aggiornare periodicamente l'elenco dei trattamenti di dati personali effettuati dalla struttura di riferimento, anche al fine di garantire un tempestivo aggiornamento del Documento Programmatico per la Sicurezza;
e. predisporre il completamento dell'informativa di cui all'art. 13 del Codice e verificare che siano adottate le modalità operative necessarie perché la stessa sia effettivamente portata a conoscenza degli interessati;
f. individuare gli incaricati del trattamento dei dati personali e fornire agli stessi istruzioni per il corretto trattamento dei dati stessi, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite; tale individuazione deve essere effettuata secondo quanto stabilito dal presente documento e , in particolare, le istruzioni devono quanto meno contenere l'espresso richiamo alle linee guida aziendali per la protezione dei dati personali;
g. predisporre ogni adempimento organizzativo necessario per garantire agli interessati il diritto di accesso ai propri dati personali secondo quanto riportato al comma 2 dell'art 7 e con le modalità previste agli articoli 8, 9 e 10 del Codice
h. provvedere, anche tramite gli *Incaricati*, a dare riscontro alle istanze degli interessati per l'esercizio del diritto di accesso;
i. provvedere direttamente al riscontro nei seguenti casi: qualora l'istanza dell'interessato sia volta ad ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali sono stati raccolti o successivamente trattati, secondo quanto previsto dal comma 3, lettera b) dell'art. 7 del Codice; qualora si tratti di opposizione al trattamento, secondo quanto previsto dal comma 4 dell'art. 7 del Codice; qualora occorra prorogare il termine per il riscontro, previa comunicazione all'interessato nel caso di richiesta di particolare complessità o per altro giustificato motivo, secondo quanto previsto dal comma 3 dell'art. 146 del Codice; qualora l'istanza dell'interessato sia volta ad ottenere l'aggiornamento, la rettificazione, ovvero, quando vi sia interesse, l'integrazione dei dati, secondo quanto previsto dal comma 3, lettera a) dell'art. 7 del Codice
j. disporre l'adozione dei provvedimenti imposti dal Garante quale misura conseguente all'accoglimento delle richieste degli interessati;

k. predisporre la documentazione e gli atti necessari per il Garante nei casi e nei modi previsti dalla legge;
l. comunicare al Coordinatore del diritto di accesso dell'interessato ai propri dati personali l'individuazione dei Responsabili esterni;
m. collaborare con il Responsabile della sicurezza e con il Coordinatore del diritto di accesso dell'interessato ai propri dati personali;
n. individuare i soggetti che effettuano il trattamento dei dati quali Incaricati, specificando anche le relative istruzioni. Devono essere designati quali incaricati, qualora effettuino operazioni di trattamento, non soltanto i dipendenti a tempo indeterminato o determinato, ma anche gli altri soggetti che, ad altro titolo, operano sotto la diretta autorità del Titolare o del Responsabile del trattamento, quali, ad esempio, i lavoratori con contratto di somministrazione di lavoro a tempo determinato,i collaboratori a progetto, i tirocinanti, individuando il profilo d'accesso individuale alle varie banche dati.

1.4. I responsabili esterni

Si ritiene opportuno stabilire che siano designati, di norma, quali Responsabili del trattamento di dati personali, i soggetti esterni all'amministrazione che siano tenuti, a seguito di convenzione, contratto, verbale di aggiudicazione o provvedimento di nomina, ad effettuare trattamenti di dati personali per conto del titolare. A riguardo vedasi Nome Documento : T0102 Oggetto : Elenco Responsabili Esterni

Pertanto, qualora occorra affidare un incarico comportante anche trattamenti di dati personali, la scelta del soggetto deve essere effettuata valutando anche l'esperienza, la capacità e l'affidabilità in materia di protezione dei dati personali del soggetto cui affidare l'incarico, affinché lo stesso soggetto sia in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza.

Per poter operare tale valutazione, occorre quindi specificare già nelle procedure di selezione del bando di gara e del capitolato d'appalto che l'incarico ricomprende anche la designazione a responsabile del trattamento di dati personali.

Tale designazione deve essere effettuata direttamente in convenzione, nel contratto, nel verbale di aggiudicazione o nel provvedimento di nomina tramite:

a. l'indicazione nominativa qualora al trattamento di dati personali siano preposte persone fisiche;
b. l'individuazione della persona giuridica qualora al suddetto trattamento sia preposta una persona giuridica;
c. l'individuazione della pubblica amministrazione o di qualsiasi altro ente qualora al trattamento siano preposti rispettivamente una pubblica amministrazione o qualsiasi altro ente;
d. l'individuazione di una o più persone fisiche qualora, nei sopra riportati casi di cui alle lettere b) e c), il trattamento di dati personali riguardi esclusivamente un settore specifico e limitato dell'ente.

Qualora i soggetti esterni siano persone fisiche ed operino sotto la diretta autorità di un responsabile del trattamento, le stesse devono essere individuate quali

incaricati del trattamento.

I compiti affidati ai Responsabili esterni del trattamento di dati personali sono i seguenti:

1) adempiere all'incarico attribuito adottando idonee e preventive misure di sicurezza, con particolare riferimento a quanto stabilito dal Codice, dall'Allegato B del Codice e dalle eventuali disposizioni esplicitate nell'incarico.
2) predisporre, qualora l'incarico comprenda la raccolta di dati personali, *l'informativa di cui all'art. 13 del Codice* e verificare che siano adottate le modalità operative necessarie perché la stessa sia effettivamente portata a conoscenza degli interessati;
3) dare direttamente riscontro oralmente, anche tramite propri incaricati, alle richieste verbali dell'interessato di cui ai commi 1 e 2 dell'art. 7 del Codice;
4) trasmettere, con la massima tempestività, le istanze dell'interessato per l'esercizio dei diritti di cui agli artt. 7 e ss. del Codice che necessitano di riscontro scritto al Responsabile del trattamento per consentire allo stesso di dare riscontro all'interessato nei termini stabiliti dal Codice e, per conoscenza, al Coordinatore del diritto di accesso dell'interessato ai propri dati personali;
5) fornire al responsabile del trattamento la massima assistenza, necessaria per soddisfare tali richieste, nell'ambito dell'incarico affidatogli;
6) individuare gli incaricati del trattamento dei dati personali e fornire agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite; le istruzioni devono quanto meno contenere l'espresso richiamo alle linee guida aziendali in materia di protezione dei dati personali;
7) attestare, qualora l'incarico affidato ricomprenda l'adozione di misure minime di sicurezza, la conformità degli interventi alle disposizioni di cui alla misura 25 dell'Allegato B del Codice e trasmettere tale attestazione al Responsabile della sicurezza

Tali compiti possono essere ulteriormente precisati e, qualora fosse necessario, adattati alla natura dello specifico incarico comportante il trattamento di dati personali attribuito al soggetto esterno. Le specificazioni e/o gli adattamenti devono essere analiticamente stabiliti in convenzione, nel contratto o nel provvedimento di nomina.

1.5. Il Responsabile della sicurezza

Il Codice impone, in particolare al Titolo V, numerosi obblighi in materia di sicurezza dei dati e dei sistemi.

Si reputa opportuno, in ragione sia della complessità organizzativa della Azienda U.S.L. di Parma sia della peculiarità della materia, che richiede particolari competenze professionali anche tecniche, designare un soggetto con la specifica responsabilità di operare per la sensibilizzazione, il coordinamento, la vigilanza e

l’applicazione di tali obblighi, secondo i compiti di seguito definiti.

Al Responsabile della sicurezza dell’ Azienda U.S.L. sono affidati i seguenti compiti:

1) curare la redazione e l’aggiornamento del Documento Programmatico per la Sicurezza relativamente all’ambito dell’Azienda U.S.L. di Parma;
2) collaborare con il Titolare per definire linee guida in materia di protezione dei dati personali;
3) curare la redazione di eventuali disciplinari tecnici da sottoporre all'approvazione del Direttore Generale, promuovendone anche l’aggiornamento ogni qualvolta l’evoluzione tecnica o normativa lo renda necessario;
4) curare la redazione del Regolamento per l’utilizzo degli strumenti informatici dell’Azienda U.S.L. di Parma relativo alle modalità e alle procedure per l’effettuazione di controlli sull’utilizzo delle strumentazioni informatiche;
5) attivarsi ogni qualvolta venga avvertito un problema di sicurezza per:
   - verificare il rispetto delle misure minime di sicurezza;
   - individuare, se necessario, altre misure idonee al miglioramento della sicurezza dei trattamenti dei dati personali;
   - inviare opportuna segnalazione in prima istanza ai Responsabili dei trattamenti e in ultima istanza al Titolare, affinché pongano in essere le misure necessarie per garantire la sicurezza dei dati;

6) individuare le misure idonee da osservare nell’esecuzione dei trattamenti dei dati personali aggiornandole in relazione all’evoluzione della tecnica, della normativa e dell’esperienza, segnalando eventuali problemi rilevati in prima istanza ai Responsabili dei trattamenti di dati personali e, in ultima istanza, al Titolare;
7) vigilare per conto del Titolare, anche tramite verifiche periodiche, sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza e al rispetto delle proprie istruzioni, segnalando eventuali problemi rilevati, in prima istanza, ai Responsabili dei trattamenti di dati personali e, in ultima istanza, al Titolare;
8) promuovere l’istruzione e la formazione, in collaborazione con il Servizio Formazione Aziendale, dei Responsabili e degli Incaricati dei trattamenti dei dati personali ivi compresi gli incaricati (ppersonale non dipendente) operanti sotto la diretta autorità del Responsabile interno del trattamento, con particolare riferimento all’adozione e all’osservanza delle singole misure di sicurezza;
9) promuovere, in collaborazione con il Servizio Comunicazione Aziendale, la cultura della sicurezza anche attraverso un piano di comunicazione e divulgazione all’interno dell’ Azienda;
10) raccogliere e conservare ai fini di eventuali verifiche, le attestazioni di conformità alle disposizioni della misura 25 dell’Allegato B del Codice.

1.6. Il Coordinatore del diritto di accesso dell’interessato ai propri dati personali

Il Codice, agli artt. 7 e ss., attribuisce agli interessati il potere di esercitare, sui propri dati personali, un diritto di accesso, relativo sia alla conoscenza dei dati stessi che ad un intervento (ad es., di integrazione o cancellazione).

L’art. 10, comma 1, lettera b) del Codice, stabilisce inoltre che il Titolare è tenuto ad adottare idonee misure volte, in particolare, a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente, anche nell’ambito di uffici o servizi preposti alle relazioni con il pubblico.

Si reputa quindi opportuno, in ragione della complessità organizzativa dell'Azienda U.S.L. di Parma, designare un soggetto con la specifica responsabilità di operare per la sensibilizzazione e il coordinamento di tale diritto, denominandolo "Coordinatore del diritto di accesso dell’interessato ai propri dati personali". Al Coordinatore del diritto di accesso dell’interessato ai propri dati personali dell' Azienda U.S.L. di Parma, sono affidati i seguenti compiti:

1) promuovere il coordinamento e la sensibilizzazione dei Responsabili e degli Incaricati del trattamento dei dati, sia in via generale e preventiva che su singola richiesta, sui diritti di cui all’art. 7 e ss. del Codice, sul loro contenuto, sulla loro applicazione e sulle modalità di ottemperanza alle richieste dell’interessato;
2) collaborare con il Titolare per definire linee guida in materia di protezione dei dati personali relativamente al diritto di accesso agli stessi dati da parte dell’interessato;
3) collaborare con i singoli interessati, anche fornendo istruzioni sul contenuto dei diritti di cui all’art. 7 del Codice e sulla procedura per il loro esercizio, alla redazione e compilazione delle istanze per l’esercizio dei diritti medesimi;
4) smistare le singole istanze verso i Responsabili del trattamento, responsabili anche del riscontro e competenti ad ottemperare alle medesime istanze;
5) vigilare, per conto del Titolare, sul puntuale e corretto invio del riscontro, segnalando eventuali problemi rilevati, in prima istanza, ai Responsabili dei trattamenti di dati personali e, in ultima istanza, al Titolare;
6) proporre l’adozione delle singole misure ritenute opportune per agevolare l’accesso ai dati personali da parte dell’interessato, coordinandosi con i Responsabili del trattamento e proporre le misure opportune per semplificare le modalità di accesso e per ridurre i tempi di attesa, indicandole, laddove necessario, ai Responsabili del trattamento e al Responsabile della sicurezza;
7) curare la pubblicazione e il relativo aggiornamento dell’elenco dei Responsabili esterni, in base alle comunicazioni effettuate dai Responsabili del trattamento;
8) individuare e promuovere, in collaborazione con il Responsabile della sicurezza, le misure idonee a garantire l’esercizio dei diritti di cui all’art. 7 del Codice, anche mediante software che consentano il facile, agevole e approfondito reperimento di tutti i dati personali trattati in forma elettronica nell’ambito dell'Azienda U.S.L. di Parma;

9) promuovere l'istruzione e la formazione, in collaborazione con il Servizio Formazione Aziendale, dei Responsabili e degli Incaricati dei trattamenti dei dati personali, con particolare riferimento all'osservanza delle procedure da adottare per favorire l'esercizio del diritto di accesso degli interessati ai propri dati personali;
10) promuovere, in collaborazione con il Servizio Formazione Aziendale e con il Servizio Comunicazione Aziendale e con il Responsabile della sicurezza, la cultura sui diritti dell'interessato, anche attraverso un piano di comunicazione e divulgazione all'interno dell'Ente;
11) proporre l'adozione di ogni altro provvedimento e adempimento necessario per la corretta applicazione dell'art. 7 e ss. del Codice.

1.7. Gli incaricati

L'art. 4, lettera h) e l'art. 30 del Codice stabiliscono che il titolare o il responsabile devono designare, quali incaricati del trattamento di dati personali, le persone fisiche che effettuano le operazioni di trattamento, operando sotto la loro diretta autorità.

Devono pertanto essere designati quali incaricati, qualora effettuino operazioni di trattamento, non soltanto i dipendenti a tempo indeterminato o determinato, ma anche gli altri soggetti che, ad altro titolo, operano sotto la diretta autorità del Titolare o del Responsabile del trattamento, quali, ad esempio, i lavoratori con contratto di somministrazione di lavoro a tempo determinato, i collaboratori a progetto, i tirocinanti, individuando il profilo d'accesso individuale alle varie banche dati.

Il Codice specifica inoltre che la designazione:

a. deve essere effettuata per iscritto, individuando puntualmente l'ambito del trattamento consentito;
b. è considerata quale designazione anche la documentata preposizione della persona fisica ad una unità organizzativa per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

I Responsabili del trattamento, devono pertanto designare/revocare per iscritto i soggetti autorizzati ad effettuare le operazioni di trattamento e darne tempestiva comunicazione, per gli adempimenti di competenza, al Responsabile della Sicurezza. La designazione deve essere aggiornata con la massima tempestività ~~almeno annualmente~~.

La gestione degli incaricati, dei responsabili, dei trattamenti e di tutto ciò che ruota attorno alla sicurezza inclusa la formazione degli operatori non è cosa semplice ed immediata.

A tal proposito è in corso da parte del Responsabile della Sicurezza, in collaborazione con il Titolare, il Coordinatore del diritto d'accesso e con i Responsabili dei trattamenti, una revisione applicativa che consenta un percorso semplificato al fine di garantire una corretta e puntuale gestione degli incarichi di Responsabile esterno al trattamento dei dati e degli incaricati interni ed esterni.

Tale revisione si basa sulla semplificazione, prevista dal Codice, secondo la quale è considerata quale designazione anche la documentata preposizione della persona fisica ad una unità organizzativa per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima e che la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

In tal senso si intende definire l'elenco dei trattamenti associati alle strutture o servizi interni ed esterni in modo da definire un ambito omogeneo di trattamenti per tutte le persone fisiche afferenti a quella struttura o servizio interno o esterno (classi omogenee di incarico).

L'afferenza della persona fisica ad una determinata struttura o servizio verrà definita come segue:

a. per strutture interne sarà mutuata dalla configurazione effettuata sull'applicativo di gestione del personale o direttamente attestata dal Responsabile del trattamento della struttura di afferenza con inserimento diretto

b. per strutture esterne sarà attestata dal Responsabile esterno del trattamento della struttura stessa con inserimento diretto

Le misure di sicurezza

Le misure di sicurezza sono articolate in gruppi correlati:

- le misure c.d. idonee e preventive (art. 31) decise in autonomia dal titolare in relazione alle proprie specificità.
- le "misure minime" indicate dal Codice (artt. 33, 34, 35 e 36) e dall'Allegato B

Mediante l'adozione preventiva di idonee misure di sicurezza si mira a raggiungere il fine ultimo della custodia e del controllo ossia la riduzione dei rischi quali:

- distruzione o perdita, anche accidentale dei dati stessi;
- accesso non autorizzato o il trattamento non consentito o non conforme ai fini per i quali i dati sono raccolti.

L'art. 31 prescrive l'obbligo della sicurezza a cui tutti devono attenersi e individua i principi fondamentali della "custodia" e del "controllo". I dati personali oggetto di trattamento devono essere custoditi e controllati durante tutto il ciclo di vita del trattamento.

La custodia e il controllo non sono misure immutabili, ma anzi devono essere adeguate in relazione alle conoscenze acquisite in base al progresso tecnico.

Per "misure minime" si intende il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;

I parametri di custodia e controllo variano sia in relazione alla natura dei dati trattati

(dati personali, sensibili o giudiziari, nelle accezioni indicate dal Codice stesso), sia in funzione delle caratteristiche del trattamento, cioè delle modalità con cui viene svolto. A tal fine il Codice distingue fra trattamenti con strumenti elettronici (Art. 34) e trattamenti senza l'ausilio di strumenti elettronici (Art. 35)

Nel primo caso (trattamento con strumenti elettronici) valgono le regole indicate nel disciplinare tecnico, Allegato B), nei punti da 1 a 26, nel secondo caso quelle indicate nei punti da 27 a 29.

Gli obblighi di sicurezza riguardano chiunque e, più in specifico, il "titolare" del trattamento, il "responsabile", e gli "incaricati".

Sistema Informatico

Viene riportata di seguito la locazione fisica del Servizio RIT e del Datacenter dell'Azienda USL di Parma:
Strada del Quartiere 2/a
43125 Parma

Per "strumenti elettronici" si intendono gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento (art. 4, comma, 3 lettera b).

La disciplina della sicurezza informatica si occupa dell'analisi delle vulnerabilità, del rischio, delle minacce o degli attacchi e quindi della protezione dell'integrità fisica (hardware) e logico-funzionale (software) di un sistema informatico e dei dati in esso contenuti o scambiati in una comunicazione con un utente.

Tale protezione è ottenuta attraverso misure di carattere tecnico-organizzativo e funzionali tese ad assicurare:

- o la correttezza dei dati (integrità);
- o la confidenzialità dei dati (cifratura);
- o l'accesso fisico e/o logico solo ad utenti autorizzati (autenticazione);
- o la fruizione di tutti e soli i servizi previsti per quell'utente nei tempi e nelle modalità previste dal sistema (disponibilità e autorizzazione);
- o la protezione del sistema da attacchi di software malevoli per garantire i precedenti requisiti (protezione)

Il DPS riporterà la descrizione degli standard comportamentali, organizzativi e tecnologici che garantiscono l'adeguatezza ed il buon uso del sistema di sicurezza dell'azienda sanitaria, al fine di prevenire quanto indicato all'Art. 31.

Tali standard, definiti conseguentemente e in coerenza con le politiche di sicurezza aziendali, sono necessari per precisare e dettagliare le direttive ivi contenute, oltre che per aggiornare dinamicamente le misure di sicurezza a seguito dei cambiamenti nell'organizzazione e nei sistemi informativi dell' Azienda USL di Parma e dell'evoluzione della tecnologia e della conoscenza.

Il Piano per la Sicurezza costituisce la raccolta delle regole e degli standards aziendali in fatto di sicurezza; per i dettagli operativi si rimanda ai documenti allegati, in particolare

Nome Documento : P0701 **Oggetto** : Regole di gestione/conservazione delle credenziali di autenticazione

Nome Documento : P0702 **Oggetto** :

Nome Documento : P0703 **Oggetto** : Regolamento per l'utilizzo degli strumenti informatici dell'Azienda USL di Parma

Nome Documento : P0704

Oggetto : Linee guida e "buone pratiche" per la manipolazione dei file

1.1. Analisi dei Rischi

Per poter applicare idonee misure di sicurezza è necessario effettuare l'Analisi dei Rischi a cui sono esposti i trattamenti dei dati.

L'analisi dei rischi costituisce la fase di partenza dell'attività di progettazione del Piano aziendale della sicurezza ed è un elemento fondamentale del Documento programmatico della sicurezza. Gli obiettivi principali dell'analisi sono:

- Avere la visibilità di esposizione al rischio del patrimonio informativo;
- Costruire una mappa delle contromisure di sicurezza .

A tal fine, è indispensabile:

- l'individuazione degli elementi del sistema informativo automatizzati e non;
- un censimento delle principali risorse di elaborazione (soprattutto server), degli applicativi e delle banche dati.

Risorse Hardware: Rientrano in questa categoria le workstations, le stampanti, i server, i router, gli switch, i dischi e tutte le apparecchiature di comunicazione. Le principali minacce di questi dispositivi sono i malfunzionamenti causati da guasti tecnici, eventi naturali, sabotaggi o intercettazioni. Quest'ultima eventualità interessa principalmente i server e la rete in generale. Occorre quindi attuare contromisure al fine di evitare intrusioni o monitoraggi indebiti.

Risorse Software: Esse sono rappresentate dai sistemi operativi, dai software

applicativi o di base e da tutto ciò che può essere eseguito su di un elaboratore. Le minacce che incombono su queste risorse sono diverse e spaziano dall'errore di sviluppo, che favorisce intrusioni, ad attacchi veri e propri portati dall'esterno via rete, o direttamente dall'interno tramite codice malicius.

Dati: Con tale termine s'intende il contenuto degli archivi cartacei od elettronici, delle basi dati, dei file di log, delle copie di salvataggio e di tutto ciò che rappresenta informazione a livello aziendale. Si identificano due principali fonti di rischio e precisamente: quella dell'accesso non autorizzato ai dati e quella che comprende una volontà precisa di arrecare danno.

Le Risorse professionali: Un elemento da tenere in considerazione per la gestione e l'applicazione della sicurezza è la preparazione professionale degli operatori del settore informatico. Fanno parte di questa categoria gli amministratori di rete e di sistema, i manutentori hardware e software.

Documentazione: Tutto ciò che riguarda la documentazione dei software, dell'infrastruttura hardware e di rete, delle procedure. Tali elementi sono soggetti al rischio di accesso e trattamento non autorizzato delle informazioni in essi contenute.

Supporti di memorizzazione: Vengono utilizzati per consentire una salvaguardia sia dei prodotti informatici dell'azienda sia dei dati di controllo (log) o dati procedurali. Come tutti i componenti appartenenti a questa categoria i rischi che incombono sono: il deterioramento nel tempo, l'inaffidabilità del mezzo fisico e, in pospettiva, un avanzamento tale della tecnologia da non consentire il riutilizzo dei supporti.

1.2. Classificazione e valutazione dei beni informatici

E' possibile individuare delle categorie di classificazione in base agli elementi di integrità, riservatezza e disponibilità. Per la valutazione dei beni sono disponibili diverse metodologie, alcune delle quali basate su principi quantitativi (costo di ripristino, costi di elaborazione tramite risorse alternative, ecc), altre su principi qualitativi (interruzione di servizi, violazione aspetti legislativi, perdità di operatività, ecc).

Di seguito vengono elencati i documenti relativi all'analisi dei rischi dei principali settori informatici.

Tipo	***Nome documento***
Server	Nome Documento : T0201
Workstations	Nome Documento : T0202
Reti	Nome Documento : T0203
Applicativi	Nome Documento : T0204
Misure	Nome Documento : T0205

1.3. Misure in essere e da adottare

1.3.1. Sicurezza Organizzativa

Il processo della sicurezza dei sistemi informativi automatizzati richiede che, vengano definite una serie di norme e procedure mirate a regolamentare gli aspetti organizzativi del processo medesimo.

Gli aspetti organizzativi della sicurezza dei sistemi informativi automatizzati riguardano principalmente:

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

In particolare modo si intende dar rilievo alle procedure da adottare nell'attivazione di connessioni verso i server aziendali da parte di operatori esterni e utenti interni e alle misure da adottare per ridurre al minimo anomalie o manomissioni. In particolare sono indicate di seguito alcune linee di massima per l'accesso ai servizi.

Per quello che riguarda invece l'adozione di misure a supporto della sicurezza e della continuità operativa si rappresenta l'organizzazione del servizio di reperibilità. Negli allegati

Nome documento: P0602 Oggetto: Allegato tecnico.doc

Nome documento: P0601 Oggetto: Reperibilità Servizio Risorse Informatiche e Telematiche-1.doc

Nei documenti oltre agli obiettivi di tale servizio sono anche indicate le modalità tecniche di erogazione (strumenti, accesso ai locali, modalità di attivazione…)

1.3.1.1. Richiesta di accesso ai trattamenti

I responsabili dei trattamenti dei dati, sia interni che esterni, individuati dall'Azienda tramite delibera, personalmente o a mezzo di loro delegati designati ufficialmente, devono richiedere per i loro incaricati le credenziali di accesso agli applicativi e alle banche di dati aziendali per mezzo del software preposto a tale scopo.

In caso di revoca di una designazione o di cessazione del rapporto contrattuale o di convenzione, il responsabile del trattamento, interno o esterno, o suo delegato, deve farne espressa comunicazione sempre utilizzando gli strumenti informatici preposti.

Come indicato in premessa, è in corso un processo di revisione e semplificazione degli strumenti informatici messi a disposizione per tali operazioni.

1.3.1.2. Gestione dei dati di accesso agli strumenti elettronici con cui si effettua il trattamento

Il titolare, il responsabile o l'incaricato hanno l'obbligo di tenere riservate le proprie credenziali di accesso agli strumenti elettronici con cui si effettua il trattamento, non dandone comunicazione ed attenendosi alle regole regole citate nell'allegato Nome Documento : P0701 Oggetto : Regole di gestione/conservazione delle credenziali di autenticazione.

1.3.2. Sicurezza Fisica

Lo scopo delle procedure per la sicurezza fisica è quello di garantire chi opera sui sistemi informatici in merito alla loro integrità hardware e software. A tale scopo vengono descritte diverse tipologie di misure che possono essere ricondotte fondamentalmente alle due seguenti categorie.

1.3.2.1. Sicurezza di area

La sicurezza di area mira a prevenire accessi fisici non autorizzati, danni o interferenze con lo svolgimento dei servizi. Le contromisure si riferiscono alle protezioni perimetrali dei siti, ai controlli fisici all'accesso, alla sicurezza della *sale macchine* rispetto a danneggiamenti accidentali o intenzionali, nonché alla protezione fisica dei supporti. A tal fine si prevede che:

- Il locale sia chiuso, anche se presidiato;
- L'accesso a locali 'delicati' avvenga tramite riconoscimento elettronico;
- L'accesso sia consentito solo alle persone autorizzate;
- I visitatori occasionali siano sempre accompagnati;

1.3.2.2. Sicurezza delle apparecchiature hardware

La sicurezza delle apparecchiature è riconducibile da un lato alle protezioni da danneggiamenti accidentali o intenzionali e dall'altro alla sicurezza degli impianti di alimentazione e di condizionamento. La manutenzione dell'hardware rientra in questa area, come anche la protezione da manomissione o furti.

Le apparecchiature informatiche per l'erogazione del servizio sono conservate in aree ad accesso controllato, dotate di impianto di rilevazione antincendio e di gruppi di continuità elettrica.

1.3.3. Sicurezza Logica

La sicurezza logica è una componente particolarmente critica della Sicurezza del Sistema Informativo. Il campo di applicazione della Sicurezza Logica riguarda principalmente la protezione dell'informazione, e di conseguenza di dati, applicazioni, sistemi e reti, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo.

Le contromisure di Sicurezza Logica sono quindi da intendersi come l'insieme di misure di *sicurezza di carattere tecnologico e di natura procedurale ed organizzativa* che concorrono nella realizzazione del livello di sicurezza da raggiungere. Diamo di seguito alcune indicazioni inerenti l'identificazione e l'autorizzazione.

Si possono considerare diversi livelli di sicurezza inerenti l'identificazione e l'autorizzazione all'accesso, classificandoli in base alle tipologie di utilizzo. In generale devono essere valide queste regole sia che avvenga un'autenticazione lato utente sulla postazione di lavoro che un accesso diretto ad un server da parte di un operatore o di un programma. Queste politiche di sicurezza vanno sotto il nome di "controllo degli accessi", che consiste nel garantire che tutti gli accessi agli

oggetti del sistema informativo avvengano esclusivamente secondo modalità controllate. Si rende indispensabile prevedere un meccanismo che costringa ogni utente ad autenticarsi (cioè dimostrare la propria identità) prima di poter accedere al sistema. Il meccanismo sinora più usato a tale scopo è quello delle password.

Se il sistema di accoglienza lo consente è consigliato l'uso di messaggistica di accoglienza (banner di log-in) per ricordare all'utente che sta entrando in una rete protetta.

In definitiva il controllo accessi può essere visto come un sistema caratterizzato da soggetti (utenti, processi) che accedono a oggetti (applicazioni, dati, programmi) mediante operazioni (lettura, aggiornamento, esecuzione).

L'autenticazione e l'accesso ai sistemi informatici avviene dopo il valido riconoscimento delle credenziali “utente” e “password” tramite il “login”, il quale deve essere sottoposto a diversi criteri:

- User-id: Lo user-id deve poter essere riconducibile ad un singolo individuo a cui è stato assegnato e che ne è il responsabile della custodia.
- Password: L'utente deve conservare con estrema cura la password di accesso ai sistemi, ha l'obbligo di non comunicarla ad altri e di sostituirla immediatamente in caso di sospetta diffusione. La password deve essere cambiata almeno ogni tre mesi. Alcune regole per la creazione delle password possono essere visionate nell'allegato Nome Documento : P0701 Oggetto : Regole di gestione/conservazione delle credenziali di autenticazione.
- Revoca delle User-id : Quando un utente non ha più la necessità di accedere ad una banca dati, lascia l’azienda o quando vengono a cadere le motivazioni che danno diritto di accesso al sistema informativo aziendale, la sua utenza deve essere disabilitata. Il Responsabile del trattamento a cui l’interessato è abilitato, o suo delegato, deve richiederne la disabilitazione attraverso apposite procedure informatiche.
- Sostituzione immediata delle password iniziali: Le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l’installazione o al primo utilizzo.
- Ripristino della password: La richiesta di ripristino della password viene effettuata dall'interessato tramite comunicazione (email, fax,..) al servizio competente e deve essere corredata di fotocopia o scansione del documento d’identità. L'operatore del servizio competente, previa identificazione dell'utente richiedente, provvede al ripristino della password di default e ne dà comunicazione al diretto interessato.

Quanto sopra vale per autenticazioni interne alla rete, in cui viene garantito un certo grado di sicurezza.

Per connessioni esterne all'azienda, oltre a quanto sopra esposto rispetto alla gestione dell’accesso del singolo utente alle procedure, occorre prevedere un controllo più accurato attraverso un sistema di “autenticazione forte”:

- Autenticazione accessi da Internet**:** Si deve prevedere il superamento dell'utilizzo della modalità userid/password poiché non forniscono sufficienti garanzie di sicurezza per le connessioni ai sistemi aziendali da internet o in dial-

up. La positiva identificazione degli accessi da internet può essere garantita solamente da una autenticazione forte, preferibilmente basata su certificato digitale e smartcard, usando i meccanismi di sfida/risposta (challenge/response). Questo meccanismo consente l'identificazione certa dell'utente e del server poiché instaura una comunicazione cifrata (secure-messaging) e garantisce dall'attacco dell' "uomo-nel-mezzo", ossia che una terza persona si intrometta nella comunicazione alterandola o compromettendone l'integrità.

- Autenticazione del Server: Avviene attraverso l'uso del certificato digitale usato dal server per presentarsi al browser. L'instaurarsi della sessione https (ssl2) dà garanzia all'utente che i dati che sta ricevendo sono certamente quelli dell'AUSL. Questa modalità garantisce l'integrità del dato all'utente finale.
- Autenticazione del Client: Avviene attraverso l'uso del certificato digitale utente da parte del browser. L'instaurarsi della sessione https (ssl3) , aggiunge alla situazione precedente la garanzia dell'identità utente. Questa modalità garantisce sia l'integrità del dato che l'identità dell'utente connesso.

Questi due ultimi tipi di autenticazione forniscono un diverso livello di sicurezza e sono da valutare quando si realizzano collegamenti alle applicazioni AUSL tramite internet. La scelta della modalità di autenticazione non può prescindere dalla natura delle informazioni trattate e dalla operatività dell'applicazione.

Al fine di garantire la tracciabilità delle operazioni effettuate sulle macchine aziendali si rende necessaria una politica di controllo basata sui log, generati da applicazioni, da sistemi di base o di rete.

- Logs richiesti alle applicazioni che trattano dati critici: Tutte le applicazioni in produzione che trattano dati critici devono generare logs che consentano di tracciare ogni modifica, aggiunta o cancellazione delle informazioni.
- Inclusione di eventi rilevanti per la sicurezza nei logs di sistema: I sistemi in produzione ritenuti critici per l'azienda, devono generare dei logs di tutti gli eventi rilevanti ai fini della sicurezza, ad esempio, tentativi di accesso con password errata, tentativi di utilizzare privilegi non assegnati, modifiche alla configurazione delle applicazioni o dei sistemi.
- Tracciabilità per tutti i comandi privilegiati di sistema: Tutti i comandi effettuati dall'operatore di sistema devono essere tracciati e riconducibili al operatore che gli ha effettuati.
- Contenuti minimi dei logs di produzione:
    - Attività della sessione utente (userid, timestamp del login e del logout, applicazioni usate).
    - Cambiamenti alle informazioni critiche della applicazione (dati di configurazione).
    - Modifiche ai privilegi utente.
- Periodo di conservazione dei logs: I logs contenenti informazioni relative agli eventi rilevanti per la sicurezza devono essere conservati per almeno 3 mesi e secondo modalità che garantiscano la non modificabilità. Potranno essere letti

solo da persone autorizzate. Sono particolarmente importanti per la determinazioni di errori, diagnosi su falle del sistema di sicurezza,ed eventuali verifiche legali.

Trattandosi di direttive di ordine generale, sarà compito del responsabile di ogni applicativo e del responsabile di sistema, realizzare e verificare il rispetto di tali politiche.

- Protezione alla disattivazione, modifica, o cancellazione dei log: Il meccanismo di registrazione degli eventi relativi alla sicurezza deve essere resistente agli attacchi. Questi includono i tentativi di disattivare, modificare o cancellare i meccanismi per la registrazione o i log stessi.
- Persone autorizzate ad esaminare i logs: Tutti i log di sistema e di applicazione devono essere conservati in maniera tale da non poter essere facilmente letti da personale non autorizzato. Una persona non è autorizzata alla lettura se non appartiene a strutture di sicurezza informatica, sistemistiche o in generale non rientra tra i suoi specifici compiti.
- Riesame dei logs di sistema: Per consentire appropriate azioni correttive è necessario predisporre regolari attività di riesame dei log relativi agli eventi di sicurezza.
- Notifica agli utenti del logging: Gli utenti devono essere informati sulle azioni che costituiscono violazioni di sicurezza e, devono altresì essere informati, che tali violazioni saranno loggate.

1.3.4. Protezione contro attacchi esterni

1.3.4.1. Antivirus

I virus informatici, indicati con il termine generico di "malicius code" (codice maligno – programma dannoso), sono i rappresentanti più noti di una categoria di programmi scritti per generare intenzionalmente una qualsiasi forma di danneggiamento ad un computer o ad una rete.

La miglior difesa contro i virus informatici consiste nel definire un'architettura antivirus composta da regole comportamentali e da procedure operative, a protezione dell'intero sistema informatico.

Tutti gli utenti del sistema sono tenuti a conoscere e rispettare tali regole e, l'amministratore di sistema, è tenuto a mantenere costantemente operative e aggiornate le procedure software predisposte.

A tal fine, tali procedure hanno la caratteristica di mantenere automaticamente aggiornati i pattern di controllo, sia sui server che sulle stazioni client.

E' possibile verificare che ogni stazione dotata di antivirus utilizzi il pattern aggiornato mantenendo attiva l'opzione di aggiornamento automatico.

1.3.4.2. Utilizzo di internet

L'utilizzazione di Internet e della Posta elettronica , già ampiamente diffusi nel contesto lavorativo, è destinata ad un rapido incremento in numerose attività svolte anche fori dalla sede lavorativa. Al datore di lavoro compete di assicurare la funzionalità e il corretto impiego di tali mezzi da parte dei lavoratori, definendone le

modalità d'uso dell'organizzazione dell'attività lavorativa, garantendo la disponibilità e l'integrità di servizi e dati e prevenendo gli accessi indebiti.

Al fine di garantire quanto sopra, tramite opportune attività di analisi, profilazione, elaborazione di log file della navigazione dei siti web ottenuti ad esempio tramite l'impiego di proxy server, tenuta di log file del traffico email e archiviazione dei messaggi, è però possibile risalire ad informazioni che rappresentano dati personali, anche sensibili riguardanti lavoratori o terzi, identificati o identificabili.

In questo quadro è opportuno adottare un disciplinare interno in merito all'utilizzo di Internet e della Posta elettronica, da pubblicizzare adeguatamente tra i lavoratori.

- Nome Documento : P0702 Oggetto : Disciplinare tecnico per l'uso di Internet e della Posta elettronica
-

1.3.4.3. Gestione dei siti web destinati alla salute

Le linee guida del Garante in materia di trattamento dei dati personali per finalità di pubblicazione e diffusione nei siti web esclusivamente dedicati alla salute del 25 gennaio 2012 riconoscono che le potenzialità del web in questo ambito sono in costante evoluzione. Lo scambio quotidiano di informazioni , consigli, commenti e testimonianze tra utenti testimonia l'utilità e il valore di tali esprienze riguardo alla condivisione di conoscenze scinetifiche, spazi di solidarietà e di sostegno. Tale condivisione avviene, nel caso dell'Azienda USL di Parma, all'interno di forum, blog, sezioni di portali, social network che si occupano di tematiche della salute attraverso specifici profili aperti e manutenuti da uno o più soggetti singoli, dipendenti dell'Azienda, in nome e per conto dei diversi Servizi Aziendali.

A tal fine il Garante sottolinea come sia opportuno che il trattamento dei dati personali identificativi su tali siti avvenga:

1. nel rispetto della disciplina sulla protezione dei dati personali, in particolare dei principi di pertinenza e non eccedenza, correttezza e buona fede (art.11 del Codice Privacy)
2. evitando una impropria esposizione delle persone e dei loro dati più intimi nella rete
3. consentendo agli utenti di partecipare in maniera consapevole alle attività messe a disposizione sul web negli spazi di condivisione

Per ognuno degli spazi sopra descritti deve essere nominato un gestore; il gestore è incaricato dal titolare e deve porre in essere tutti gli adempimenti previsti in materia di protezione dei dati personali, in due contesti diversi che si possono verificare:

1. siti che prevedono la registrazione dell'utente per partecipare alle attività, tramite procedure di iscrizione in cui vengono raccolti dati come nome, cognome, indirizzo di posta elettronica, data di nascita, residenza, domicilio e altri dati utili all'identificazione
2. siti web che non prevedono la registrazione dell'utente

<u>Caso 1:</u>
Il gestore è tenuto a :

1. fornire l'informativa agli interessati prima della compilazione del modulo di raccolta dati di registrazione; tale informativa deve:
    a. essere consultabile in qualsiasi momento in una apposita pagina del sito ad essa dedicata

b. indicare le finalità per le quali i dati sono raccolti e le modalità del trattamento
c. specificare quali dati di registrazione sono necessari e quali facoltativi per partecipare alle attività del sito
d. indicare per quanto tempo verranno conservati i dati personali raccolti
e. indicare all'utente come esercitare i dirittti di accesso, modifica e cancellazione dei dati, i riferimenti del titolare dei dati e dei responsabili
f. invitare l'utente a confermare, apponendo un segno di spunta in apposita casella, l'avvenuta presa visione dell'informativa ai fini della registrazione

2. il gestore, in relazione alla sensibilità dei dati trattati, deve predisporre una specificha **avvertenza di rischio** in relazione al fatto che:
   a. immettendo i propri dati sensibili e collegandoli a dati identificativi nel sito web, la persona è collegabile alla propria specifica patologia
   b. in merito al punto 2.a, deve sempre essere possibile per l'utente mantenere l'anonimato, ovvero registrarsi utilizzando nickname che non consenta di risalire all'identità della persona
   c. i dati di contatto, come la posta elettronica, forniti all'atto della registrazione non saranno pubblicati unitamente ai commenti dell'utente
   d. deve essere avvertito l'utente di porre attenzione a non utilizzare all'interno dei commenti:
      i. dati personali atti a rivelarne anche indirettamente l'identità (indirizzo email, riferimenti a luoghi, persone e circostanze, etc)
      ii. foto o video nei quali si possano identificare precisamente persone o luoghi etc)
      iii. dati che possano rivelare l'identità di terzi
   e. il gestore deve specificare se i dati immessi dall'utente sono consultabili solo dagli iscritti al sito o da qualsiasi utente che acceda al sito e che effettui ricerche interne al sito
   f. deve essere specificato se il sito presenza meccanismi di indicizzazione da parte di motori di ricerca (es Google, Yahoo…)
   g. l'utente deve essere inviato a porre un apposito segno di spunta sulla presa visione dell'avvertenza di rischio

L'interessato ha diritto, qualora non voglia più partecipare alle attività del sito, di ottenere la cancellazione dei propri dati.
I dati raccolti dal gestore devono essere opportunamente protetti per ridurre al minimo gli episodi di distruzione, perdita, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta.
I dati raccolti dal gestore devono essere riservati e non possono essere comunicati o diffusi a terzi.
Il fornitore dal cui è stato realizzato il sito e presso il quale eventualmente è ospitato e/o che effettua la manutenzione del sito, deve essere incaricato esterno al trattamento dei dati.

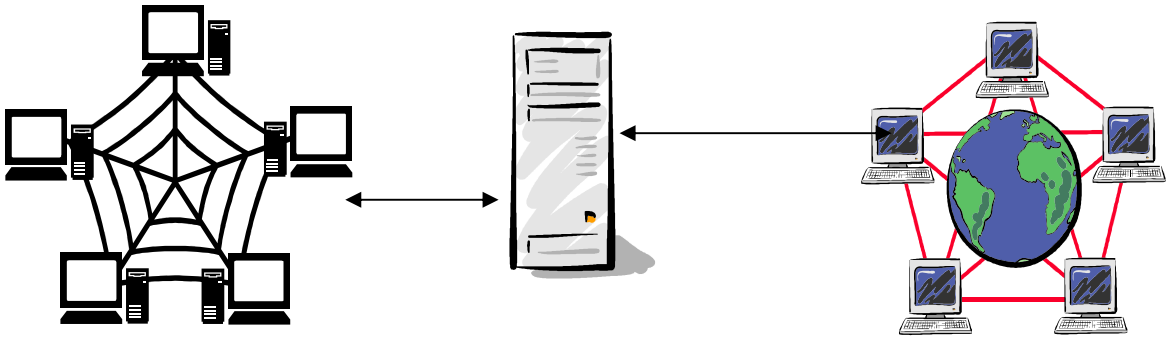
<u>Caso 2:</u>
Nel caso in cui non sia prevista la registrazione dell'utente, ai gestori non è richiesto di rilasciare l'informativa (art. 13 Codice privacy) in quanto non vi è trattamento dei dati personali.
Tuttavia al gestore è richiesto di predisporre la specifica avvertenza di rischio secondo quanto indicato precedentemente al Caso 1.

1.3.4.4. Configurazione della rete.

Presso l'Azienda USL di Parma è in corso un progetto di revisione dell'infrastruttra di rete che porterà ad alcuni importanti cambiamenti nell'arco del triennio 2015-2017, rispetto a quanto descritto di seguito.

Basandoci su un classico schema a blocchi diamo una sintetica descrizione dello schema fisico della rete aziendale.

Internet:



Il collegamento tra l'azienda USL con altre reti non fidate (ad esempio Internet) deve essere protetto da un sistema antintrusione denominato Firewall. Nel caso in esame utilizziamo un proxy che funge da filtro per le chiamate in entrata ed in uscita dalla rete interna.

Vanno delineate alcune regole al fine di evitare intrusioni indesiderate :

- tutto il traffico deve passare per il Proxy;
- solo il traffico autorizzato dal servizio può transitare per il Firewall;
- l'integrità del Firewall da accessi esterni non conformi alle regole definite sarà periodicamente verificata tramite auditing esterno;

Trasmissione di informazioni riservate: Il passaggio di informazioni riservate da una rete esterna (Internet, collegamento dial-up) deve essere protetto tramite crittografia. In particolare sono riservati i dati user-id e password, ne segue che l'autenticazione via rete deve essere crittografata.

Collegamenti via modem: I collegamenti via modem devono essere strettamente controllati. Tali collegamenti vanno possibilmente raggruppati su un asynchronous communications server, su cui verranno attivati sistemi di autenticazione; l'accesso alle risorse di rete verrà abilitato solo al completamento positivo di tale autenticazione. Dove possibile vanno attivate funzioni di logging. Quando non utilizzati, i modem collegati alle workstation devono restare spenti.

Verifiche e controlli di tali comportamenti saranno svolte nell'ambito delle attività di audit esterno delle rete.

Collegamenti tramite Reverse Proxy

Vista la crescente richiesta dei servizi aziendali da parte di strutture accreditate (farmacie, case di cura, etc...) si è reso necessario alzare il livello di controllo qualitativo del traffico in entrata. Il Reverse Proxy pone una barriera tra ciò che l'azienda può erogare ed il mondo esterno limitando la visibilità della rete aziendale ed aumentando il controllo sulle richieste esterne.

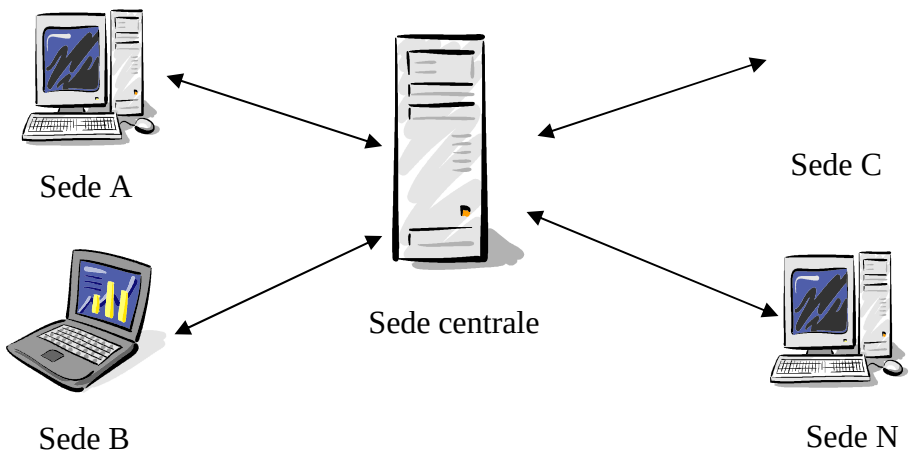
Collegamenti via VPN: è una rete privata instaurata tra soggetti che utilizzano un sistema di trasmissione pubblico e condiviso come per esempio internet. Lo scopo delle reti VPN è di dare alle aziende le stesse possibilità delle linee private in affitto ad un costo inferiore sfruttando le reti condivise pubbliche.

Le reti VPN utilizzano collegamenti che necessitano di autenticazione per garantire che solo gli utenti autorizzati vi possano accedere, per garantire la sicurezza che i dati inviati in Internet non vengano intercettati o utilizzati da altri non autorizzati, esse utilizzano sistemi di crittografia.

Le reti VPN sicure adottano dunque protocolli che provvedono a cifrare il traffico transitante sulla VPN. Oltre alla cifratura, una VPN sicura deve prevedere nei suoi protocolli dei meccanismi che impediscano violazioni della sicurezza, come ad esempio il furto dell'identità digitale o l'alterazione dei messaggi

Tipo	***Nome documento***
Elenco Connessioni VPN	T0305 Allegato n.17

Intranet:



Trattandosi di connessioni interne, quindi ragionevolmente sicure, il traffico di rete interno non subisce particolari trattamenti di sicurezza se non quelli riconducibili al software utilizzato. Dalla conformità della struttura della rete se ne evince che la comunicazione tra la sede N e la sede C passa sempre per la sede centrale posta presso il Servizio RIT.

Server:

Con il termine server si intendono tutte quelle apparecchiature che forniscono dei servizi. Tali apparati ricoprono un ruolo fondamentale all'interno dell'azienda in quanto rappresentano lo snodo tra il servizio informatico ed i servizi che richiedono accesso alle procedure.

Il personale addetto alla loro attività deve essere in possesso di uno skill altamente qualificato ed il più possibile aggiornato. Tali soggetti sono i responsabili del corretto funzionamento dei server e degli accessi a tali macchine.

Tali operatori vengono identificati all'interno del servizio come 'amministratori di rete'.

Sotto la loro supervisione ricade anche la gestione, manutenzione e sicurezza di tutti gli apparati che costituiscono per intero la rete fisica aziendale come gli switches o similari.

Documenti allegati:

Tipo	***Nome documento***
Linee Trasmissione Dati	T0301 Allegato n.9
Elenco Strutture Aziendali	T0302 Allegato n.10
Elenco Server Aziendali	T0304 Allegato n.15

1.3.4.5. Sistema di protezione dati (backup)

Un aspetto molto importante della sicurezza dei dati è rappresentato dalla loro conservazione. Il controllo degli accessi alle macchine server è strettamente controllato dalla sicurezza di rete, dalle infrastrutture predisposte nei locali nonchè dai controllo di accesso ai locali stessi. Malgrado tutti i possibili controlli che possono essere messi in opera non vi è nessuna garanzia della conservazione delle informazioni.

Un ulteriore passo per salvaguardare i dati, è quello di predisporre una procedura di backup. In azienda, al momento è predisposta una batteria di nastri che esegue giornalmente il salvataggio dei dati presenti nei server. Si possono ottenere così due livelli di sicurezza in quanto la copia della domenica viene clonata e conservata in cassaforte per un mese.

1.3.4.6. Conservazione password e chiavi cassaforte

Oltre alle procedure per il controllo della password ed ai normali controlli di accesso ai locali, si sta approntando un'altro grado di protezione al fine di evitare intrusioni o manomissioni: le password di amministrazione delle principali macchine di lavoro dell'azienda verranno singolarmente riposte all'interno di buste sigillate. Tali buste vanno riposte in un apposito luogo ad accesso fortemente ristretto, quale una cassaforte a combinazione o similari. Qualora le esigenze lo rendesse necessario si potranno aprire le buste, previo cambio della password e la sigillazione delle stesse. Stesso discorso vale per le chiavi delle casseforti le quali

vanno prelevate la mattina e riposte al termine della giornata lavorativa in un luogo protetto. Resta inteso che qualunque variazione delle password o la scelta del luogo di conservazione va comunicato solo a chi di dovere.

Videosorveglianza

Con il provvedimento del 29 aprile 2004 il Garante ha specificato in maniera approfondita il provvedimento del 29 novembre 2000 e ha individuato 4 principi da osservare affinchè la videosorveglianza sia legittima: **liceità, necessità, proporzionalità, finalità**.

Il principio di liceità consente la raccolta e l'uso delle immagini qualora esse siano necessarie per adempiere ad obblighi di legge o siano effettuate per tutelare un legittimo interesse. La videosorveglianza è consentita, **senza necessità di alcun consenso**, qualora essa sia effettuata nell'intento di perseguire fini di tutela di persone e beni rispetto a possibili aggressioni, furti, rapine, atti di vandalismo, prevenzione di incendi, sicurezza del lavoro.

Secondo il principio di necessità va escluso ogni uso superfluo ed evitati eccessi e ridondanze nei sistemi di videosorveglianza. La raccolta e l'uso delle immagini deve essere proporzionale agli scopi perseguiti.

Il principio di proporzionalità pur consentendo margini di libertà nella valutazione da parte del titolare del trattamento, non comporta però scelte del tutto discrezionali e insindacabili.

Secondo il principio di finalità gli scopi perseguiti devono essere determinati, espliciti e legittimi. Ciò comporta che il titolare possa perseguire solo finalità di sua pertinenza. La videosorveglianza non ha quindi finalità di sicurezza pubblica, prevenzione o accertamento dei reati che competono invece solo ad organi giudiziari o di polizia giudiziaria oppure a forze armate o di polizia.

L'eventuale **conservazione temporanea delle immagini** deve essere commisurata al grado di indispensabilità e per il solo tempo necessario e predeterminato a raggiungere la finalità perseguita. La durata della conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione.

Le ragioni delle scelte di conservazione delle immagini devono essere adeguatamente documentate in un atto autonomo conservato presso il titolare ed il responsabile del trattamento e ciò anche ai fini della eventuale esibizione in occasione di visite ispettive.

Tipo	***Nome documento***
Videosorveglianza	P0301 Allegato n.18

1.4. Addebiti Telefonici

Per quanto concerne la trattazione dei dati sia in formato elettronico che cartaceo del traffico telefonico aziendale si rimanda alla disposizione con protocollo numero 104825/int del 24 Novembre 2006.

1.5. Archiviazione Cartacea

La gestione degli archi cartacei è demandata alle singole strutture le quali provvederanno alla sistemazione, manutenzione e controllo degli stessi nei limiti delle posiibilità e delle strutture.

1.6. Formazione / Informazione

In questi ultimi anni sono stati approntati dei piani di sensibilizzazione inerenti la sicurezza della gestione dei dati sensibili in modo da affrontare, per ogni situazione specifica, le particolari problematiche. Il piano di formazione impostato è stato progettato con l'obiettivo di informare i responsabili e gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni. A tale fine, il piano è stato suddiviso sulla base delle specifiche esigenze di ciascuna area aziendale in relazione alla natura dei dati trattati e dei rischi generici o specifici che incombono sui dati e sui criteri e modalità di evitare tali rischi.

I contenuti esposti sono:

1) Informazioni sul D. Lgs. 196/2003, e sui principi legislativi comunitari.
2) Funzionamento della normativa nell'ambito dei diritti del cittadino e comportamenti aziendali.
3) Rischi possibili e probabili cui sono sottoposti i dati (con richiami a casi di crimini informatici, frodi, abusi, danni).
4) Misure di sicurezza tecniche, organizzative e comportamentali deputate alla prevenzione dei rischi.
5) Comportamenti e modalità di lavoro per prevenire i rischi.

1.6.1. Informativa capillare

Come precedentemente accennato, tutti i dipendenti della AUSL sono formalmente incaricati dei trattamenti di dati personali e sensibili nei rispettivi ambiti di trattamento.
Per questo motivo si è deciso di attuare una politica capillare d'informazione sui temi delCodice Privacy (D.Lgs. 196/03) e sui comportamenti necessari a tutelare il diritto del cittadino alla privacy.
E' in via di valutazione la modalità da adottare per comunicare capillarmente a tutti i dipendenti e collaboratori detta informativa.

1.6.2. Pubblicazione sulla intranet

Sulla intranet aziendale sarà pubblicata un'informativa generale riguardante gli obiettivi e i contenuti del D.Lgs. 196/2003.

ELENCO ALLEGATI

Allegato 1: P0700 Nomenclatura documenti
Allegato 2: P0701 Regole di gestione/conservazione delle credenziali di autenticazione
Allegato 3: P0702 Disciplinare tecnico per l'uso di Internet e della Posta elettronica
Allegato 4: T0201 Analisi dei rischi per apparecchiature Server
Allegato 5: T0202 Analisi dei rischi per Workstation
Allegato 6 T0203 Analisi dei rischi per apparecchiature di rete
Allegato 7: T0204 Analisi dei rischi per le applicazioni
Allegato 8: T0205 Misure di sicurezza
Allegato 9: T0301 Linee di trasmissione dati
Allegato 10: T0302 Elenco Strutture Aziendali
Allegato 11: T0101 Elenco Responsabili dei Trattamenti
Allegato 12: T0102 Elenco Responsabili Esterni
Allegato 13: T0103 Elenco Trattamenti
Allegato 14: P0703 Regolamento per l'utilizzo degli strumenti informatici dell'Azienda USL di Parma
Allegato 15: P0704 Linee guida e "buone pratiche" per la manipolazione dei file
Allegato 16: T0304 Elenco Server Aziendali
Allegato 17: T0305 Elenco connessioni VPN
Allegato 18: P0301 Videosorveglianza
Allegato 19: P0401 Linee di indirizzo per la gestione del dossier sanitario nelle aziende sanitarie di AVEN
Allegato 20: P0601 Reperibilità Servizio Risorse Informatiche e Telematiche-1.doc
Allegato 21: P0602 Allegato tecnico.doc

Nome Documento :P0700

Oggetto : Nomenclatura documenti

Data Ultima Modifica:31/03/2015

Si definisce di seguito il sistema di numerazione delle procedure riguardanti il sistema di sicurezza e la documentazione del DPS in generale. Ogni documento sarà numerato secondo il seguente schema:

N YXX

Dove il significato delle lettere è il seguente....

Simbolo	***Valore***	***Significato***
N	P	Documento di procedura o definizione
	S	Schema, Diagramma o Flow Chart
	T	Tabella

Simbolo	***Valore***	***Significato***
Y	0	Sistema di sicurezza
	1	Identificazione e suddivisione delle funzioni e delle responsabilità.
	2	Analisi ed abbattimento del rischio
	3	Catalogazione delle fonti di dati e dei computers
	4	Configurazione e gestione degli apparati di rete, dei computers, sistemi operativi, applicativi. Procedura di aggiornamento o informativa.
	5	Autentificazione Utenti
	6	Integrità dei dati e disponibilità dei sistemi (backup, disaster recovery, gruppi di continuità)
	7	Formazione del personale

Simbolo	***Valore***	***Significato***
XX	XX	Progressivo all'interno dell'area tematica

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : P0701

Oggetto : Regole di gestione/conservazione delle credenziali di autenticazione

Data Ultima Modifica :31/03/2015

La definizione e la gestione dell'account di autenticazione da parte di un utente ad un trattamento dati sono caratterizzate dalle seguenti regole comportamentali, che lo rendono responsabile di qualsiasi operazione di violazione e/o danneggiamento riconducibili a tali credenziali di accesso ai dati:

- La lunghezza minima della password è di 8 caratteri;
- La password deve contenere almeno un carattere alfabetico ed uno numerico;
- La password non deve contenere più di due caratteri identici consecutivi;
- La password non deve essere simile alla password precedente;
- La password non deve contenere il nome dell'utente o user-id;
- La password deve essere cambiata almeno ogni 3 mesi;
- La password non deve essere comunicata ad altri utenti.

Laddove la tecnologia lo permette, tali regole sono rese obbligatorie dal software applicativo, altrimenti è responsabilità dell'utente stesso applicarle e rispettarle.

Alcuni suggerimenti utili, per creare una password efficace, sono che la password deve essere facile da ricordare e presentare al tempo stesso difficoltà alle terze parti, che cercano di individuarla. Questo significa, che è preferibile scegliere una password, che **NON** sia riconducibile alla denominazione della propria attività piuttosto che a il numero di targa della propria auto o il nome di un proprio familiare.

E' in corso l'integrazione di tutti gli applicativi con il sistema centrale di autenticazione aziendale LDAP e è in corso la messa in dominio di tutte le postazioni di lavoro.
Al termine di tali lavori l'utente sarà vincolato all'utilizzo di una utenza propria unica e personale sulle postazioni di lavoro e sugli applicativi, con il vantaggio dell'univocità della password ma l'obbligo di utilizzo della propria utenza personale in qualunque contesto.

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : P0702

Oggetto : Disciplinare tecnico per l'uso di Internet e della Posta elettronica

Data Ultima Modifica 23/07/2015

USO DI INTERNET:

1) L’Azienda consente di utilizzare Internet, durante l’orario di lavoro, esclusivamente per finalità lavorativa. L’utilizzo è consentito comunque sempre nei limiti di quanto espresso al punto 3).

2) La richiesta di attivazione alla navigazione deve essere inoltrata al Responsabile della Sicurezza, per approvazione, dal Responsabile del trattamento dei dati da cui dipende il dipendente, per iscritto su apposito modulo aziendale che ne riporta le motivazioni e debitamente sottoscritto dal Responsabile stesso. Il modulo può essere inoltrato in cartaceo o in formato elettronico (scansione) tramite email aziendale.

3) Qualunque attività che appesantisca il traffico o i servizi sulla rete deteriora il rendimento complessivo della rete. Si raccomanda pertanto di effettuare queste operazioni solo se strettamente necessarie e dopo aver consultato il Responsabile della Sicurezza, in modo da ridurre il più possibile l'impatto sulla rete.

   In particolare si raccomanda di:

   a) Effettuare i trasferimenti di archivi voluminosi negli orari e nelle modalità indicate dal Responsabile della Sicurezza;

   b) Non effettuare il download di software, file di grandi dimensioni, file musicali e filmati dalla rete senza prima essersi consultati con il Responsabile della Sicurezza. Il software, le immagini e i filmati reperibili dalla rete, oltre a provocare deterioramento delle prestazioni di rete per le loro consistenti dimensioni, possono essere coperti da brevetti e/o vincoli di utilizzo di varia natura.

4) L’Azienda utilizza sistemi di filtro del traffico internet che consentono di creare una black list di siti considerati pericolosi o non attinenti con l’attività lavorativa e di porre limiti all’utilizzo della banda per le operazioni di upload e download

   I siti sono filtrati in logica di “lista nera”, ovvero siti non accessibili a fronte di una accessibilità aperta ma tracciata tramite proxy.

5) L’Azienda memorizza temporaneamente in appositi file di log i dati relativi al traffico Internet.

   I log del traffico internet sono di 2 tipologie e contengono le seguenti informazioni:

   <u>Log di accesso</u>:

   - Ip di provenienza della postazione da cui è effettuato l’accesso
   - L’utente del proxy
   - Gli url visitati con data e ora di accesso

   <u>Log di black list</u>

   - Ip di provenienza della postazione da cui è effettuato l’accesso
   - L’utente del proxy
   - Gli url richiesti in black list con data e ora di richiesta di accesso

Sono archiviati sul server del proxy per un periodo di tempo pari a 6 mesi, sono consultabili dal Responsabile della Sicurezza e dall'Amministratore di sistema

6) Comportamenti palesemente scorretti da parte di un utente, quali:

a) Violare la sicurezza di archivi e computers della rete;

b) Violare la privacy di altri utenti della rete, leggendo o intercettando la posta elettronica loro destinata;

c) Compromettere il funzionamento della rete e degli apparecchi che la costituiscono con programmi (virus, trojan horses, ecc.) costruiti appositamente

d) Accedere, consultare o scaricare materiale illecito

costituiscono veri e propri crimini elettronici e come tali sono punibili dalla legge.

7) L'Azienda si riserva di effettuare controlli saltuari e occasionali in conformità alla legge, al fine di verificare la corretta funzionalità del sistema, la sua sicurezza ed eventuali utilizzi impropri delle risorse aziendali. Tali controlli vengono effettuati in prima istanza attraverso il monitoraggio di dati in forma aggregata che consentono di verificare i siti maggiormente acceduti; in caso di accesso a siti non pertinenti all'attività lavorativa o illeciti viene analizzato, con dati di maggior dettaglio, da quali risorse aziendali è stato tentato l'accesso.

8) In caso di rilevazione di abusi il Responsabile della Sicurezza invierà in via preventiva un avviso collettivo a tutti i dipendenti.

9) In caso di reiterati accessi abusivi il Responsabile della Sicurezza invierà un avviso individuale al Responsabile del trattamento del servizio di afferenza della risorsa aziendale che ha effettuato l'accesso, il quale Responsabile provvederà a predisporre le opportune misure nei confronti del dipendente

10) Il Responsabile della Sicurezza è tenuto a fornire il contenuto dei file di log relativi a richieste circostanziate e puntuali delle Autorità preposte, dopo aver concordato modalità e tempi con il Titolare e senza essere tenuto ad avvisare preventivamente il dipendente e il Responsabile del trattamento del Servizio di afferenza del dipendente

POSTA ELETTRONICA

1) L'utilizzo della posta elettronica è consentito solo per fini lavorativi e non per uso personale.

2) Deve essere cura del dipendente procedere alla cancellazione e/o al salvataggio nei propri archivi personali, degli eventuali messaggi di posta elettronica personale ricevuti da terzi o inviati a terzi.

3) Non inviare per posta elettronica grosse moli di dati; indicare (ove possibile) la locazione (URL) dei dati nel messaggio, rendendoli disponibili per il prelievo o la consultazione sulla rete. Non è consentito allegare file di dimensioni superiori ai 10M.

4) Non inviare messaggi ad un numero eccessivo di destinatari; in caso di necessità di mailing list molto numerose contattare il Responsabile della sicurezza al fine di predisporre la migliore configurazione del sistema

5) Non è consentito, salvo specifica autorizzazione del Responsabile della sicurezza, utilizzare più di 800M di spazio per la propria casella di posta

aziendale. Il dipendente ha l'onere di cancellare o archiviare i messaggi e gli allegati in appositi archivi predisposti dall'Azienda.

6) L'Azienda memorizza temporaneamente in appositi file di log i dati relativi alla Posta elettronica.

I log della posta elettronica contengono le seguenti informazioni

- Mittente
- Destinatario
- Data e ora di invio o ricezione
- Stato della transazione

Sono archiviati sul server di posta per un periodo di tempo pari 5 anni, sono consultabili dal Responsabile della Sicurezza e dall'Amministratore di sistema

7) L'Azienda conserva una copia di backup dei messaggi della posta elettronica aziendale. Il backup viene effettuato aggiornando in tempo reale la fotografia (transazioni e contenuto dei messaggi) della casella di posta. Il recupero è consentito con profondità di 90 giorni. L'insieme delle immagini viene archiviato settimanalmente su apposita unità di backup aziendale e mantenuto per 30 giorni. Le copie di backup sono accessibili da parte del Responsabile della Sicurezza e dell'Amministraotre di sistema .

8) Al fine di garantire la massima riservatezza e cooperazione tra i lavoratori, nonché la continuità dell'attività lavorativa in caso di assenze, l'Azienda predispone e impone:

a. L'utilizzo di indirizzi di posta condivisi tra più lavoratori (indirizzi generici di segreterie/dipartimenti/servizi..), che devono essere utilizzati in affiancamento alle caselle individuali, per gestire la posta condivisa con altre persone.

b. In caso di assenze pianificate è fatto obbligo di utilizzare il servizio di predisposizione del messaggio di risposta automatica. Il messaggio deve contenere indicazioni rispetto ad alternative modalità di contatto della struttura.

c. In caso di assenze non programmate è consigliato, dove possibile, utilizzare il servizio di webmail per impostare il risponditore automatico.

d. In ogni caso il dipendente, in caso di assenza improvvisa o prolungata, deve essere messo in condizione di delegare un altro lavoratore (fiduciario) alla verifica dei propri messaggi di posta e all'inoltro, al Titolare o ai Responsabili, di quelli ritenuti rilevanti ai fini dell'attività lavorativa. Tale attività da parte del fiduciario deve essere verbalizzata a cura del Titolare e ne deve essere data informazione all'interessato alla prima occasione utile. La comunicazione deve avvenire tramite email o fax al Responsabile della sicurezza e/o all'Amministratore di sistema

e. Il Titolare, perdurando l'assenza oltre i 30 giorni lavorativi, può predisporre, mediante il Responsabile della Sicurezza e l'Amministratore di sistema, l'apertura della posta elettronica, avvertendo l'interessato.

f. I messaggi di posta elettronica devono contenere obbligatoriamente la firma con le indicazioni di titolo, nome e cognome, ruolo aziendale, servizio di appartenenza, indirizzo, recapiti telefonici aziendali, fax e

email aziendale. Nel messaggio deve essere riportata in calce anche la dicitura “Il presente messaggio non ha natura personale, le risposte potranno essere conosciute da altro personale dell’Azienda USL di Parma”. Il Servizio RIT mette a disposizione un formato unico per la firma aziendale.

9) In caso di risoluzione del contratto di lavoro il Titolare ha la facoltà di cancellare, archiviare o rendere consultabili per un certo periodo i messaggi di posta elettronica

10) La violazione, anche singola, dei punti precedenti, autorizza il Responsabile della Sicurezza, ad effettuare una segnalazione diretta al dipendente. In casi di violazioni reiterate il Responsabile della sicurezza ne darà comunicazione al Responsabile del trattamento a cui il dipendente fa riferimento.

Fra gli utenti dei servizi telematici di rete, prima fra tutte la rete Internet, si sono sviluppati nel corso del tempo una serie di "tradizioni" e di "principi di buon comportamento" (galateo) che vanno collettivamente sotto il nome di "netiquette". Riportiamo di seguito un breve sunto dei principi fondamentali della "netiquette", a cui tutti sono tenuti ad adeguarsi.

a) Se si manda un messaggio, è bene che esso sia sintetico e descriva in modo chiaro e diretto il problema. Specificare sempre, in modo breve e significativo, l'oggetto (campo "Subject") del testo incluso nella mail. Se si utilizza un "signature file", mantenerlo breve e significativo;

b) Se si risponde ad un messaggio, evidenziare i passaggi rilevanti del messaggio originario, allo scopo di facilitare la comprensione da parte di coloro che non lo hanno letto, ma non riportare mai sistematicamente l'intero messaggio originale, se non quando sia necessario;

c) Non pubblicare mai, senza l'esplicito permesso dell'autore, il contenuto di messaggi di posta elettronica;

d) Non inviare tramite posta elettronica messaggi pubblicitari o comunicazioni che non siano state sollecitate in modo esplicito;

e) Non essere intolleranti con chi commette errori sintattici o grammaticali. Chi scrive, è comunque tenuto a migliorare il proprio linguaggio in modo da risultare comprensibile alla collettività.

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : T0201

Oggetto : Analisi dei rischi per apparecchiature Server

Data Ultima Modifica :31/03/2015

Vengono di seguito riportate le principali categorie di rischio a cui sono soggette le apparecchiature server.

Interruzione di Servizi

to	***I.R.***
Assenza di alimentazione	5
Manomissione volontaria	2
Accesso non autorizzato alla rete	5
Presenza di virus	5
Guasti Hardware	4
Errori umani non volontari	3
Uso improprio di autorizzazione di accesso	3
Sottrazioni autorizzazioni di accesso	1

6) **Manomissioni archivi**

Evento	***I.R.***
Incuria nella gestione	2
Comportamenti sleali o fraudolenti	1
Accesso non autorizzato alla rete	4
Guasti ai supporti di memorizzazione	6
Sottrazioni autorizzazione di accesso	1
Presenza Virus	3

Intercettazione e diffusione dati

Evento	***I.R.***
Accesso non autorizzato alla rete	4
Uso improprio di autorizzazione di accesso	4
Uso improprio dei dati	2
Sottrazioni autorizzazione di accesso	3
Comportamenti sleali o fraudolenti	3

Evento	***I.R.***
Presenza di Virus	3

Glossario:
I.R. : Indice di rischio
Rappresentato con una scala da 1 a 10 (10 = massimo valore) indica la possibilità che un evento si verifichi.

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : T0202

Oggetto : Analisi dei rischi per Workstation

Data Ultima Modifica :31712/2015

Vengono di seguito riportate le principali categorie di rischio a cui sono soggette le apparecchiature workstations.

Interruzione di Servizi

to	***I.R.***
Assenza di alimentazione	7
Manomissione volontaria	4
Accesso non autorizzato alla rete	5
Presenza di virus	5
Guasti Hardware	5
Errori umani non volontari	5
Uso improprio di autorizzazione di accesso	5
Sottrazioni autorizzazioni di accesso	5

7) **Manomissioni archivi**

Evento	***I.R.***
Incuria nella gestione	6
Comportamenti sleali o fraudolenti	3
Accesso non autorizzato alla rete	5
Guasti ai supporti di memorizzazione	4
Sottrazioni autorizzazione di accesso	6
Presenza Virus	5

Intercettazione e diffusione dati

Evento	***I.R.***
Accesso non autorizzato alla rete	5
Uso improprio di autorizzazione di accesso	5
Uso improprio dei dati	1
Sottrazioni autorizzazione di accesso	5
Comportamenti sleali o fraudolenti	2

Evento	***I.R.***
Presenza di Virus	4

Glossario:

I.R. : Indice di rischio

Rappresentato con una scala da 1 a 10 (10 = massimo valore) indica la possibilità che un evento si verifichi.

Nome Documento : T0203

Oggetto : Analisi dei rischi per apparecchiature di rete

Data Ultima Modifica : 31/03/2015

Vengono di seguito riportate le principali categorie di rischio a cui sono soggette le apparecchiature di rete.

Interruzione di Servizi

to	***I.R.***
Assenza di alimentazione	5
Manomissione volontaria	2
Accesso non autorizzato alla rete	3
Presenza di virus	1
Guasti Hardware	2
Errori umani non volontari	3
Uso improprio di autorizzazione di accesso	3
Sottrazioni autorizzazioni di accesso	3

8) **Intercettazione e diffusione dati**

Evento	***I.R.***
Accesso non autorizzato alla rete	3
Uso improprio di autorizzazione di accesso	2
Sottrazioni autorizzazione di accesso	2
Comportamenti sleali o fraudolenti	4

Glossario:

I.R. : Indice di rischio

Rappresentato con una scala da 1 a 10 (10 = massimo valore) indica la possibilità che un evento si verifichi.

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : T0204

Oggetto : Analisi dei rischi per le applicazioni

Data Ultima Modifica :31/03/2015

Vengono di seguito riportate le principali categorie di rischio a cui sono soggette le applicazioni.

Manomissioni archivi

Evento	***I.R.***
Incuria nella gestione	3
Comportamenti sleali o fraudolenti	3
Accesso non autorizzato alla rete	5
Guasti ai supporti di memorizzazione	2
Sottrazioni autorizzazione di accesso	5
Presenza Virus	4

9) **Intercettazione e diffusione dati**

Evento	***I.R.***
Accesso non autorizzato alla rete	4
Uso improprio di autorizzazione di accesso	5
Uso improprio dei dati	4
Sottrazioni autorizzazione di accesso	5
Comportamenti sleali o fraudolenti	3
Presenza di Virus	4

Glossario:

I.R. : Indice di rischio

Rappresentato con una scala da 1 a 10 (10 = massimo valore) indica la possibilità che un evento si verifichi.

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : T0205

Oggetto : Misure di sicurezza

Data Ultima Modifica :31/03/2015

Misure	Descrizione dei rischi contrastati	Trattamenti interessati	Misure già in essere	Misure da adottare	Struttura o persone addette all'adozione
Stock in magazzino di parti di ricambio specifiche	Deterioramento periferiche Input/Output	Tutti	Stato Effettivo	Controllo forniture di ricambio	Servizio RIT
Presenza UPS	Assenza alimentazione di rete	Tutti	In corso revisione delle sedi	Monitoraggio del corretto funzionamento delle apparecchiature e implementazione nuove sedi	Servizio RIT
Stock in magazzino di parti di ricambio specifiche	Rottura schede interne	Tutti	Stato Effettivo	Controllo forniture di ricambio	Servizio RIT
Installazione di software antivirus, protezioni hardware associate, politiche di gestione utenti.	Infezione delle macchine da attacchi malaware	Tutti	Stato Effettivo	Controllo forniture di nuovi aggiornamenti	Servizio RIT
Installazione di software antivirus, protezioni hardware associate, politiche di gestione utenti.	Infezione delle macchine da attacchi spam	Tutti	Stato Effettivo	Monitoraggio del corretto funzionamento delle apparecchiature	Servizio RIT

Accessi alle attrezzature controllate	Furto	Tutti	In fase di miglioramento	Incremento delle procedure di prevenzione	Servizio RIT
Istruzioni e formazione al personale	Uso improprio di credenziali	Tutti	Stato Effettivo – dopo aver effettuato corsi.	Aggiornamenti e corsi	Servizio RIT
Istruzioni e formazione al personale	Archiviazione errata della documentazione	Tutti	In corso	Aggiornamenti e corsi e documentazione	Servizio RIT
Monitoraggio e apparecchiature di scorta	Mancanza di collegamenti di rete	Tutti	Stato Effettivo	Aggiornamento del personale e controllo magazzino	Servizio RIT
Messa in sicurezza della stanza dove risiedono le apparecchiature	Danni provocati da eventi accidentali	Tutti	Stato Effettivo	Controlli e monitoraggio di consistenza apparati di sicurezza	Servizio RIT
Operazioni Backup	Perdita dati accidentale e dolosa	Tutti	Stato Effettivo	Controlli di consistenza apparati di sicurezza	Servizio RIT

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : T0301

Oggetto : Linee di trasmissione dati

Data Ultima Modifica :24/03/2015

Di seguito le linee di trasmissione dati per la connettività delle sedi aziendali

		Comune - Sede	Indirizzo	Attuale TGU	BMA	BMG	BANDA REAL TIME DEDICATA	COPERTURA ESTESA	ALTA AFFIDABILITA
1	**Ospedale di Borgotaro**	**Borgotaro Distretto / Ospedale**	Via dei Benefattori 12	52513340615 52513340604	**6,5M**	**4M**	320	SI	**SI**
2	Parma	**Parma Cup Lubiana Parma Est**	Via Leonardo Da Vinci 43	52113046714	**6,5M**	**4M**	320	SI	**SI**
3		**Fidenza ex Collegio gesuiti Berenini**	Via Berenini 151	52413347144-5	**10M**	**10M**	400	SI	**SI**
4	Parma	**Parma Via Vasari**	Via Vasari	052113048403 - 052113048405	**100M**	**100M**	320	NO	**NO**
5	Parma	**Parma Distretto**	Viale Basetti 8	52113046716	**10M**	**10M**	320	SI	**SI**
6	Valli Taro e Ceno	**Bedonia**	Piazza Caduti 1	52513340610	**6,5M**	**4M**	320	SI	**SI**
7	Fidenza	**Fontanellato Poliambulatorio**	Via XXIV Maggio	52113047985	**3,25M**	**2M**	200	NO	**NO**
8	Sud-Est	**Collecchio Veterinari**	Via Spezia 89	52113046721	**3,25M**	**2M**	480	NO	**NO**
9	Parma	**Parma Programma Adolescenza**	Via Mazzini 2	52113046722	**3,25M**	**2M**	240	SI	**SI**

10	Parma	**Parma Spazio Giovani**	Via Melloni 1/B	52113046723	**6,5M**	**4M**	120	SI	**SI**
	Parma	**Via Turchi**							
11	Valli Taro e Ceno	**Centro Medico Borgotaro**	Via Bellinzona 2	52513340611					
12	Parma	**San Polo di Torrile**	Via M.Margotti 2	52113046727	**6,5M**	**4M**	640	SI	**SI**
14		**Traversetolo**	Via IV Novembre 33	52113046731	**20M**	**20M**	320	SI	**SI**
15	Parma	**Parma Via XXII Luglio**	Via XXII Luglio	52113046732	**6,5M**	**4M**	480	SI	**SI**
16	Parma	**Parma Via del Campo**	Via Giuseppe del Campo 12	52113046735	**10M**	**10M**	400	SI	**SI**
17	Parma	**Parma Cup Via Verona**	Via Verona	52113046736	**10M**	**10M**	480	SI	**SI**
18	Parma	**Parma Sert , Parma**	strada dei mercati 15	52113040029	**10M**	**10M**	200	SI	**SI**

19	Sud-Est	**Dialisi Sala Baganza**	Strada del Mulino	52113046406	**6,5M**	**4M**	400	SI	**SI**
20	Parma	**Don Gnocchi**	Piazzale dei Servi 3	52113046742	**1,6M**	**1M**	240	NO	**NO**
21	Valli Taro e Ceno	**Nuova linea Medesano**	Piazza Rastelli 2	52513340721	**6,5M**	**4M**	360	SI	**SI**
				525422177					
22	Parma	**Parma**	V. R. I. BOCCHI angolo via Savani	52113048800	**10M**	**10M**		SI	**SI**
23	Valli Taro e Ceno	**bardi**	Via Arandora Star 11	52513340677	**6,5M**	**4M**	320	SI	**SI**
				525733017					
24	Parma	**Parma Drop-In**	Strada dei Mercati 9/B	52113048975	**6,5M**	**4M**	-	SI	**SI**

25		**Parma Salute Mentale(c/o Gruppo appartamento)**	Via Po' 72	52113048658	**?**	**?**	-	NO	**NO**
26	Valli Taro e Ceno	**Veterinari Borgotaro**	Via G. Micheli 2	52513340803	**6,5M**	**4M**	-	SI	**SI**
27	Sud-Est	**Sede AUSL Via Perlasca FELINO**	Via Perlasca 11	52113048232	**6,5M**	**4M**	-	SI	**SI**
29	Fidenza	**Centro Casa Il Ponte**	Via Piave 19/A	52413347016	**3,25M**	**2M**	-	SI	**SI**
30	Sede Centrale	**Magazzino Economale**	Via Franklin, 31	52113048397	**3,25M**	**2M**	320	SI	**SI**
31		**Nuova senologia c/o Ospedale Maggiore e, Padiglione Braga c/o Azienda Ospedaliera,**	Nuova senologia c/o , Via Gramsci, 14		**100M**	**100M**	1000	SI	**SI**
			Distribuzioni farmaci						
			Guardia medica Rasori						

		Distribuzione farmaci, Guardia Padiglione Rasori, Punto Bianco nel monoblocco	Punto bianco						
	Parma		Braga, via Gramsci						
32	Parma	**Parma - Sert Via del Taglio**	Via del Taglio 2	52113346375	**3,25M**	**2M**	320	SI	**SI**
	Sede Centrale	**Centrale trsporti ordinari**	Via del Taglio 6	?	**10M**	**10M**		SI	**SI**
33	Sud-Est	**Corniglio (PR)**	Piazza Castello, 1/3	52113054096	**3,25M**	**2M**	320	SI	**SI**
34	Parma	**Sorbolo**	Via Gruppini 4/B	52113053887	**3,25M**	**2M**	0	SI	**SI**
35	Parma	**Parma - centro autismo**	Via La Spezia, 30 o via Spezia 142????	52113053889	**10M**	**10M**	320	SI	**SI**
36	Fidenza	**Centro disturbi Cognitivi, Fidenza**	Via Don Tincati, 5	52413347151	**20M**	**20M**	0	SI	**SI**
28	Ospedale di Vaio	**Ospedale di Vaio**	Loc. Cabriolo 97	52413346988	**100**	**100**		SI	**SI**
37	Sede Centrale	**Parma Sede**	Strada del Quartiere 2/A	52113053843 52113053851	**200**	**200**		SI	**SI**
54	Sede Centrale			52113008341	**100**	**100**		SI	**SI**

				52113008342					
71	Sede Centrale			52113347047	**7**	**7**	-	NO	**NO**
39	Parma	**Parma**	Via Carmignani 13	52113046726	**10M**	**10M**	400	SI	**SI**
40		**SalsoMaggiore**	Parco G. Mazzini 11 (no Parco Mazzini ma via Roma 9)	52413347146	**20M**	**20M**	400	SI	**SI**
41		**Noceto**	Via Gen C.A. Dalla Chiesa 30	52113053853	**100M**	**100M**	400	SI	**SI**
42		**Busseto**	Via Nicolò Paganini 13	52413347147	**10M**	**10M**	1200	SI	**SI**
43		**Collecchio**	via aldo moro/via berlinguer	52113053863	**100M**	**100M**	200	SI	**SI**
46		**SalsoMaggiore**	Parco Mazzini 4	52413347224					
		Salsomaggiore	VIA Parco Mazzini 1						
48	Sud-Est	**Montechiarugolo, Monticelli**	**Via Laura Bassi 4**	**52113046741**	**3,25M**	**2M**	**320**	**SI**	**SI**
49	Parma	**Colorno - 1 maggio**	Via Roma 16	52113004706	**3,25M**	**2M**	320	SI	**SI**

50	Parma	**Parma**	Via Burla 56	52113045165	**20M**	**20M**	1200	SI	**SI**
51	Valli Taro e Ceno	**Berceto**	Salita Pietro Silva 7	52513341114	**6,5M**	**4M**	320	SI	**SI**
52	Parma	**PARMA**	LARGO PALLI 1 (adiacente Viale Fratti)	52113004316 521130043 17	**100M**	**100M**	640	SI	**SI**
53	Sede Centrale	**Parma**	Via Spalato 2	52113048233	**30M**	**30M**	120	NO	**NO**
55	Parma	**Parma Cup Via Pintor**	Via Pintor 1	52113046773 521130467 00	**100M**	**100M**	320	NO	**NO**
56		**Fornovo - Polo Territoriale**	Via Solferino 52	52513340616 525133406 06	**100M**	**100M**	320	SI	**SI**
57		**Langhirano Distretto**	Via Roma 42/1	52113046778 521130466 94	**100M**	**100M**	320	SI	**SI**
58		**San Secondo**	Via V. Mazza 1	52113046776 521130466 96	**100M**	**100M**	320	SI	**SI**
59		**Casa di Cura Valparma Langhirano**	Via XX Settembre 22	052113046740	**3,25M**	**2M**			
62	Fidenza	**Busseto**	V. XXV APRILE 6 - 43011	52413347555	**3,25M**	**2M**	-	SI	**SI**
63	Sud-Est	**Calestano**	Via del Bocco 1	52552243	**3,25M**	**2M**	-	SI	**SI**

64	Sud-Est	**Scurano**	c/o ambulatorio Delegazione Croce Rossa	521849002	**3,25M**	**2M**	-	SI	**SI**
65	Sud-Est	**Tizzano**	Via Europa Unita 41	521869002	**3,25M**	**2M**	-	SI	**SI**
66	Sud-Est	**Monchio**	Località Monchio Basso 11	521894030	**3,25M**	**2M**	-	SI	**SI**
67	Sud-Est	**Palanzano**	Strada Del Torchio 3	521896619	**3,25M**	**2M**	-	SI	**SI**
69	Sud-Est	**Neviano degli Arduini - Casa protetta**	Loc. Ca' Bonaparte (43024), Mozzano di Neviano Arduini	521845023	**3,25M**	**2M**	-	SI	**SI**
	Sud-Est	**Neviano degli arduini - Comune**	P.zza IV Novembre 1	521845023	**3,25M**	**2M**	-	SI	**SI**
	Parma	**Colorno Polo sanitario**	via Suor Maria 1		**6,5M**	**4M**		NO	**NO**
	Valli Taro e Ceno	**Pellegrino Veterinar**	Via Roma 8/B		**3,25M**	**2M**		SI	**SI**
	Parma	**Sorbolo**	Via al Donatore 2	52113046728	**3,25M**	**2M**		SI	**SI**
		Sissa Trecasali		-					

Sono inoltre installati i PAL di Lepida nelle sedi di Parma Ugolino, Fidenza Vaio, Ospedale di Borgo val di Taro e Parma via Pintor e via Vasari.
E' in corso di attivazione il PALF per la sede di Colorno.
Sono in corso di valutazione i collegamenti infibra per le sedi di:

- Fidenza ex Collegio gesuiti, via Berenini 151
- Traversetolo, via IV Noevembre
- Salsomaggiore, via Roma 9
- Noceto, via Generale Dalla Chiesa 30
- Busseto, via Nicolò Paganini 13
- Collecchio, via Aldo Moro/via Berlinguer
- Fornovo
- Langhirano
- San Secondo
-

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : T0302

Oggetto : Elenco Strutture Aziendali

Data Ultima Modifica :Elenco in corso di verifica e aggiornamento

DIREZIONE GENERALE

MAGAZZINO ECONOMALE LA CITTADELLA	Via Franklin, 31	PARMA
DIPARTIMENTO PER LA QUALITA' (EX ARPA)	Via Spalato, 4	PARMA
SERVIZIO PREVENZIONE E PROTEZIONE AZIENDALE (EX ARPA)	Via Spalato, 4	PARMA
CHIESA DEL QUARTIERE	Strada del Quartiere	PARMA
DIPARTIMENTO TECNICO E DELLE TECNOLOGIE	Via Spalato, 2	PARMA
DIREZIONE GENERALE	Strada del Quartiere, 2 A	PARMA

DISTRETTO DI PARMA

CASA DELLA SALUTE "PINTOR"	Via Pintor, 1	PARMA
CASA DELLA SALUTE "CITTADELLA - MONTANARA"	Via Carmignani, 13	PARMA
CASA DELLA SALUTE "COLORNO - TORRILE"	Via Suor Maria, 3 (1)	COLORNO
CASA DELLA SALUTE "SAN LEONARDO"	Via Verona, 23/A	PARMA
CASA DELLA SALUTE "SORBOLO - MEZZANI"	Via Donatori, 2	SORBOLO
PARMA CENTRO	Largo Palli 5 A (1)	PARMA
CENTRO AUTISMO	Via La Spezia, 147 (142 o 30??)	PARMA
CENTRO DIURNO PSICHIATRICO "IL FILO DI ARIANNA"	Via Po, 70/72	PARMA
CENTRO PSICHIATRICO SANTI - DAY HOSPITAL	Via Vasari, 13	PARMA
CENTRO PSICHIATRICO SANTI - EX PORTINERIA (SEDE VA PENSIERO)	Via Vasari, 13	PARMA
CENTRO PSICHIATRICO SANTI - RESIDENZA	Via Vasari, 13	PARMA
APPARTAMENTI PSICHIATRICI "LO SCOIATTOLO"	Via Mamiani della Rovere, 5	PARMA
CENTRO SALUTE MENTALE PARMA OVEST (CENTRO SANTI)	Via Vasari, 13	PARMA
CENTRO SEMIRESIDENZIALE DISABILI PASUBIO	Via Pasubio, 42	PARMA
CENTRO SENOLOGICO "V. BAGNASCO"	Via Gramsci, 14 - presso AOSP - pad. MONOBLOCCO	PARMA
DEPOSITO LASTRE MAMMOGRAFICHE - EX SEDE 118 AOSP	Via Rasori, 10	PARMA
SERVIZIO GUARDIA MEDICA - EX SEDE 118 AOSP	Via Rasori, 10	PARMA
PUNTO BIANCO	Via Gramsci, 14 - presso AOSP - pad. MONOBLOCCO	PARMA
DIPARTIMENTO SANITA PUBBLICA	Via Vasari, 13/A	PARMA
NPI E NFR VIA SAVANI angolo VIA BOCCHI	Via Savani angolo via Bocchi, 10	PARMA
PADIGLIONE BRAGA - SEDE SPDC - SPOI	Via Gramsci, 14 - presso AOSP	PARMA
POLO SANITARIO PARMA CENTRO (Dentisti, Carcere (PEC e Protocollo), Farmacia fino a	Via Basetti, 8	PARMA

Dicembre) ?????		
POLO SANITARIO PARMA EST	Via Leonardo da Vinci, 42	PARMA
PROGRAMMA ADOLESCENZA VIA MAZZINI	Via Mazzini, 12 (2)	PARMA
RESIDENZA PSICHIATRICA S.POLO TORRILE	Piazzale Pertini, 2 (Via Margotti 2)	TORRILE
RESIDENZA PSICHIATRICA "PRIMO MAGGIO"	Via Roma, 16	COLORNO
RESIDENZA PSICHIATRICA CASALE MEZZANI	Via IV Novembre, 4	MEZZANI
SALA CONFERENZE INFORMATICHE	Via Vasari, 13/A	PARMA
SERT	Strada dei Mercati, 15/B	PARMA
SERT CENTRO DISTRIBUZIONE METADONE	Via del Taglio, 2	PARMA
SERT DROP-IN	Strada dei Mercati, 7/A (9/B)	PARMA
SERVIZIO FARMACEUTICO	C/O Azienda Ospedaliera Parma	PARMA
SPAZIO GIOVANI VIA MELLONI	Via Macedonio Melloni,1 (via Turchi?????)	PARMA
SPAZIO IMMIGRATI (???)	Via XXII, Luglio 27	PARMA
PARMA VIA DEL CAMPO	Via Del Campo 12	
DISTRETTO SUD EST		
AMBULATORI DI MONCHIO	Via Monchio Basso, 1	MONCHIO
AMBULATORI DI PALANZANO	P.zza Ferrari, 1 (strada del Torchio 3)	PALANZANO
AMBULATORI DI TIZZANO VAL PARMA	Via della Croce Rossa, 1/3 (via Europa Unita 41)	TIZZANO
AMBULATORI CALESTANO	Via Bocco, 1	CALESTANO
AMBULATORI CORNIGLIO	via Castello (1/3)	CORNIGLIO
CASA DELLA SALUTE SALA BAGANZA (Solo Dialisi)	Via del Mulino, 1	SALA BAGANZA
CASA DELLA SALUTE FELINO	Via Perlasca, 9 (11)	FELINO
CASA DELLA SALUTE TRAVERSETOLO	Via IV Novembre, 33	TRAVERSETOLO
CASA DELLA SALUTE LANGHIRANO	Via Roma, 42/1	LANGHIRANO
CASA DELLA SALUTE COLLECCHIO	Via Berlinguer, 2	COLLECCHIO
CASA DELLA SALUTE MONTICELLI	Via laura bassi 4	MONTICELLI
SERVIZIO VETERINARIO DI COLLECCHIO	Via La Spezia, 89/B	COLLECCHIO
DISTRETTO DI FIDENZA		
CASETTA C/O SCUOLA ELEMENTARE "COLLODI"	Via Torricelli Evangelista 8	FIDENZA
CENTRO RESIDENZIALE DISABILI "IL PONTE"	Via Piave, 5 (19/A)	FIDENZA
EX GESUITI (SIMAP, SERT, PUNTO PRELIEVI, RESIDENZA PSICHIATRICA)	Via Berenini, 151/152/153	FIDENZA
ATELIER CASTELLINA DI SORAGNA	Via Santa Maria, 32	SORAGNA
CASA DELLA SALUTE SAN SECONDO	Via M. Vitali Mazza, 1	SAN SECONDO
POLIAMBULATORI NOCETO	Via C.A. della Chiesa, 30	NOCETO
CASA DELLA SALUTE BUSSETO	Via Paganini, 13 (via XXV APRILE)	BUSSETO
POLIAMBULATORI DI FONTANELLATO	Via XXIV Maggio, 16/A	FONTANELLATO

POLIAMBULATORI SALSOMAGGIORE	Via Roma, 9/A	SALSOMAGGIORE
COMPLESSO OSPEDALIERO DI VAIO - CORPI DISTRETTUALI	Via Don Tincati n°5	FIDENZA
APPARTAMENTO BUSSETO	Via B.Bartòk	BUSSETO

DISTRETTO VALLI TARO E CENO

AMBULATORI BARDI	Via Arandora Star, 11	BARDI
CASA DELLA SALUTE BORGOTARO (attività distrettuali nell'ospedale)	Via Benefattori, 12	BORGOTARO
SERVIZIO VETERINARIO BORGOTARO	Via Micheli, 2	BORGOTARO
POLIAMBULATORI FORNOVO - PALAZZINA 1	Via Solferino, 37	FORNOVO
POLIAMBULATORI FORNOVO - PALAZZINA 2	Via Solferino, 37	FORNOVO
POLIAMBULATORI FORNOVO - PALAZZINA 3	Via Solferino, 37	FORNOVO
CASA DELLA SALUTE MEDESANO	Piazza Rastelli, 1 (2)	MEDESANO
POLO ODONTOIATRICO MEDESANO - POLO 2	P.ZZA RASTELLI,3 (2)	MEDESANO
CASA DELLA SALUTE BERCETO	Via Salita Silva (7)	BERCETO
CENTRO MEDICO BORGOTARO	Via Bellinzona 2	
PELLEGRINO VETERINARI	Via Roma 8/B	
CASA DELLA SALUTE DI BEDONIA	Piazza Caduti per la Patria 1	BEDONIA

PRESIDIO OSPEDALIERO AZIENDALE

OSPEDALE DI BORGOTARO	Via Benefattori, 12	BORGOTARO
OSPEDALE DI VAIO	Via Don Tincati n°5	FIDENZA
OSPEDALE SAN SECONDO - CORPO A (OSPEDALIERO)	Via M. Vitali Mazza, 1	SAN SECONDO

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : T0101

Oggetto : Elenco Responsabili dei Trattamenti

Data Ultima Modifica :31/08/2015

DENOMINAZIONE INCARICO	TIPO AREA PERS. DESCRIZIONE	COGNOME E NOME	DESCRIZIONE
Dir. Serv. Innovaz.e Progetti Spec./U.O. Formazione	Direz. U.O. Complessa	FERRARI LUCIANO	Dir. P.T.A.
Dir. Serv. Prevenzione e Protezione Aziendale	Direz. U.O. Complessa	BERTOLI PAOLA	Dir. Sanitari
Dir. Sviluppo ed Integr. dei Processi Amm.vi/Trasparenza e Integrità	Direz. U.O. Complessa	BLADELLI GIOVANNI	Dir. P.T.A.
DG/Direz. Dip. Valutazione e Controllo	Direz. Dipart. Az.le	ROSSI GIUSEPPINA	Dir. Medici
DG/Dir. Serv. Sviluppo e Integrazione Servizi Sanitari	Direz. U.O. Complessa	ROSSI GIUSEPPINA	Dir. Medici
DIR. ATTIVITA' SOCIO-SANITARIE	Direz. Attività Socio-San.	VOLTA PAOLO	Dir. Medici
DA/Direz. Serv. Affari Generali, Accordi e Convenzioni	Direz. U.O. Complessa	POMI MARIA CRISTINA	Dir. P.T.A.
DA/Dir. Serv. Risorse Umane e Sviluppo Organizz.	Direz. U.O. Complessa	BUZZI MARIA RITA	Dir. P.T.A.
DA/Dir. Serv. Risorse Economico-Finanziarie	Direz. U.O. Complessa	GAZZOLA CRISTINA	Dir. P.T.A.
DA/Direz. Dip. Tecnico e delle Tecnologie	Direz. Dipart. Az.le	DEOLMI ERMENEGILDO	Dir. P.T.A.
DA/Dir. Servizio Attività Tecniche	Direz. U.O. Complessa	SAVIANO RENATO MARIA	Dir. P.T.A.
DA/Dir. Serv. Acquisizione beni e servizi	Direz. U.O. Complessa	MILLI MARINA	Dir. P.T.A.
DA/Dir. Serv. Logistica, Gest. e Monit. Servizi Estern.	Direz. U.O. Complessa	DEOLMI ERMENEGILDO	Dir. P.T.A.
DA/Dir. Serv. Risorse Telematiche-Informatiche	Direz. U.O. Complessa	ANGELETTI DEBORA	Dir. P.T.A.
DS/Dir. U.O. Governo Clinico	Direz. U.O. Complessa	LOMBARDI MARCO	Dir. Medici
DS/Dir. U.O. Committ. e Accordi forn. Serv. San. Osp.	Direz. U.O. Complessa	MARCHESI LEONARDO	Dir. Medici
DS/Dir. U.O. Servizio Infermieristico e Tecnico Aziendale	Direz. U.O. Complessa	CAMMI EMILIO	Dir. Prof. Sanitarie
Direz. Dip. Sanità Pubblica	Direz. Dipart. Az.le	COZZOLINO PAOLO	Dir. Veterinari
DSP/Direz. S.I.S.P. Aziendale	Direz. U.O. Complessa	SCIARRONE FRANCA	Dir. Medici
DSP/Direz. UO Area Disc. Ig. Territorio e Amb. Costr.	Direz. U.O. Complessa	IMPALLOMENI MAURIZIO	Dir. Medici
DSP/Direz. UO Area Disc. Profilassi Malattie Infettive	Direz. U.O. Complessa	ZATELLI MARELLA	Dir. Medici
DSP/Direz. U.O. Attività Motoria e Medicina Sportiva	Direz. U.O. Complessa	ANEDDA ALBERTO	Dir. Medici
DSP/Direz. S.I.A.N. Aziendale	Direz. U.O. Complessa	ZILIOLI FRANCESCO	Dir. Medici
DSP/Direz. S.P.S.A.L. Aziendale	Direz. U.O. Complessa	MAGNANI FRANCESCO F.F.	Dir. Medici

DSP/Direz. Area Dip. Sanità Pubblica Veterinaria	Direz. Dipart. Territ.	COZZOLINO PAOLO	Dir. Veterinari
DSP/Direz. U.O. Serv. Veterinario "A"	Direz. U.O. Complessa	CAVALCA MAURO	Dir. Veterinari
DSP/Direz. U.O. Serv. Veterinario "B"	Direz. U.O. Complessa	PIERANTONI MARCO	Dir. Veterinari
DSP/Direz. U.O. Serv. Veterinario "C"	Direz. U.O. Complessa	ZARENGHI LUCA	Dir. Veterinari
Direz. DAI-Salute Mentale e Dipendenze Patologiche	Direz. Dipart. Az.le	PELLEGRINI PIETRO	Dir. Medici
DAI-SMDP/Direz. U.O. Servizi Psichiatrici Ospedalieri	Direz. U.O. Complessa	MARCHESI CARLO	Dir. Medici
DAI-SMDP/Direz. U.O. Psichiatria Adulti e Progr. Psicopatologici	Direz. U.O. Complessa	PAULILLO GIUSEPPINA F.F.	Dir. Medici
DAI-SMDP/Direz. U.O. Alcologia, Tabagismo, Att. Medico-Legali DP	Direz. U.O. Complessa	RUSTICHELLI PAOLO	Dir. Medici
DAI-SMDP/Direz. U.O. Salute Mentale Adulti Parma	Direz. U.O. Complessa	PELLEGRINI PIETRO	Dir. Medici
DAI-SMDP/Direz. U.O. Dipendenze Patologiche Parma	Direz. U.O. Complessa	ANTONIONI MARIA	Dir. Medici
DAI-SMDP/Direz. U.O. S.M.A./D.P. Fidenza	Direz. U.O. Complessa	MIGLIOLI MARISTELLA	Dir. Medici
DAI-SMDP/Direz. U.O. S.M.A./D.P. Borgotaro	Direz. U.O. Complessa	DE DONNO LORENZO	Dir. Medici
DAI-SMDP/Direz. U.O. S.M.A./D.P. Sud-Est	Direz. U.O. Complessa	GIANNATTASIO VALERIO F.F.	Dir. Medici
DAI-SMDP/Direz. Servizio N.P.I.A. Aziendale	Direz. U.O. Complessa	*PELLEGRINI PIETRO F.F.*	Dir. Medici
DAF/Direz. Dip. Assistenza Farmaceutica	Direz. Dipart. Az.le	GAZZOLA ANNA MARIA	Dir. Sanitari
DAF/Dir. Serv. Assistenza Farmaceutica Territoriale	Direz. U.O. Complessa	NEGRI GIOVANNA	Dir. Sanitari
DAF/Dir. Serv. Assistenza Farmaceutica Ospedaliera	Direz. U.O. Complessa	GAZZOLA ANNA MARIA	Dir. Sanitari
Direz. Medica P.O. Aziendale	Direz. Medica di P.O.	MARCHESI LEONARDO	Dir. Medici
Direz. Dip. Amministrativo P.O. Aziendale	Direz. Dipart. Az.le	CANTINI MARIO	Dir. P.T.A.
Dir. Amministrativa Osp. Fidenza	Direz. U.O. Complessa	CANTINI MARIO	Dir. P.T.A.
Dir. Medica Ospedale Fidenza	Direz. U.O. Complessa	ALIANI MARIA CRISTINA	Dir. Medici
OSF/Direz. Dip. Medicina Interna, Spec. e Riabil.	Direz. Dipart. Osped.	MONTANARI ENRICO	Dir. Medici
OSF/Dir. U.O. Medicina Interna	Direz. U.O. Complessa	PEDRETTI GIOVANNI	Dir. Medici
OSF/Dir. U.O. Neurologia	Direz. U.O. Complessa	MONTANARI ENRICO	Dir. Medici
OSF/Dir. U.O. Cure Palliative	Direz. U.O. Complessa	GHISONI FRANCESCO	Dir. Medici
OSF/Direz. Dipartimento Chirurgia Gen. e Spec.	Direz. Dipart. Osped.	CROVINI GIUSEPPE F.F.	Dir. Medici

OSF/Dir. U.O. Chirurgia Generale	Direz. U.O. Complessa	VIOLI VINCENZO	Dir. Medici
OSF/Dir. U.O. Urologia	Direz. U.O. Complessa	PRATI ANDREA	Dir. Medici
OSF/Dir. U.O. Ginecologia e Ostetricia Fidenza	Direz. U.O. Complessa	CROVINI GIUSEPPE	Dir. Medici
OSF/Dir. U.O. Ortopedia e Traumatologia Fidenza	Direz. U.O. Complessa	VAIENTI ENRICO	Dir. Medici
OSF/Dir. U.O. Endoscopia Digestiva	Direz. U.O. Complessa	ORSI PAOLO	Dir. Medici
OSF/Direz. Dip. Emergenza-Urgenza e Diagnostica	Direz. Dipart. Osped.	MORUZZI PAOLO	Dir. Medici
OSF/Dir. U.O. Anestesia, Rianim. e Camera Iperbarica	Direz. U.O. Complessa	CANTADORI LUCA	Dir. Medici
OSF/Dir. U.O. Pronto Soccorso e Medicina d'Urgenza	Direz. U.O. Complessa	RASTELLI GIANNI	Dir. Medici
OSF/Dir. U.O. Cardiologia e UTIC	Direz. U.O. Complessa	MORUZZI PAOLO	Dir. Medici
OSF/Dir. U.O. Radiologia e Diagnostica per immagini	Direz. U.O. Complessa	PEDRAZZINI MASSIMO	Dir. Medici
OSF/Dir. U.O. Emergenza Territoriale	Direz. U.O. Complessa	CANTADORI LUCA F.F.	Dir. Medici
Dir. Medica Ospedale Borgotaro	Direz. U.O. Complessa	MARCHESI LEONARDO	Dir. Medici
OSB/Direz. Dip. Medicina e Diagnostica	Direz. Dipart. Osped.	FORTUNATI CARLO F.F.	Dir. Medici
OSB/Dir. U.O. Medicina Interna	Direz. U.O. Complessa	BELLEI MARISA F.F.	Dir. Medici
OSB/Dir. U.O. Radiologia	Direz. U.O. Complessa	FORTUNATI CARLO	Dir. Medici
OSB/Direz. Dip. Chirurgico Osp. Borgotaro	Direz. Dipart. Osped.	GUARDOLI ALDO	Dir. Medici
OSB/Dir. U.O. Chirurgia Generale	Direz. U.O. Complessa	VIOLI VINCENZO F.F.	Dir. Medici
OSB/Dir. U.O. Ortopedia e Traumatologia	Direz. U.O. Complessa	GUARDOLI ALDO	Dir. Medici
OSB/Dir. U.O. Ginecologia e Ostetricia	Direz. U.O. Complessa	PISTOLESI ANTONIO	Dir. Medici
OSB/Dir. U.O. Anestesia e Rianimazione	Direz. U.O. Complessa	SOLARI GIACOMO	Dir. Medici
Direz. Distretto di Parma	Direz. di Distretto	CIOTTI GIUSEPPINA	Dir. Medici
Dir. U.O. Direzione Amministrativa Distr. Parma	Direz. U.O. Complessa	GRASSI ROSSELLA	Dir. P.T.A.
Dir. Dip. Cure Primarie Distretto di Parma	Direz. Dipart. Territ.	CELENDO MARIA TERESA	Dir. Medici
DCP Parma/Dir. U.O. Salute negli Istituti Penitenziari	Direz. U.O. Complessa	CIUSA FRANCESCO F.F.	Dir. Medici
Direz. Distretto di Fidenza	Direz. di Distretto	SALATI MARIA ROSA	Dir. Medici
Resp. Gestionale Casa della Salute San Secondo Parmense	Direz. U.O. Complessa	BOCCHI BRUNO	Dir. Medici

Dir. Dip. Cure Primarie Distr. Fidenza	Direz. Dipart. Territ.	GELMINI GIOVANNI F.F.	Dir. Medici
Direz. Distretto Valli Taro e Ceno	Direz. di Distretto	FRATTINI GIUSEPPINA	Dir. Medici
Dir. U.O. Direzione Amministrativa Distr. Borgotaro	Direz. U.O. Complessa	MORI STEFANO	Dir. P.T.A.
Dir. Dip. Cure Primarie Distretto Valli Taro e Ceno	Direz. Dipart. Territ.	GELMINI GIOVANNI	Dir. Medici
Direz. Distretto Sud-Est	Direz. di Distretto	LUCERTINI STEFANO	Dir. Medici
Dir. Dip. Cure Primarie Distretto Sud-Est	Direz. Dipart. Territ.	LUCERTINI STEFANO F.F.	Dir. Medici

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : T0102

Oggetto : Elenco Responsabili Esterni

Data Ultima Modifica :31/03/2015

DESCRIZIONE1	RIFERIMENTO	INDIRIZZO	LOCALITA	CAP
rmacia Colajacomo	Colajacomo Dott. Adele	P.le Pablo 5/d	Parma	43100
Farmacia comunale Campioni	Molinari Dr. Mauro	V. Campioni	Parma	43100
Farmacia comunale Campioni	Molinari Dr. Mauro	V. Campioni	Parma	43100
Farmacia comunale Fleming	Molinari Dr. Mauro	V. Fleming	Parma	43100
Farmacia comunale Mille	Molinari Dr. Mauro	V.le dei Mille, 52b	Parma	43100
Farmacia S. Ilario	Ruggiero Dr.ssa Tina	p.le Lubiana 31/a	Parma	43100
Farmacia Colajacomo	Colajacomo Dott. Adele	P.le Pablo 5/d	Parma	43100
Farmacia Colajacomo	Colajacomo Dott. Adele	P.le Pablo 5/d	Parma	43100
Farmacia Colajacomo	Colajacomo Dott. Adele	P.le Pablo 5/d	Parma	43100
Farmacia Comunale Collecchio	Raffi Dr.ssa Silvana	v. Togliatti, 6/a	Collecchio	43044
Farmacia Costa	Costa Dott. M. Grazia	Via Callani 20	Parma	43100
Farmacia Costa	Costa Dott. M. Grazia	Via Callani 20	Parma	43100
Farmacia Colajacomo	Colajacomo Dott. Adele	P.le Pablo 5/d	Parma	43100
Farmacia Sorbolo		Via Italo Focherini 11	sorbolo	
Farmacia Costa	Costa Dott. M. Grazia	Via Callani 20	Parma	43100
Farmacia Silvia	Mossini dr.ssa Paola	v. Cavour, 23	Colorno	43052
Farmacia Silvia	Mossini dr.ssa Paola	v. Cavour, 23	Colorno	43052
Farmacia Siviero	Siviero Dott. Giampiero	V. Matteotti 16	Colorno	43052
Farmacia Siviero	Siviero Dott. Giampiero	V. Matteotti 16	Colorno	43052
Farmacia Zanetti	Zanetti Dott. Filippo	Str. Vecchia di Bag. 51	Parma	43100
Farmacia S. Martino	Busani Dot.. Franco	V.Trento, 59a	Parma	43100
Farmacia Zanetti	Zanetti Dott. Filippo	Str. Vecchia di Bag. 51	Parma	43100
Farmacia Stadio Tardini	Mezzadri Dr.Ursula e Sonia	P.le Risorgimento 11c	Parma	43100
Farmacia Stadio Tardini	Mezzadri Dr.Ursula e Sonia	P.le Risorgimento 11c	Parma	43100
Farmacia Stadio Tardini	Mezzadri Dr.Ursula e Sonia	P.le Risorgimento 11c	Parma	43100
Farmacia Mantovani	Mazzocchi Dott. Alessandro	V. Garibaldi 281b	Parma	43100
Farmacia S. Lazzaro	Lusuardi Senatore Dr. Pietro	v. XXIV Maggio 10/a	Parma	43100
Farmacia Prati Bocchi	Turco dr. Paolo Cesare	v. Gramsci, 15/b	Parma	43100
Farmacia Mantovani	Mazzocchi Dott. Alessandro	V. Garibaldi 281b	Parma	43100
Farmacia Mentana	Bonfanti Dott. Clara	V.le Mentana 1/e	Parma	43100
Farmacia Mentana	Bonfanti Dott. Clara	V.le Mentana 1/e	Parma	43100
Farmacia Mentana	Bonfanti Dott. Clara	V.le Mentana 1/e	Parma	43100
Farmacia Mentana	Bonfanti Dott. Clara	V.le Mentana 1/e	Parma	43100
Farmacia Zanetti	Zanetti Dott. Filippo	Str. Vecchia di Bag. 51	Parma	43100
Farmacia Parenti	Parenti Dr.ssa Micaela	V. D. Alighieri 2/a	Chiozzola	43050
Farmacia Mantovani	Mazzocchi Dott. Alessandro	V. Garibaldi 281b	Parma	43100
Farmacia Prati Bocchi	Turco dr. Paolo Cesare	v. Gramsci, 15/b	Parma	43100
Farmacia Prati Bocchi	Turco dr. Paolo Cesare	v. Gramsci, 15/b	Parma	43100
Farmacia Prati Bocchi	Turco dr. Paolo Cesare	v. Gramsci, 15/b	Parma	43100
Farmacia Romano	Rocco Gavazzoli	v. Solferino 34/c	Parma	43100
Farmacia Tomatis	Tomatis Dott. Roberto	V. Toscana 94/a	Parma	43100
INPAL	dott. Begani	v. Inzani, 23	Parma	43100
Farmacia Parenti	Parenti Dr.ssa Micaela	V. D. Alighieri 2/a	Chiozzola	43050
Farmacia Landini	Landini Dott. Giovanni	V.le V. Emanuele 39	Sala Baganza	43038
Farmacia Costa	Costa Dott. M. Grazia	Via Callani 20	Parma	43100
Farmacia Costa	Costa Dott. M. Grazia	Via Callani 20	Parma	43100
Farmacia Costa	Costa Dott. M. Grazia	Via Callani 20	Parma	43100
Farmacia Costa	Costa Dott. M. Grazia	Via Callani 20	Parma	43100
Farmacia Crocetta	Balderi Dott. Marco	V. Emilia Ovest	Parma	43100
Farmacia Mentana	Bonfanti Dott. Clara	V.le Mentana 1/e	Parma	43100

Farmacia Landini	Landini Dott. Giovanni	V.le V. Emanuele 39	Sala Baganza	43038
Farmacia Costa	Costa Dott. M. Grazia	Via Callani 20	Parma	43100
Farmacia Landini	Landini Dott. Giovanni	V.le V. Emanuele 39	Sala Baganza	43038
Farmacia Leporati	Eredi Dott. Leporati	V. Silvio Pellico 5/e	Parma	43100
Farmacia Leporati	Eredi Dott. Leporati	V. Silvio Pellico 5/e	Parma	43100
Farmacia Leporati	Eredi Dott. Leporati	V. Silvio Pellico 5/e	Parma	43100
Farmacia Leporati	Eredi Dott. Leporati	V. Silvio Pellico 5/e	Parma	43100
Farmacia S. Ilario	Ruggiero Dr.ssa Tina	p.le Lubiana 31/a	Parma	43100
Farmacia Crocetta	Tegoni Dott. Paolo	V. Emilia Ovest	Parma	43100
Farmacia Bixio	Pattini Dott. Pier Luigi	str. Bixio, 5	Parma	43100
Farmacia Cassitto	Cassitto Dr. Antonio	v. F. Parri 41/g	Parma	43100
Farmacia Baganza	Barbieri dott. Marco	V. Baganza 11/a	Parma	43100
Farmacia Baganza	Barbieri dott. Marco	V. Baganza 11/a	Parma	43100
Farmacia Baganza	Barbieri dott. Marco	V. Baganza 11/a	Parma	43100
Farmacia Baganza	Barbieri dott. Marco	V. Baganza 11/a	Parma	43100
Farmacia Baganza	Barbieri dott. Marco	V. Baganza 11/a	Parma	43100
Farmacia Baganza	Barbieri dott. Marco	V. Baganza 11/a	Parma	43100
Farmacia SS. Annunziata	Barbieri Laura	via Gramsci 1/e	Parma	43100
Farmacia Bixio	Pattini Dott. Pier Luigi	str. Bixio, 5	Parma	43100
Farmacia Bixio	Pattini Dott. Pier Luigi	str. Bixio, 5	Parma	43100
Farmacia Cassitto	Cassitto Dr. Antonio	v. F. Parri 41/g	Parma	43100
Farmacia Cassitto	Cassitto Dr. Antonio	v. F. Parri 41/g	Parma	43100
Farmacia Cassitto	Cassitto Dr. Antonio	v. F. Parri 41/g	Parma	43100
Farmacia S. Francesco	Del Porto Dr.ssa Giuseppina	V. Spezia 3/a	Parma	43100
Farmacia Baganza	Barbieri dott. Marco	V. Baganza 11/a	Parma	43100
CGIL Parma	Devincenzi, Pollari	V. Confalonieri, 151	Parma	43100
Farmacia Cassitto	Cassitto Dr. Antonio	v. F. Parri 41/g	Parma	43100
AVIS Vigatto (Corcagnano)	Colla Paolo-Benassi Adriano	v. donatori sangue 4	Corcagnano	43030
AVIS Vigatto (Corcagnano)	Colla Paolo-Benassi Adriano	v. donatori sangue 4	Corcagnano	43030
AVIS Vigatto (Corcagnano)	Colla Paolo-Benassi Adriano	v. donatori sangue 4	Corcagnano	43030
AVIS Vigatto (Corcagnano)	Colla Paolo-Benassi Adriano	v. donatori sangue 4	Corcagnano	43030
Farmacia Baganza	Barbieri dott. Marco	V. Baganza 11/a	Parma	43100
AVIS Vigatto (Corcagnano)	Colla Paolo-Benassi Adriano	v. donatori sangue 4	Corcagnano	43030
Farmacia Cavallina	Pezzani Dr. Giulio	v. Emilio Lepido, 4/b	Parma	43100
CGIL Parma	Devincenzi, Pollari	V. Confalonieri, 151	Parma	43100
Farmacia Allegri	Maggiorelli dott.M.Cristina	V. Repubblica, 70/b	Parma	43100
Farmacia Allegri	Maggiorelli dott.M.Cristina	V. Repubblica, 70/b	Parma	43100
Farmacia Allegri	Maggiorelli dott.M.Cristina	V. Repubblica, 70/b	Parma	43100
Farmacia Amadasi	Corbelli Dr.ssa Nella	v. S. Pertini, 10	Parma	43100
Farmacia SS. Annunziata	Barbieri Laura	via Gramsci 1/e	Parma	43100
AVIS Vigatto (Corcagnano)	Colla Paolo-Benassi Adriano	v. donatori sangue 4	Corcagnano	43030
Farmacia XXII Luglio s.n.	Lucchetti Dott. Natalia	V. XXII Luglio 13	Parma	43100
Farmacia Cassitto	Cassitto Dr. Antonio	v. F. Parri 41/g	Parma	43100
Farmacia Coop. Gibertini	Manfredi Dott. Umberto	V. Repubblica 10/a	Parma	43100
Farmacia Coop. Gibertini	Manfredi Dott. Umberto	V. Repubblica 10/a	Parma	43100
Farmacia Coop. Gibertini	Manfredi Dott. Umberto	V. Repubblica 10/a	Parma	43100
Farmacia Guareschi	Farnetti Dr. Alberto	V. Farini 5/c	Parma	43100
Farmacia Coop. Gibertini	Manfredi Dott. Umberto	V. Repubblica 10/a	Parma	43100
Farmacia Guareschi	Farnetti Dr. Alberto	V. Farini 5/c	Parma	43100
Farmacia Zarotto	Chierici Dott. Nadia	V. Zarotto 30/e	Parma	43100
Farmacia XXII Luglio s.n.	Lucchetti Dott. Natalia	V. XXII Luglio 13	Parma	43100

Farmacia Montebello	Coperchini Dott. Bianca	V. Montebello 84/d	Parma	43100
Farmacia Montebello	Coperchini Dott. Bianca	V. Montebello 84/d	Parma	43100
Farmacia Nazionale	Chiesi Dott. Anita	P.le V. Emanuele 19	Parma	43100
Farmacia Nazionale	Chiesi Dott. Anita	P.le V. Emanuele 19	Parma	43100
Farmacia Pezzana	Gerevini Dr. Alberto	v. Bixio, 72	Parma	43100
Farmacia Guareschi	Farnetti Dr. Alberto	V. Farini 5/c	Parma	43100
Farmacia Ponte Dattaro	Bruschi Dr. Enrico	Str. Montanara, 23/b	Parma	43100
Farmacia Corradini	Corbellini Dott. Paola	V. Repubblica 20	Parma	43100
Farmacia Cordero	Merli Dott. Alessandro	str. Asolana 31	S.Polo di Torrile	43056
Farmacia Ponte Dattaro	Bruschi Dr. Enrico	Str. Montanara, 23/b	Parma	43100
Farmacia Ponte Dattaro	Bruschi Dr. Enrico	Str. Montanara, 23/b	Parma	43100
Farmacia Ponte Dattaro	Bruschi Dr. Enrico	Str. Montanara, 23/b	Parma	43100
Farmacia Coop. Gibertini	Manfredi Dott. Umberto	V. Repubblica 10/a	Parma	43100
Farmacia Ponte Dattaro	Bruschi Dr. Enrico	Str. Montanara, 23/b	Parma	43100
Farmacia Ponte Dattaro	Bruschi Dr. Enrico	Str. Montanara, 23/b	Parma	43100
Farmacia Ponte Dattaro	Bruschi Dr. Enrico	Str. Montanara, 23/b	Parma	43100
Farmacia Donetti Collecchio	Giovanelli Dr.ssa Maria Cristina	p. Avanzini, 1	Collecchio	43044
Farmacia Donetti Collecchio	Giovanelli Dr.ssa Maria Cristina	p. Avanzini, 1	Collecchio	43044
Farmacia Donetti Collecchio	Giovanelli Dr.ssa Maria Cristina	p. Avanzini, 1	Collecchio	43044
Farmacia Fornari	Fornari Dr.ssa Beatrice	V. Farini 42/a	Parma	43100
Farmacia Ponte Dattaro	Bruschi Dr. Enrico	Str. Montanara, 23/b	Parma	43100
Farmacia Zacconi	Bustaffa Dr. Stefano	v. Cavour, 21	Fidenza	43036
Farmacia Parolari	Parizzi Dr.ssa Donatella	v. Berenini, 82	Fidenza	43036
Farmacia Parolari	Parizzi Dr.ssa Donatella	v. Berenini, 82	Fidenza	43036
Farmacia Pelizza s.n c.	Arfini Dott. Lindo	P.za Garibaldi 26	Soragna	43019
Farmacia Riccardi	Riccardi Dr. Andrea	V. Emilia 14/c	Ponte Taro	43010
Farmacia Romanini	Romanini Dott. Carlo	V. Gramsci, 14	Noceto	43015
Farmacia Romanini	Romanini Dott. Carlo	V. Gramsci, 14	Noceto	43015
Farmacia Spotti	Spotti Dott. Patrizia	V. Statale 122	Castione Marchesi	43030
Farmacia S. Vitale	Franzan Dott. Giuseppe	V. Vaccari 17	Fontanellato	43013
Farmacia Zacconi	Bustaffa Dr. Stefano	v. Cavour, 21	Fidenza	43036
Farmacia S. Vitale	Franzan Dott. Giuseppe	V. Vaccari 17	Fontanellato	43013
Farmacia Malchiodi	Malchiodi dr. Paolo	P.za Garibaldi, 42	Fidenza	43037
Farmacia San Donnino	Contini Dott.ssa Paola	l.go Leopardi, 2	Fidenza	43036
Farmacia S. Vitale	Franzan Dott. Giuseppe	V. Vaccari 17	Fontanellato	43013
Comune Zibello	Michelazzi	V. Matteotti, 10	Zibello	43010
Farmacia Malchiodi	Malchiodi dr. Paolo	P.za Garibaldi, 42	Fidenza	43037
Comune Salsomaggiore	Gorra Lorena	p.zza Libertà, 1	Salsomaggiore Terme	43039
Comune Salsomaggiore	Gorra Lorena	p.zza Libertà, 1	Salsomaggiore Terme	43039
Farmacia S. Vitale	Franzan Dott. Giuseppe	V. Vaccari 17	Fontanellato	43013
Comune Salsomaggiore	Gorra Lorena	p.zza Libertà, 1	Salsomaggiore Terme	43039
Farmacia Centrale	Lunardini Dott. Maria	P.zza Repubblica 23	Noceto	43014
Comune Polesine	Contini Maria Rosa	v.le delle Rimembranze, 12	Polesine	43010
Farmacia Comunale Iezzi	Iezzi Dr.ssa Miriam	v. Roma, 34	Fontevivo	43010
Farmacia Cuoghi	Cuoghi Dott. Iginio	via Tabiano, 63	Tabiano terme	43030
Farmacia Mainardi	Mainardi dott.ssa Katia	via Ghiara Sabbioni 15	Fontanellato	43012
Farmacia Cuoghi	Cuoghi Dott. Iginio	via Tabiano, 63	Tabiano terme	43030
Farmacia Gemignani	Gemignani Dr.ssa Elisabetta	v. Berenini, 26	Fidenza	43036
Farmacia Concari	Concari dott. Luiigino	v. Provinciale 39	Fontanelle	43010
Comune Salsomaggiore	Gorra Lorena	p.zza Libertà, 1	Salsomaggiore Terme	43039
Farmacia Scimonelli	Simoncelli Dr. Piergiuseppe	V. Roma 18	Varsi	43049

Farmacia lorio	lorio Dott.ssa Maria	V. Fondovalle 16	Solignano	43040
Farmacia Leonardi	Leonardi Dott. Filippo	V. Martiri Libertà, 31	Varano de Melegari	43040
Farmacia Piazza	Piazza Dott. Fabrizio	V. Repubblica 17	Felegara	43040
Farmacia Piazza	Piazza Dott. Fabrizio	V. Repubblica 17	Felegara	43040
Farmacia Piazza	Piazza Dott. Fabrizio	V. Repubblica 17	Felegara	43040
Farmacia Raggi	Raggi Dott. Anna	P.za Micheli 28	Bedonia	43042
Farmacia S. Angela	Schianchi Dott. Eugenio	V. Principale	Albareto	43051
Farmacia del taro	Munafò dr. Vincenzo	v. Nazionale, 82	Fornovo Taro	43044
Farmacia Rosso	Scamoni Dott. Isabella	V. Roma 26	Bore	43030
Farmacia S.Alfonso	Lombardo Dr. Fabrizio	V. Roma 12	Bardi	43032
Farmacia S. Giovanni	Dott.sse Rita e Donatella Surace	v. P. Cella 25	Bardi	43032
Farmacia S. Giovanni	Virgilio Dott. Giuseppe	V. Colla 25	Bardi	43033
Farmacia S. Rocco	Feccia Dott. Tiziana	V. Stazione 14	Valmozzola	43050
Comune Pellegrino	Pirroni Sonia	V. Micheli, 1	Pellegrino P.se	43047
Farmacia Denegri	Denegri Dott. Antonella	V. Puccini 2	S. Andrea Bagni	43048
Farmacia Compiano	Mancini Dott. Annamaria	V.Ponte 5	Compiano	43053
Farmacia S. Giorgio	Chiesi Carlos	via Nazionale 79/c	Collecchio	43044
Farmacia Pettenati	Frattini Dott. Amina	V.Roma 68	Medesano	43056
Comune Terenzo	Calza Silvana	loc. Terenzo	Terenzo	43040
Comune Berceto (Casa Protetta)	Guelfi, Pezzani	V. G. Marconi, 18	Berceto	43042
Farmacia Bocchialini	Bocchialini Dott. Gianfranco	V. Garibaldi 4	Bedonia	43041
Farmacia Cardinali	Cardinali Dott.ssa Gabriella	v.le Libertà, 18	Borgo val di taro	43043
Farmacia Chiappari	Chiappari Dott. Maria Rosa	Provinciale Sud 21	Tarsogno	43051
Farmacia Corbelletta	Corbelletta Dott.ssa Daniela	v. C. Battisti, 19	Borgo val di taro	43043
Farmacia Corbelletta	Corbelletta Dott.ssa Daniela	v. C. Battisti, 19	Borgo val di taro	43043
Farmacia Costella	Dott. Costella Corrado e Luca	p.zza Manara, 12	Borgo Val di Taro	43043
Farmacia Costella	Dott. Costella Corrado e Luca	p.zza Manara, 12	Borgo Val di Taro	43043
Farmacia S. Giorgio	Chiesi Carlos	via Nazionale 79/c	Collecchio	43044
Farmacia S. Giorgio	Chiesi Carlos	via Nazionale 79/c	Collecchio	43044
Farmacia S. Giorgio	Chiesi Carlos	via Nazionale 79/c	Collecchio	43044
Farmacia Cardinali	Cardinali Dott.ssa Gabriella	v.le Libertà, 18	Borgo val di taro	43043
Farmacia S. Rita	Pasini Dott. Francesca	V. Parma 26	Basilicagoiano	43020
Farmacia Comunale Lagrimone	Bocchi Dr.ssa Simona	loc. Lagrimone	Lagrimone	43020
Farmacia Bracchi	Bracchi Dott. Gian Antonio	V. Carducci 1 lla	Felino	43035
Farmacia Ferri	Ferri Dr.ssa Emilia	v. Provinciale	Palanzano	43025
Farmacia Ferri	Ferri Dr.ssa Emilia	v. Provinciale	Palanzano	43025
Farmacia S. Michele	Pinotti Dr.ssa Maria	v. Alighieri, 6/b	S. Michele Tiorre	43030
Farmacia S. Michele	Pinotti Dr.ssa Maria	v. Alighieri, 6/b	S. Michele Tiorre	43030
Farmacia Comunale di Scurano	Fadani Dr.ssa Nicoletta	Scurano	Scurano	43020
Farmacia S. Michele	Pinotti Dr.ssa Maria	v. Alighieri, 6/b	S. Michele Tiorre	43030
Farmacia S. Rita	Pasini Dott. Francesca	V. Parma 26	Basilicagoiano	43020
Farmacia S. Rita	Pasini Dott. Francesca	V. Parma 26	Basilicagoiano	43020
Farmacia Dedali	Dedali Corrado	via Matteotti 28	Montechiarugolo	43022
Farmacia S. Rita	Pasini Dott. Francesca	V. Parma 26	Basilicagoiano	43020
Farmacia Comunale Pastorello	Urbani Dott. Marilena	Strada Monchio 9/b	Pastorello di Langhirano	43013
Farmacia Comunale Pastorello	Urbani Dott. Marilena	Strada Monchio 9/b	Pastorello di Langhirano	43013
Farmacia Comunale Pastorello	Urbani Dott. Marilena	Strada Monchio 9/b	Pastorello di Langhirano	43013
Farmacia Comunale Pastorello	Urbani Dott. Marilena	Strada Monchio 9/b	Pastorello di Langhirano	43013
Farmacia Monchio	Musmeci Clementina	Via F. Bocchialini 2	Monchio delle Corti	43010
Farmacia Maturo	Cimino Dr.ssa Giuseppina	V. Buca 72	Neviano degli Arduini	43024
Farmacia Ghiare di Corniglio	Bandini Dott. Claudia	Str. Provinciale 6/a	Ghiare di Corniglio	43020

Farmacia Dei Bono	Pontillo Dr.ssa Giuseppa	V. Mazzini 25	Langhirano	43014
Farmacia Chehade	Chehade Dott. Salah El Din	V.le Europa Unita 8	Tizzano	43028
Farmacia Agnelli	Agnelli Dott. Umberto	V. Argini, 28	Lesignano Bagni (PR)	43037
Comune Calestano	Benedetto Federica	v. Mazzini,18	Calestano	43030
Farmacia Lonetti	Lonetti Dott. Antonio	P.za Rustici 10	Corniglio	43021
Farmacia Rizzoli	Rizzoli Dott. Francesca	P.za Veneto 41	Traversetolo	43030
Comune Roccabianca	Barbarini Angela	v.le Rimembranze, 3	Roccabianca	43010
AVIS Sorbolo	Cantoni, Frigeri, Bellanova	V. Gruppini	Sorbolo	43058
Farmacia S. Maria delle Grazie	Maria Teresa vecchia	via M. libertà 100	Mezzani inf.	
Farmacia S. Antonio	Melegari Dott. Andrea	P.za Ferrari 4/a	Sissa	43018
Farmacia Amadei	Amadei Dott. Mario	V. Matteotti 361a	Sissa	43018
Comune Trecasali	Canu Giovanna	V. Nazionale, 50	Trecasali	43010
Comune Roccabianca	Barbarini Angela	v.le Rimembranze, 3	Roccabianca	43010
AVIS Sorbolo	Cantoni, Frigeri, Bellanova	V. Gruppini	Sorbolo	43058
AVIS Sorbolo	Cantoni, Frigeri, Bellanova	V. Gruppini	Sorbolo	43058
AVIS Sorbolo	Cantoni, Frigeri, Bellanova	V. Gruppini	Sorbolo	43058
AVIS Sorbolo	Cantoni, Frigeri, Bellanova	V. Gruppini	Sorbolo	43058
AVIS Sorbolo	Cantoni, Frigeri, Bellanova	V. Gruppini	Sorbolo	43058
Comune Roccabianca	Barbarini Angela	v.le Rimembranze, 3	Roccabianca	43010

E’ in corso la raccolta dei documenti di nomina a Responsabile esterno al trattamento dei dati per i fornitori dell’Azienda USL che per motivi di erogazione di servizi di manutenzione e sviluppo abbiamo accesso ai dati aziendali.

Al momento sono stati deliberate le seguenti nomine:
Ditta Engineering Ingegneria Informatica Spa
Sede legale Via S. Martino della Battaglia, 56 - 00185 Roma
“Contratto di manutenzione e assistenza dei moduli software “Invalidi civili” e Patenti Speciali” per il triennio 2013/2015”.
Responsabile al trattamento dei dati: Dario Buttita

Ditta GPI Spa
Sede legale Via Ragazzi del 99’, 13 – 38123 Trento
“Contratto di manutenzione e assistenza software del sistema informatico-amministrativo denominato “Eusis”, per il triennio 2013/2015”
Responsabile del trattamento dei dati: Fausto Manzana

Ditta HMS Sipac Spa
Sede legale Milano Fiori, Strada 1, Palazzo F/1 – 20090 Assago (MI)
“Contratto di manutenzione della piattaforma Zimbra OpenSource e Zextras Backup per il periodo dal 01/07/2013 al 31/12/2015”
Responsabile del trattamento dei dati: Marco Ricciardiello

Ditta HMS Sipac Spa
Sede legale Milano Fiori, Strada 1, Palazzo F/1 – 20090 Assago (MI)
“Contratto di manutenzione e assistenza del software VPN (Virtual Private Network) – IntranetDPS fino al 31/12/2016”
Responsabile del trattamento dei dati: Marco Ricciardiello

Ditta Info Line SRL
Sede Legale Via Colorno, 63 – 43122 Parma
“Contratto di manutenzione ordinaria, evolutiva e assistenza tecnica ai moduli software Job Time Plus per il quadriennio 2013/2016”
Responsabile del trattamento dei dati: Bettati Andrea

Ditta Info Line SRL
Sede Legale Via Colorno, 63 – 43122 Parma
“Contratto “Service elaborazioni denunce annuali dipendenti” – “Service paghe e denunce medici specialisti” – “Service paghe e denunce medicina penitenziaria” - “Service paghe e denunce Guardia Medica” - "Service paghe e denunce Medici dell’Emergenza Sanitaria Territoriale”per il quadriennio 2013/2016”
Responsabile del trattamento dei dati: Bettati Andrea

Ditta Noemalife Spa
Sede Legale Via Gobetti, 52 – 40129 Bologna
“Contratto di manutenzione e assistenza dei software applicativi per il triennio 2013/2015”
Responsabile del trattamento dei dati: Francesco Serra

Cooperativa EDP La Traccia

Sede legale Recinto II Fiorentini, 10 – 75100 Matera
“Contratto di manutenzione e assistenza del software Gepadial per il biennio 2014/2015”
Responsabile del trattamento dei dati: Vito Domenico Gravela

Ditta Sferacarta Net SAS (ora Sferacarta GPI Srl)
Sede legale Via Bazzanese, 69 – 40033 Casalecchio di Reno (BO)
“Contratto di manutenzione e assistenza software gestionale in dotazione al Servizio Veterinario per il periodo dal 01/01/2013 al 31/12/2015 ed acquisizione nuovi moduli”
Responsabile del trattamento dei dati: Gambarini Alberto

Ditta Meteda Srl
Sede legale Via Silvio Pellico, 4 - 63074 S. Benedetto del Tronto (AP)
“Contratto di manutenzione ed assistenza tecnica del software di cartella clinica diabetologica MyStar Connect, anno 2014”
Responsabile del trattamento dei dati: Fausta Brancaccio

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : T0103

Oggetto : Elenco Trattamenti

Data Ultima Modifica :29/03/2015

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

REGOLAMENTO PER IL TRATTAMENTO DEI DATI PERSONALI SENSIBILI E GIUDIZIARI
(*Art.20 - 21 D.Lgs 196/2003 Codice in materia di protezione di dati personali)*

Elenco dei trattamenti di competenza delle Aziende Sanitarie

2. Tutela dai rischi infortunistici e sanitari connessi con gli ambienti di vita e di lavoro
3. Sorveglianza epidemiologica delle malattie infettive e diffusive e delle tossinfezioni alimentari
4. Attività amministrative e certificatorie correlate alle vaccinazioni e alla verifica assolvimento obbligo vaccinale
5. Attività amministrative correlate ai programmi di diagnosi precoce
6. Attività fisica e sportiva
7. Attività di assistenza socio - sanitaria a favore di fasce deboli di popolazione e di soggetti in regime di detenzione
8. Medicina di base - pediatria di libera scelta - continuità assistenziale (guardia medica notturna e festiva, guardia turistica)
9. Assistenza sanitaria di base: riconoscimento del diritto all'esenzione per patologia/invalidità/reddito e gestione archivio esenti
10. Assistenza sanitaria di base: assistenza sanitaria in forma indiretta
11. Cure all'estero urgenti e programmate
12. Assistenza sanitaria di base: assistenza agli stranieri in Italia (particolari categorie)
13. Assistenza integrativa
14. Assistenza protesica
15. Assistenza domiciliare programmata e integrata
16. Attività amministrative correlate all'assistenza a soggetti non autosufficienti, a persone con disabilità fisica, psichica e sensoriale e a malati terminali nei regimi residenziale, semiresidenziale ambulatoriale e domiciliare
17. Assistenza termale
18. Attività amministrativa, programmatoria, gestionale e di valutazione relativa all'assistenza ospedaliera in regime di ricovero
19. Attività amministrativa, programmatoria, gestionale e di valutazione concernente l'attività immuno - trasfusionale
20. Attività amministrativa, programmatoria, gestionale e di valutazione concernente la donazione, il trapianto di organi, tessuti e cellule
21. Soccorso sanitario di emergenza/urgenza sistema "118". Assistenza sanitaria di emergenza
22. Attività amministrative correlate ad assistenza specialistica, ambulatoriale e riabilitazione
23. Promozione e tutela della salute mentale
24. Attività amministrative correlate alle dipendenze (tossicodipendenze e alcooldipendenze)
25. Assistenza socio-sanitaria per la tutela della salute materno - infantile ed esiti della gravidanza
26. Attività amministrative correlate all'assistenza farmaceutica territoriale e ospedaliera

27. Sperimentazione clinica
28. Farmacovigilanza e rilevazione reazioni avverse a vaccini e farmaci
29. Attività amministrative correlate all'erogazione a totale carico del servizio sanitario nazionale, qualora non vi sia alternativa terapeutica valida, di medicinali inseriti in apposito elenco predisposto dall'Agenzia Italiana del Farmaco
30. Attività amministrative correlate all'assistenza a favore delle categorie protette (morbo di Hansen)
31. Attività amministrativa programmatoria, gestionale e di valutazione concernente l'assistenza ai nefropatici cronici in trattamento dialitico
32. Attività medico - legale inerente l'istruttoria delle richieste di indennizzo per danni da vaccinazioni obbligatorie, trasfusioni e somministrazione di emoderivati
33. Attività medico - legale inerente gli accertamenti finalizzati al sostegno delle persone con disabilità (riconoscimento dello stato di invalidità, cecità e sordità civili, della condizione di handicap ai sensi della L. 104/92, accertamenti per il collocamento mirato al lavoro delle persone con disabilità ai sensi della L. 68/99)
34. Attività medico - legale inerente l'accertamento dell'idoneità in ambito di diritto al lavoro (assunzione nel pubblico impiego; idoneità allo svolgimento di attività lavorative; controllo dello stato di malattia dei dipendenti pubblici e privati; accertamenti sanitari di assenza di tossicodipendenza o di assunzione di sostanze stupefacenti o psicotrope in lavoratori addetti a mansioni che comportino particolari rischi per la sicurezza, l'incolumità e la salute di terzi)
35. Attività medico - legale inerente l'accertamento dell'idoneità al porto d'armi, ai fini della sicurezza sociale
36. Attività medico - legale inerente l'accertamento dell'idoneità alla guida, ai fini della sicurezza sociale
37. Consulenze e pareri medico legali in tema di riconoscimento della dipendenza delle infermità da causa di servizio
38. Consulenze e pareri medico legali in tema di ipotesi di responsabilità professionale sanitaria, di supporto all'attività di gestione del rischio clinico, informazione e consenso ai trattamenti sanitari e consulenze e pareri in materia di bioetica
39. Attività medico - legale in ambito necroscopico
40. Attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria
41. Attività amministrative correlate alla gestione e verifica sull'attività delegata a soggetti accreditati o convenzionati del SSN

Nome Documento : P0703

Oggetto : Regolamento per l'utilizzo degli strumenti informatici dell'Azienda USL di Parma

Data Ultima Modifica:23/04/2013

Introduzione

La gestione dei processi dell'Azienda USL di Parma è prevalentemente basata su strumenti informatici. Il punto d'accesso principale è la stazione di lavoro, generalmente composta da un Personal Computer (fisso, portatile, palmare, ecc.) e da eventuali periferiche (stampante, unità dischi esterne, ecc.).

L'utilizzo della stazione di lavoro avviene in ambito locale (es. creazione e salvataggio su disco di documenti, fogli di lavoro, ecc.) e/o in rete aziendale (es. Intranet, posta elettronica, procedure aziendali, ecc.). In entrambi i casi l'utilizzo è sottoposto alla normativa vigente in materia di trattamento dei dati e sicurezza degli stessi (D.lgs 196/2003 “Codice sulla Privacy”). Il presente regolamento ha come finalità quella di garantire un corretto utilizzo del sistema informatico per gli scopi istituzionali assicurando, nel contempo, il rispetto della normativa citata.

Ambito di applicazione e requisiti

L'Azienda USL, attraverso il Servizio Risorse Informatiche e Telematiche (S.RIT), recepisce i seguenti criteri in merito alla gestione e fruizione dei propri dati da parte degli utenti:

2. Confidenzialità - I dati non devono essere accessibili ai non aventi diritto
3. Integrità - Non deve essere possibile alterare i dati
4. Disponibilità - I dati devono essere sempre disponibili agli aventi diritto

Al fine di gestire un sistema “sicuro”, è necessario che gli utenti abbiano ricevuto formazione adeguata e che siano informati sui rischi di una cattiva gestione dei sistemi. Si assume perciò che l'atteggiamento sia ispirato alla correttezza ed alla buona fede, restando valida in ogni caso l'assunzione di responsabilità personale per le attività svolte.

L'adozione del presente regolamento è finalizzata a:

a) fornire la massima disponibilità ed efficienza del servizio nell'interesse della produttività aziendale;

b) garantire la massima sicurezza possibile nell’accesso alla rete privata (Intranet) e pubblica (Internet);

c) garantire il rispetto delle leggi in materia di “Tutela della Privacy” attraverso un utilizzo lecito delle risorse informatiche per l’elaborazione di dati personali e sensibili;

d) provvedere ad un'efficiente attività di monitoraggio e controllo a fini diagnostici ed evolutivi .

E' vietato l'uso delle risorse informatiche aziendali per tutte le attività illegali e quelle:

1. commerciali o a fini di lucro;
2. personali che sottraggano risorse al sistema aziendale;
3. che possono rappresentare una violazione della legge in materia di

Copyright e Licenza d'uso, fra le quali la copia non autorizzata di software brevettato e/o protetto;

4. che compromettono in qualsiasi modo la sicurezza delle risorse;
5. non conformi alla normativa sulla privacy.

Il presente regolamento è applicabile a tutti coloro che accedono alle risorse informatiche aziendali. L'accesso a tali risorse è riservato ai dipendenti dell'Azienda USL di Parma e a coloro che, a seguito di atti aziendali, hanno acquisito il diritto di accesso. Si assume che:

a) l'Azienda USL di Parma adotta il principio secondo il quale ogni strumento informatico deve essere utilizzato dall'utente per i soli scopi istituzionali per cui è stato implementato, perciò le attività di monitoraggio e controllo di detti strumenti non intendono violare la privacy dell'utente interessato;

b) ogni azione non conforme al presente regolamento verrà considerata una violazione della sicurezza e, come tale, comporterà la revoca dell'accesso alle risorse informatiche e la segnalazione al Responsabile; i casi più gravi (che violino anche la legislazione vigente) verranno segnalati all'Autorità competente e potranno essere soggetti ad azioni disciplinari o legali;

c) considerata la dinamicità tecnologica e legislativa dell'argomento trattato, occorre considerare il presente regolamento come elemento dinamico, quindi soggetto ad aggiornamenti periodici; perciò l'utente è tenuto a prendere visione e accettare anche gli eventuali aggiornamenti che verranno pubblicati sulla pagina Intranet aziendale (http://intra.ausl.pr.it); il presente documento va considerato come parte integrante della normativa vigente in materia di sicurezza informatica, che ogni utente è tenuto a conoscere e rispettare.

Regole di comportamento e utilizzo delle risorse

Stazione di lavoro (Personal Computer, periferiche, software, attrezzature elettromedicali…)

a) L'utente risponde del buon uso della stazione di lavoro che gli è stata affidata, comprese le eventuali periferiche associate e il software preinstallato. In particolare è responsabile dell'installazione del SW, specie se sprovvisto di regolare licenza. Qualsiasi software fornito dall'utente (anche se prelevato da siti Internet o in allegato a riviste e libri o in dotazione a periferiche specifiche) deve essere installato e utilizzato dietro approvazione del S.RIT. E' proibito l'uso di software Peer to Peer, Instant Messaging e Chat.

b) L'utente è tenuto a utilizzare in modo ottimale la dotazione software standard, per utilizzare la quale può richiedere eventualmente l'inserimento in piani di attività formativa aziendale pianificata.

c) L'utente è obbligato a disconnettere la sessione corrente quando la stazione di lavoro rimane non presidiata, per salvaguardarla da accessi indesiderati.

d) L'utente è tenuto a presidiare adeguatamente le proprie stampe prodotte dalle stampanti in rete, in particolar modo se contengono dati sensibili.

e) L'utente deve sottoporre a scansione antivirus i files acquisiti nella stazione di lavoro attraverso le diverse tipologie di trasferimento (dischetto, porta USB, CD, ecc).

f) Se l'utente viene autorizzato come Amministratore Locale del Personal Computer (es: programmi che non funzionano in ambienti con diritti “User”) diventa automaticamente responsabile di ogni cosa che avviene da/su detta postazione essendo in grado di accedere con pieno controllo al sistema; ad esso viene assegnata la responsabilità di perdita/abuso di dati o “attacchi” informatici perpetrati tramite quel sistema.

g) Ogni utente che ne abbia necessità può richiedere di inserire in rete un sistema di sua proprietà, dietro richiesta scritta e avvallo da parte della Direzione del servizio di appartenenza e dietro parere tecnico del S.RIT, rimanendo comunque responsabile delle manutenzione HW/SW preventiva/correttiva e di ogni danno cagionato tramite il sistema stesso. Il S.RIT si riserva la possibilità di effettuare controlli su tale sistema.

h) E' vietato cablare o collegare apparecchiature (di qualsiasi natura e tipo) alle prese di rete senza l'autorizzazione del S.RIT, modificare le impostazioni predefinite e assegnate dal S.RIT, installare modem configurati per l'accesso remoto, intraprendere azioni allo scopo di degradare le risorse del sistema e impedire ad utenti autorizzati l'accesso alle risorse, effettuare copie di file di configurazione del sistema operativo.

i) E’ vietato diffondere software prelevato da infrastrutture aziendali al di fuori dei termini delle licenze, diffondere software che possa danneggiare le risorse informatiche, accedere a dati e/o applicativi per i quali non si è ricevuta esplicita autorizzazione o incarico.

j) Le postazioni collegate ad attrezzature elettromedicali NON possono e non devono, per motivi di integrità e sicurezza dei dati, essere utilizzate come archivio degli studi propdotti dalle attrezzature. Le attrezzature medicali devono, per quanto possibile compatibilmente con i requisiti tecnologici, essere messe in rete con la rete aziendale ed essere interfacciate con memorie di massa che consentano la corretta archiviazione dei dati, in sicurezza, sottoposti a backup e in modalità di continuità operativa.

k) I dati, i documenti, i filmati e le immagini, non possono essere archiviati su supporti mobili come chiavette USB o dischi esterni. Qualora ciò si renda necessario in regime di urgenza, è necessario che tali periferiche siano fornite dal Servizio RIT, utilizzate previa autorizzazione e riconsegnate al Servizio RIT per la conservazione delle attrezzature in sicurezza. In nessun caso possono essere lasciate incustodite o portate all’esterno della struttura

l) L’acquisto e l’installazione delle attrezzature elettromedicali deve sempre essere effettuato dopo essere stata concordato con il Servizio RIT e il SIC, in modo da poter predisporre i parametri di configurazione e l’attrezzatura hardware migliore rispetto alle specifiche esigenze, al fine di garantire integrità e sicurezza dei dati.

Rete, modalità di accesso (Posta elettronica, Internet, Intranet) e protezione dei dati

- L'accesso alle risorse avviene mediante un identificativo (account, ovvero user/utente e password, ovvero smart card) strettamente personale e non

cedibile ad altri; in ogni caso l'utente viene considerato responsabile di eventuali atti illeciti perpetrati con il proprio account.

•L'utente deve proteggere il proprio account mediante password nel rispetto della normativa vigente (lunghezza minima della password, modifica periodica, utilizzo di caratteri numerici e maisucoli/minuscoli).

•L'utente è responsabile della protezione e dei salvataggi periodici dei dati utilizzati e/o memorizzati nei sistemi nei quali ha accesso, ad eccezione di quelli memorizzati su sistemi centralizzati, al cui salvataggio periodico sovrintende il S.RIT.

•E' responsabilità dell'utente segnalare una prolungata assenza (per comando, maternità, ecc…ecc…) per poter bloccare l'account ed evitare possibili abusi.

•Il contenuto e la manutenzione della casella di posta elettronica è posta sotto la diretta responsabilità dell'utente, compresa la verifica di eventuali messaggi malevoli (phishing), allegati infetti (virus), propagazione di messaggi indesiderati (spam).

•Non è permesso l'invio di dati personali o sensibili tramite posta elettronica se non preventivamente autorizzati dalla direzione di competenza; è comunque vivamente sconsigliato l'uso della posta elettronica per l'invio di dati personali o identificativi di terzi verso utenti esterni, poiché il transito sulla rete Internet è in "chiaro" e quindi potenzialmente leggibile da qualsiasi utente collegato alla rete Internet.

•E' permesso l'accesso a siti che forniscono servizi gratuiti di Posta Elettronica esclusivamente in modalità Web (protocollo http).

•L'utente è personalmente responsabile della violazione degli accessi protetti e dei contenuti prelevati in rete Internet. Il S.RIT ha la facoltà di interrompere il collegamento degli utenti qualora il sito visitato sia ritenuto in contrasto con i principi del servizio pubblico o lesivo della dignità della persona.

•Non è permesso l'invio di dati personali o sensibili tramite la rete internet (Upload) se non preventivamente autorizzati dalla direzione di competenza.

•Non è permesso l'utilizzo della rete Internet per Instant Messaging, Chat, telefonate virtuali e Stazioni Radio/Video, se non preventivamente autorizzati e configurati dal S.RIT.

•Non è consentita l'installazione e l'utilizzo di programmi di file sharing (condivisione).

•Non è consentita la memorizzazione/consultazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica,opinione e appartenenza sindacale e/o politica.

•E' vietato utilizzare strumenti/procedure di rete di esclusiva pertinenza del S.RIT, come cracker o software di monitoraggio della rete, configuratori di servizi centralizzati (quali DNS-Domain Name Service, DHCP-Dynamic Host Configuration Protocol, NTP-Network Time Protocol, LDAP, mailing, Web Server, accesso remoto o dial-up); installare apparecchiature di rete (quali Switch, Hub, Access point ecc… ecc..) , effettuare operazioni di routing/bridging/tunneling, intercettare pacchetti sulla rete utilizzando "Sniffer"

o software analoghi.

- E' vietato divulgare i numeri telefonici e le password dei modem aziendali.

Cartelle condivise

Al fine di soddisfare l'esigenza di aree di lavoro condivise tra gli utenti aziendali, il Servizio RIT, mette a disposizione alcune aree condivise preposte allo scopo. L'acceso a tali aree può essere richiesto dall'incaricato per se stesso e per altre risorse e deve approvato dal Responsabile o dai Responsabili delle rispettive risorse; nella richiesta devono essere specificate le esigenze per le quali viene effettuata la richiesta e la tipologia di documenti che si intendono condividere. All'area condivisa è possibile accedere solo tramite utenza e pwd di LDAP.

L'area condivisa deve essere gestita tenendo in considerazione:

1. I principi di pertinenza e non eccedenza, correttezza e buona fede previsti dal Codice privacy
2. Sull'area condivisa non possono essere trattati dati, documenti, foto o video che contengano dati identificativi e/o sensibili di terze parti o attraverso i quali un soggetto possa essere identificato e associato ad una particolare patologia o evento clinico/sanitario, senza aver fornito l'informativa e acquisito il consenso al trattamento dei dati in base a quanto riportato nel Codice privacy
3. Le cartelle condivise non possono essere utilizzate come archivi o backup della documentazione. La documentazione deve essere mantenuta sulla cartella condivisa per un periodo limitato di tempo, tendenzialmente identificato con il periodo di lavorazione del documento. Il Responsabile della sicurezza si riserva di effettuare controlli a campione sulle cartelle condivise al fine di identificare materiale non idoneo ad essere gestito tramite questo strumento per la presenta di dati identificativi o sensibili, materiale illecito o materiale la cui data di ultima modifica sia antecedente i 6 mesi dalla data del controllo. Rilevata la presenza di materiale con queste caratteristiche il Responsabile della Sicurezza può autonomamente predisporne, senza preavviso, la rimozione.
4. Le cartelle non accedute da più di 6 mesi verranno rimosse

Controllo e monitoraggio

Il Sistema di monitoraggio (Amministrazione del sistema) opera nel rispetto delle politiche adottate dall'Azienda USL di Parma in materia di sicurezza, al fine di garantire la massima riservatezza/disponibilità/integrità nei trattamenti dei dati personali e sensibili.

L'Azienda USL di Parma si è dotata di uno strumento per il controllo degli accessi Internet. Tale strumento non garantisce l'inaccessibilità totale a siti non istituzionali o a rilevanza penale, di conseguenza la responsabilità della navigazione è totalmente a carico dell'utente. Il S.RIT e/o gli amministratori di sistema si riservano il diritto di revocare l'accesso alle risorse senza preavviso, qualora essi siano utilizzati impropriamente o in violazione delle leggi vigenti.

Gli Amministratori di Sistema devono essere in grado in qualsiasi momento, specialmente in caso di emergenza, di poter accedere ai locali e ai Sistemi

loro affidati;

Gli accessi vengono registrati nel tempo attraverso opportuni log di sistema e i controlli possono essere fatti al momento e/o a campione dal S.RIT, oppure in tempi successivi. Qualsiasi comportamento ritenuto non ammissibile alla luce dei regolamenti verrà segnalato alla Direzione Aziendale e/o alle Autorità Competenti.

Gli Amministratori di Sistema, dietro richiesta esplicita del Responsabile e del Titolare del trattamento dati, possono accedere ai Sistemi per scopi di monitoraggio e controllo del corretto utilizzo del sistema stesso da parte dell'utente.

Gli Amministratori di Sistema, dietro richiesta esplicita del Responsabile e/o del Titolare del trattamento dati, possono accedere ai dati sui Sistemi Informatici per garantire la continuità del servizio garantendo la riservatezza del singolo utente.

Gli Amministratori di Sistema possono provvedere senza preavviso (in caso di emergenza da attacco informatico o da "Virus"), all'aggiornamento Software di tutte le postazioni anche se questo prevede un immediato riavvio dell'elaboratore. Gli utenti sono invitati a segnalare al S.RIT l'elenco di quegli elaboratori che devono essere riavviati in modo presidiato per evitare disservizi.

Gli Amministratori di Sistema, dietro richiesta esplicita del Responsabile e/o del Titolare del trattamento dati, possono accedere al personal computer e al sistema di messaggistica per scopi di monitoraggio/controllo o continuità di servizio.

Gli Amministratori di Sistema e i Tecnici di Supporto, possono accedere al personal Computer (anche senza preavviso) per manutenzione preventiva e correttiva.

Standard aziendali e accesso al Servizio RIT

Lo standard aziendale prevede l'utilizzo di software aderente alle normative in merito al Codice Digitale della P.A. L'Azienda utilizza formati di documenti (testo, foglio elettronico, ecc.) aperti (open) e, quando non sia richiesta possibilità di modifica, viene privilegiato il PDF (Portable Document Format). Gli utenti sono tenuti a comunicare agli interlocutori istituzionali queste istanze e, nel caso si verifichino incompatibilità di formati, devono comunicare al S.RIT il problema incontrato in modo dettagliato, riproducibile e fornire i riferimenti dell'interlocutore.

Al fine di limitare la diffusione di utilizzo di software proprietari, pur garantendo e agevolando la realtà

L'accesso al S. RIT deve avvenire prevalentemente attraverso l'help desk, attivato via Intranet, tramite mail o attraverso una chiamata al call center rispondente al 3931 che garantisce la tracciabilità della chiamata. Esiste una lista di utenti V.I.P. (Direzione, Direttori di Distretto, di Presidio, di Dipartimento etc etc) secondo organigramma aziendale, che potrà essere reindirizzata direttamente alle risorse interne del S.RIT. L'Helpdesk fornisce risposte a quesiti

specifici o richieste di assistenza, riguardanti le infrastrutture informatiche, l'utilizzo degli applicativi e la fornitura di dati. Per ottimizzare e tracciare le richieste si adotta un flusso ad elevato grado di informatizzazione, che prevede come modalità di accesso la pagina Intranet, la mail, la chiamata al call center. Viene posta attenzione sul fatto che la richiesta telematica segue un percorso ottimizzato.L'attività di helpdesk, in particolare per quanto riguarda il supporto sugli applicativi, deve essere in grado di filtrare eventuali richieste non pertinenti, ovvero di natura funzionale/applicativa anzichè informatica, veicolandole verso le sedi opportune. L'attività di helpdesk deve consentire una rapida presa in carico delle richieste e una rapida individuazione di competenza.
.

4. Sanzioni

In caso di violazione delle regole sopra citate e a seconda della gravità delle medesime, fatte salve le ulteriori conseguenze di natura penale, civile e amministrativa (Esempio: Titolo III D.lgs 196/2003), possono essere comminate le seguenti sanzioni:

11) richiamo verbale;

12) richiamo scritto;

13) segnalazione alla Commissione Disciplinare Aziendale.

Nome Documento : P0704

Oggetto : Linee guida e “buone pratiche” per la manipolazione dei file

Data Ultima Modifica:31/03/2015

Sempre di più in Azienda viene richiesto di limitare l'utilizzo di copie cartacee di documenti o addirittura di eliminarle completamente. Per passare alla copia digitale dei documenti è necessario avere una conoscenza di base dei formati più comuni, avere una idea di massima di quanto alcuni tipi di file pesano in termini di dimensioni e quanto andranno ad impattare sugli applicativi che ne permettono l'archiviazione, primo fra tutti l'applicativo di protocollazione.
Il primo aspetto fondamentale è capire che ogni tipo di file possiede la cosiddetta **estensione**. Tutti i nomi dei file sono quindi composti da un nome "proprio" (quello che il proprietario ha deciso di assegnargli) seguito da una estensione. I due sono separati da un punto. Quindi avremo una sintassi del tipo:
[*nome file*].[*estensione*]
Un tipico esempio potrebbe essere *relazione.pdf*, quindi un documento a cui è stato assegnato il nome "relazione" ed è stato salvato in uno dei formati più comuni e standardizzati, ovvero il PDF.
Il sistema operativo Windows spesso nasconde l'estensione del file per dare una visione più pulita della scrivania all'utente. Invece di far vedere l'estensione Windows cambia l'icona del file basandosi proprio su di essa. Questo significa anche che Windows sa che programma utilizzare per aprire il documento.
Ecco alcuni esempi. L'icona successiva rappresenta un file PDF, che potrebbe essere l'esempio fatto sopra, relazione.pdf

L'esempio sotto invece è l'icona di un documento creato con Microsoft Word. I file Word possono avere un'estensione **.doc** o **.docx** a seconda della versione di Office installata. L'estensione **docx** è quella dei file prodotti con le versioni di Office più recenti.

Quando Windows incontra un file con una estensione sconosciuta mostra un'icona come questa:

Questo significa che Windows non sa come aprire questo documento, ovvero non sa cosa sia l'estensione PDA. Per fare questo esempio è stata modificata a mano l'estensione da PDF a PDA. Questo innesca un altro aspetto importante, la modifica manuale dei nomi file, che tratteremo più avanti.
Vediamo quali sono le estensioni più comuni che si incontrano nel nostro ambiente lavorativo:

- **PDF** -> sta per Portable Document Format, è un formato diffusissimo creato per eliminare i confini tra applicazioni, macchine e sistemi operativi diversi. E' uno standard riconosciuto a livello globale.

- **DOC**, **DOCX**, **XLS**, **XLSX** -> sono i formati dei file prodotti da Microsoft Word e Microsoft Excel della suite Microsoft Office. Le versioni con la X in fondo rappresentano la più recente evoluzione del formato.

- **ZIP**, **RAR** -> sono i cosiddetti file compressi. Un file compresso è un contenitore al cui interno sono presenti più file. Possiamo pensarlo come ad una cartella il cui spazio interno è stato ottimizzato per essere il meno capiente possibile, in un'ottica di risparmio di spazio disco. Una cartella compressa in sostanza. Sono un ottimo strumento per scambiare più file contemporaneamente e per risparmiare risorse.

- **P7M** -> è l'estensione più tipica dei file firmati digitalmente. L'estensione P7M viene aggiunta in fondo alla estensione classica, quindi il tipico formato del file firmato digitalmente sarà **[*nome file*].[*estensione*].P7M**. Viene aggiunta un'estensione in fondo per restituire all'utente il concetto di "imbustamento", ovvero si prende il file originale con estensione, lo si racchiude in una "busta" e lo si firma, passaggio che aggiunge automaticamente l'estensione P7M in fondo.

- **EML** -> è un formato che concettualmente si avvicina molto a quello degli ZIP/RAR ma applicato esclusivamente al mondo della posta elettronica. In sostanza un file EML non è altro che un pacchetto che contiene il testo di una mail e tutti i suoi allegati, tutto in un unico contenitore. Questo formato viene prodotto da alcuni programmi di posta elettronica (Outlook Express, Mozilla Thunderbird), dall'interfaccia web Legalmail della PEC e da alcuni applicativi aziendali (??).

Fatta questa introduzione, vediamo di seguito alcune buone pratiche sull'utilizzo di questi file e contestualmente come evitare procedure scorrette che potrebbero creare problemi.

File firmati digitalmente

Abbiamo visto qual è il formato dei file con firma digitale, ovvero **[*nome file*].[*estensione*].P7M**. Abbiamo anche capito come il sistema operativo (Windows) riconosca i file in base all'estensione. Quando sul PC installiamo un programma per la firma digitale, Windows capisce automaticamente come aprire i file P7M. Se andiamo a scardinare il formato del nome file scritto sopra rischiamo di mandare in confusione il sistema operativo. Con "scardinare" si intende soprattutto manomettere a mano il nome file e le sue estensioni. Vediamo alcuni esempi riscontrabili abbastanza spesso in situazioni reali di lavoro.

1. **Rimuovere a mano l'estensione originale** -> ogni tanto capita di vedere dei file con formato **[*nome file*].P7M**. Questo significa che l'utente ha cancellato a mano la prima estensione o ha modificato il nome file in fase di salvataggio. Quando Windows cerca di aprire questo file prima carica il programma di firma digitale perché riconosce l'estensione P7M, ma al passaggio successivo non sa più cosa fare, perché non sa cosa usare per aprire il documento senza estensione. In sostanza questa operazione non va MAI fatta. Se si ricevono file di questo tipo è necessario contattare il mittente e si hanno due opzioni: o ci si fa rimandare il file nel formato corretto (scelta migliore, anche per educare la controparte) o ci si fa dire qual era l'estensione originale, cosa che possiamo rimettere noi a mano (pratica comunque sconsigliata, perché la regola è MAI manomettere i nomi file, soprattutto quelli con firma digitale)

2. **Nomi file "sporchi" che possono trarre in inganno il sistema operativo o gli applicativi** -> sebbene i sistemi operativi moderni permettano di dare nomi complessi ai documenti (tipo una frase), non è detto che gli applicativi di firma digitale siano altrettanto intelligenti. A volte si trovano file con nomi troppo articolati, tipo *documento.1.doc.p7m* oppure *documento[1] (relazione).doc.p7m*. Nel

primo caso il primo punto potrebbe far pensare che *.1* è la prima estensione e quindi tutto il discorso del formato nome file corretto espresso finora salta. Windows cercherebbe un programma per aprire i file *.1* e sicuramente non lo troverebbe. L'applicativo di firma digitale poi cercherebbe di aprire un file *.1.doc* e anche lui molto probabilmente restituirebbe un errore. Nel secondo esempio le parentesi quadre, quelle tonde e lo spazio potrebbero mandare in confusione il sistema di riconoscimento del formato file. Il succo del discorso è cha la parte [nome file] va tenuta il più pulita possibile. Gli spazi potrebbero non essere un problema, ma punti, parentesi, barre, ecc. vanno evitati assolutamente. Possibile soluzione se l'applicativo di firma digitale non apre in automatico il file: una volta riconosciuto il formato originale ad occhio (tipo *.doc.p7m*) lo si può salvare sul desktop e rinominarlo nel modo più semplice possibile, quindi da *documento.1.doc.p7m* a *a.doc.p7m*, giusto per riuscire ad arrivare al documento originale e consultarlo. Anche qui, se il file ci arriva in questi strani formati possiamo o avvertire il collega dall'altra parte o utilizzare la soluzione scritta sopra

3. **Eccezione: file con tripla estensione del tipo *documento.doc.p7m.p7m*** -> a dispetto di quanto scritto finora, questa è una estensione corretta. Si tratta di un file firmato digitalmente e controfirmato da una seconda persona. Quindi c'è un doppio imbustamento.

Formato PDF

Il file PDF deve sempre essere, quando possibile, il punto di arrivo ideale della versione definitiva del nostro documento. Questo per vari motivi. Il primo è quello esposto sopra nella descrizione del formato PDF. Infatti il formato PDF è ormai entrato ovunque come standard e permette di scavalcare le barriere create dall'usare, per esempio, applicativi diversi o sistemi operativi diversi. Quindi, quasi sempre, quando usiamo un file PDF, non dobbiamo preoccuparci di che programmi o sistema operativo utilizza il nostro interlocutore. Altro vantaggio è che il file PDF non è modificabile, quindi il nostro collega potrà consultare il documento ma non apportarvi modifiche e magari riutilizzarlo per fini a noi sconosciuti. Noi abbiamo l'originale, magari un .doc, lo salviamo in PDF e diamo questa copia al nostro interlocutore. Laddove possibile quindi, utilizzare sempre i PDF.

Strumenti di compattazione: ZIP/RAR e EML

Ogni PC dell'Azienda dovrebbe essere dotato di un programma di compattazione. Quello più diffuso è senz'altro **IZArc**, un programma open source gratuito. Questi programmi permettono di selezionare un gruppo di file e trasformarli in unico file-contenitore con estensione .**ZIP** o .**RAR**. In questo passaggio il programma tenta anche di comprimere i file originali, quindi è possibile che il file finale sia di dimensioni minori rispetto alla somma della dimensione dei singoli file in esso contenuti. I vantaggi di questi aspetti si intuiscono molto rapidamente se si pensa alla posta elettronica. E' infatti molto meglio inviare un unico file piuttosto che 10 o 15 allegati separati. Se questo file poi ci ha fatto risparmiare spazio significa che manderemo sulla rete meno dati e creeremo meno traffico. Quando riceviamo un file ZIP di solito lo riconosciamo da questa icona:

Per analizzare il suo contenuto sarà sufficiente fare doppio clic sul file, selezionare la voce **ESTRAI** dal programma e decidere una destinazione (una cartella o il desktop).

I file con estensione **EML** si avvicinano molto come concetto ai file ZIP, però sono utilizzati solo in ambito di posta elettronica. Molti client di posta elettronica (come Mozilla Thunderbird)

permettono di salvare un messaggio di posta elettronica al di fuori del programma, proprio come si salverebbe un documento di Word o Excel. Così facendo si crea un file con estensione EML. Un file salvato da Mozilla Thunderbird ha un'icona come questa:

Per aprire un file EML che ci arriva da un interlocutore saremo costretti ad avere installato sulla postazione un applicativo (o client) di posta elettronica. Sebbene un salvataggio di questo tipo sia indubbiamente comodo, non è detto che altri interlocutori riescano ad aprire un file del genere, dato che sempre di più si utilizzano webmail al posto dei client (vedi per esempio Gmail, Zimbra, Legalmail PEC) che non possono aprire i file basandosi sulle estensioni, perché sono vere e proprie pagine web, non programmi. Lo standard aziendale dell'AUSL di Parma è il client Zimbra, quindi una soluzione webmail che non si abbina con il formato EML.
Esistono soluzioni alternative per salvare un messaggio di posta con allegati che, sebbene all'apparenza un po' più macchinose, garantiscono più compatibilità con gli interlocutori e più aderenza agli standard utilizzati nel mondo del lavoro. Gli allegati si possono sempre salvare come di consueto, mentre il testo della mail può essere salvato in un documento PDF tramite una "finta stampa", ovvero si segue la procedura di stampa tradizionale ma si ridirige l'output verso un programma che crea un file PDF con all'interno il testo della mail. Si potrebbe poi anche compattare il tutto in unico pacchetto ZIP.
Con la soluzione EML e quella ZIP alla fine si ottiene lo stesso risultato, però i formati della seconda soluzione (PDF + ZIP o ZIP unico) sono molto più vicini alla standardizzazione riconosciuta a livello globale e sono formati preferibili per il lavoro in Azienda. Per esempio protocollare allegati PDF o ZIP è preferibile a protocollare un file EML.
La PEC Aziendale permette da qualche tempo di salvare un messaggio in formato EML. Se per esempio questo passaggio venisse fatto su una postazione su cui non è installato un client di posta elettronica, l'utente stesso che ha fatto il salvataggio non sarebbe in grado di aprire il file che lui stesso ha appena salvato. Il formato EML è quindi molto vincolato ad applicativi che non sono presenti nella gran parte delle postazioni aziendali e molto probabilmente su quelle di colleghi di altre Aziende.

Acquisizione documenti da fotocopiatori e scanner
La trasformazione da cartaceo a digitale passa sempre più spesso da un processo di scansione. In Azienda sono ormai piuttosto diffusi dei fotocopiatori con funzioni di rete che permettono di inviare nelle caselle di posta elettronica una copia digitale di un documento cartaceo.
L'impostazione di default degli scanner è quella di produrre file **PDF**. Spesso però questi PDF sono di qualità troppo elevata, non necessaria per l'utilizzo che se ne fa in Azienda. In questi casi la cosa migliore da fare è contattare il Servizio RIT e chiedere che il fotocopiatore venga impostato per produrre scansioni di una qualità standard che non produca file di dimensioni eccessive. Una pagina PDF scansionata "male" potrebbe anche occupare tanto spazio su disco quanto una fotografia scattata in alta qualità. Queste dimensioni eccessive si ripercuotono in maniera negativa sugli applicativi più utilizzati in Azienda, ovvero la posta elettronica e il protocollo. Razionalizzando sulle dimensioni dei documenti digitali si crea un beneficio globale sul traffico di rete e sulla mole di lavoro che gli applicativi sono chiamati a gestire.
Altri tipi di file ed estensioni
Durante il lavoro quotidiano è possibile incappare in file con estensioni che non rientrano in quelle descritte sopra. Vediamone alcune:

1. **EXE** -> sono i file eseguibili di Windows, ovvero quei file che avviati fanno partire una applicazione. Sono file utilizzati in locale sulle postazioni e non vanno MAI protocollati

o inviati in allegato. Nel 99% dei casi se arriva un file EXE in allegato ad una mail questo è o un virus o qualcosa di altrettanto pericoloso. La nostra posta elettronica blocca gli allegati EXE sia in ingresso che in uscita

2. **JPG** o **JPEG** -> sono il formato più diffuso per le immagini. Sono tipi di file sicuri e spesso utilizzati per inviare immagini. Gli scanner aziendali possono produrre file JPG da cartaceo, ma questa è una impostazione non standard che va corretta, dato che l'output dei fotocopiatori deve essere sempre in formato PDF.

Nome Documento : T0304

Oggetto : Elenco Server Aziendali

Data Ultima Modifica : 29/03/2015

Di seguito l'elenco dei server aziendali installati presso la sala server all'Ugolino in strada del Quartiere 2/A

ARMADIO SX1

DEVICE	HOSTNAME	S/N	UTILIZZO
IBM x346	SERVERLTT	KKRXG5V	Server Intranet LTT, Legge 190/2012
IBM x346	DBEUROSOFT	KKRXG1F	DB Server Appl. Eurosoft
IBM x346	GESCEL	KKRXG9W	Server Gestione Celiaci (DB + A.S.)
IBM x3650	PARMAWEB	KDWKKCC	Application Server Veterinari (Sferacarta) Veterinari (old da dismettere)
IBM x3650	PARMAWEB1 (SICER)	KDWHWTC	Application Server Veterinari (Sferacarta) Veterinari SICER
ACER AR385FI	PARMADB1	SRR8HEE0012410002B9700	db Server Veterinari (Sferacarta) Veterinari)
IBM x345	PROXYINTERNET	551213G	Proxy Internet
IBM x345	PROXYAUSL1	551214M	Server Proxy
IBM x345	PROXYAUSL3	551214R	server proxy Internet
IBM x345	ITACA	551211Z	Servizi SOLE NOEMALIFE - LIS
IBM x345	BACKUPSERVER	551209R	Server di Backup EMC Legato Networker
IBM x345	NEWTSSAN	551212P	Terminal Server Sanitario (ADS) + SOFTWARE DRG
IBM x345	X345_DF	551213F	Server Intranet (old), DB Punto Bianco, DB e applicativo DELIBERE (docflow)
IBM x345	NACSERVER	551211N	Server autenticazione NAC
IBM x345	PRGSCOMPENSO	551167Y	server per Prog. Scompenso Cardiaco

ARMADIO SX2

DEVICE	HOSTNAME	S/N	UTILIZZO
DELL P.E. 1850	ITACA1	7SK9F1J	DBServer Itaca-Galileo (cluster)
DELL P.E. 1850	ITACA2	6SK9F1J	DBServer Itaca-Galileo (cluster)
BLADE DELL	DBProtocollo	9BQLF1J	DB procedura Protocollo - DATABASE ORACLE PROCEDURA DI PROTOCOLLO
P.E. 1855	ASITACA1	DBQLF1J	Appl. server procedura Itaca-Galileo
(inferiore)	NAGIOS1	CQSHG2J	Server per monitoraggio rete (Nagios, …)

service tag 39QLF1J	BDSOLEDB	1DQLF1J	db DWH Case della Salute, appropriatezza, Statistiche, Indicatori, Business intelligence
	ASITACA2	H9QLF1J	Appl. server procedura Itaca-Galileo

ARMADIO SX3

DEVICE	HOSTNAME	S/N	UTILIZZO
DELL P.E. 1850	AMMINISTRATIVOTEST	7WK9F1J	db oracle per le procedure contabilita' ordini magazzino richieste consegna a paziente-cassamav-casse-silor conto deposito-gest-status (TEST)
F.S. RX300S4	PLUTONE	YKAF023447	StandBy + Report DB Sanitario (ADS)
HP PROLIANT DL560 G8	AMBPRDB1	CZ25030118	DB server Ambulatoriale (Elco) (cluster nodo1)
HP PROLIANT DL560 G8	AMBPRDB2	CZ2503011K	DB server Ambulatoriale (Elco) (cluster nodo2)
HP PROLIANT DL560 G8	SIAVRDB1	CZ2503011J	DB Server Vaccinazioni (ONIT) (cluster nodo1)
HP PROLIANT DL560 G8	SIAVRDB2	CZ2503011H	DB Server Vaccinazioni (ONIT) (cluster nodo2)
F.S. RX300S4	VADPPROXY	YKAF023441	Proxy per il backup dei server virtuali
F.S. RX300S4	DBRUR	YKAF023443	DB+AS Server Invalidi Civili
F.S. RX300S4	LHADEDALUS	YKAF023445	servizio LHA Celiaci di Dedalus (DB+AS)
F.S. RX300S4	DBENG	YKAF023442	DB server Engineering E-Prescription
F.S. RX600S6	RISPRDB1	YL6T028514	OracleDBServer RIS-POLARIS - ELCO (nodo1)
F.S. RX600S6	RISPRDB2	YL6T028515	OracleDBServer RIS-POLARIS - ELCO (nodo2)
IBM BLADECENTER H p/n 8852-4TG s/n KD0M2K2 (192.168.19.7)	MARTE	06LAPH7	DB Server Sanitario ADS
	VENERE	06LAPH6	DB Server Sanitario ADS
		06LAPH5	NON UTILIZZATO
	dnlabpr2	06LAPH3	DB server DNLAB-Mercurio (nodo 2)
	amministrativo	06LAPH4	DBServer Bilancio - db oracle per le procedure contabilita' ordini magazzino richieste consegna a paziente - cassamav - casse - silor conto deposito - gest - status
	dnlabpr1	06LAPH2	DB server DNLAB-Mercurio (nodo 1)
		06YETZ3	NON UTILIZZATO
	ESX8	06YETY9	VMWare vSpherre host nodo 8
	ESX9	06YETZ0	VMWare vSpherre host nodo 9
	ESX10	06YETZ1	VMWare vSpherre host nodo 10
	ESX11	06YETY8	VMWare vSpherre host nodo 11
	ESX12	06YETZ2	VMWare vSpherre host nodo 12
	ESX13	06YETZ5	VMWare vSpherre host nodo 13

	ESX14	06YETZ4	VMWare vSpherre host nodo 14

ARMADIO DX1

DEVICE	HOSTNAME	S/N	UTILIZZO
DELL P.E. 1850	DNSEXT	8SK9F1J	DNS + Spazio Giovani - spazio FTP per scambio file con fornitori
DELL P.E. 1850	VPNAVEN	GSK9F1J	server VPN verso AVEN (IPSec)
DELL P.E. 1850	SERVER.RETE	BSK9F1J	DHCP+DNS+autoparco
DELL P.E. 1850	PROXYWOL	HSK9F1J	Proxy Wake On Lan
DELL P.E. 1850	DPS	3HCBF1J	Server DPS (vecchio)
BLADE DELL P.E. 1855 (superiore)	OPENVPNNEW	GQSHG2J	Server per accesso via OpenVPN
	PARMA.SFERACARTA.COM	DQSHG2J	Server applicativo "Sferacarta" (Veterinaria)

ARMADIO DX2

DEVICE	HOSTNAME	S/N	UTILIZZO
HP PROLIANT DL560 G8	?	CZ2503011P	cartella clinica
HP PROLIANT DL560 G8	?	CZ2503010Q	cartela clinica
HP PROLIANT DL560 G8	?	CZ25030103	DNLab LIS (Nomalife)
HP PROLIANT DL560 G8	?	CZ25030104	DNLab LIS (Nomalife)
F.S. RX300S4	VCENTER	YKAE004693	vCenterServer (di riserva)
F.S. RX300S4	PROXYCUP	YKAE004700	era stata battezzata come reverse proxy fisico di riserva
F.S. RX300S4	DBZEN	YKAF022677	Zensistemi (DB SPSAL UOIA SIP MEDICO COMPETENTE NIP)
F.S. RX300S4	DBPERSONALE	YKAF023366	DB Server Personale - db oracle per procedure paghe presenze giurdica formazione
F.S. RX300S4	ASPERSONALE	YKAF023365	Application Server Personale - application per procedure paghe presenze e giurdica formazione - PROCEDURA OROLOGI ANTIGUA- PROCEDURA TIMBRA.EXE - PROC. MEDICI CONVENZIONATI - WORKFLOW GIUSTIFICATIVI

ARMADIO DX3

DEVICE	HOSTNAME	S/N	UTILIZZO
HP PROLIANT DL560 G8	PIESSEDB1	CZ2503011N	PIESSE (CBIM) (cluster nodo1)
HP PROLIANT DL560 G8	PIESSEDB2	CZ2503010T	PIESSE (CBIM) (cluster nodo2)

HP PROLIANT DL560 G8	**ADSANAMPI1**	CZ25030115	Anagrafe MPI (ADS)(cluster nodo1)
HP PROLIANT DL560 G8	**ADSANAMPI2**	CZ25030113	Anagrafe MPI (ADS)(cluster nodo2)
HP PROLIANT DL560 G8	**ADSADTDB1**	CZ25030119	DB server ADT (ADS)(cluster nodo1)
HP PROLIANT DL560 G8	**ADSADTDB2**	CZ2503011L	DB server ADT (ADS)(cluster nodo2)
HP PROLIANT DL560 G8	**ESX15**	CZ250603JK	Host vSphere (h24)
HP PROLIANT DL560 G8	**ESX16**	CZ250603J2	Host vSphere (h24)
HP PROLIANT DL560 G8	**ESX17**	CZ250603JO	Host vSphere (h24)
NEC EXPRESS 5800	**WEBTAX**	100013721128	server WEBTAX per registrazione call telefoniche
HP PROLIANT DL385G6	**PACSFED**	CZC9313QXQ	PACS Federale (CUP2000)
HP PROLIANT DL360G7	**SANETHOST**	??	appliance monitoraggio SANET (Lab. Marconi)

Di seguito l'elenco dei server aziendali installati presso la sala server nell'Ospedale di Fidenza in via Don Tincati a Fidenza

RACK SERVER HP

schema del Rack	S/N	hostname	Utilizzo
HP ProLiant DL380 G4	GB85158NN0	SERVERPDF	Server generatore PDF x Firma Digitale Lab Fidenza
HP ProLiant DL380 G4	GB85158NNH	MULTIFUNC	Multifunzione Statistche Lab e Collegamenti Termina Server
HP ProLiant DL380 G4	GB85158NNB	WINDOPATH	Server applicativo Windo Path (ANATOMIA PATOLOGICA CITOLOGIA)
HP ProLiant DL380 G4	GB85158NNT	VMWAREFID	Host VMWare Server
ACER AR385FI	SRR8HEE001241000299700	PROXYFID1	proxy Internet
ACER AR385FI	SRR8HEE001241000289700	PROXYFID2	proxy Internet

Di seguito l'elenco dei server aziendali installati presso l'Ospedale di Borgo val di Taro in via Benefattori a Borgo val di Taro

BORGOTARO

schema del Rack	S/N	hostname	Utilizzo

ACER AR385FI	SRR8HEE001241000229700	PROXYBOR1	proxy Internet
ACER AR385FI	SRR8HEE001241000279700	PROXYBOR1	proxy Internet
Tecnosteel KVM	1218GC0031		

Di seguito l'elenco dei server installati nell'ambiente virtuale VMWARE

hostname VM	Utilizzo VM
3pstudiovm	server applicativi 3Pstudio - procedure per la gestione dei pazienti del Dipartimento di salute mentale ELEA e EFESO
adsbridge	macchina ponte per ADS
adsias1	application server iAS Sanità
adsias2	application server iAS Sanità
adsias3	application server iAS Sanità
adsias4	application server iAS Sanità
adstom1	application server Tomcat Sanità
adstom2	application server Tomcat Sanità
adstom3	application server Tomcat Sanità
adstom4	application server Tomcat Sanità
alfresco	server documentale Alfresco - DATI DI PROTOCOLLO, PEC DIREZIONE, UFFICIO LEGALE, FORMAZIONE - doc/er
anagrafesole	Application server Anagrafe Sole (Tomcat anagrafe Sole gestita da CUP2000)
asdedalus	AS Server applicativi Dedalus (Screening)
asdedalustest	AS di test applicativi Dedalus
aseurosoft1	Application Server Eurosoft (ADI, Medicina Sportiva, Consultori, Spazio Immigrati)
aseurosoft1test	Application Server Eurosoft (test)
aseurosoft2	Application Server Eurosoft (ADI, Medicina Sportiva, Consultori, Spazio Immigrati)
aseurosoft3	Application Server Eurosoft (ADI, Medicina Sportiva, Consultori, Spazio Immigrati)
asigc	AS applicativi IGConsulting (Mercurio, Tantra, Nettuno, ….)
asprotocollo	DB procedura Protocollo - DATABASE ORACLE PROCEDURA DI PROTOCOLLO
asprototest	as protocollo di test
adsiastest	test application server iAS Sanità
adstomtest	test application server Tomcat Sanità
aszen1	Application Server Zensistemi
aszen2	Application Server Zensistemi
auriga	server progetto Auriga (flusso ASA) (DB+AS)
ausldom	Dominio di rete, LDAP slave, PDC
ausldomtest	Dominio di rete, LDAP slave, PDC (per test e collaudo)
bct	server centralino BCT
bdcpr	Backup Domain Controller PR
bsoleas	AS server progetto Bsole CUP2000 (DWH Case della Salute, appropriatezza, Statistiche, Indicatori, Business intelligence)
busterspid	monitoraggio armadi farmaci Fidenza DBSERVER MS SQL SERVER + integrazioni
carcere	applicativo Carcere CCI
cardioline	DB ECG CARDIOLINE e prove da sforzo (Fidenza)
cassaedile	Cassa Edile
cdg	AS per Controllo di Gestione

centos5test	macchina di test linux
centos5test64	macchina di test linux
co118	server Centrale Operativa 118
dbdedalus	DB Server applicativi Dedalus (Screening, Medicina, Sportiva, Consultori, Spazio Immigrati)
dbdedalustest	DB di test applicativi Dedalus
dbigc	DB Server IGConsulting MERCURIO
dbrurtest	DB Server applicativi RUR-ER di TEST
docer	applicativo Docer middleware comunicazione documentale
egate	server applicativo eGate (Itaca)
energybrain	sistema monitoraggio Energy Brain - Electrex (Fidenza)
esrsgw	EMC Secure Remote Support Gateway
etichette1	ISEE Etichette + Applicativi Interni + DNWEB x Azienda Ospedaliera
etichette2	ISEE Etichette
eurotouch	Server applicativo Eurotouch (Diabetici)
farmadati	Server applicativo Farmadati - Gestione automatizzata degli aggiornamenti da farmadati a ns. gestionali - applicativo farmadati - scarico notturno della tab mmg-rer notturna
federation	server IdP per autenticazione con AVEN
firmadigitale	postazione Firma Digitale Borgotaro DNREFERTI
flowdoc	server documentale Flowdoc (Alfresco)
kofax	server Kofax firma ellettronica Calamaio
gammacompmd	Server GammaComMD calibrazione monitor medicali NEC
geriatria	Server applicativi Lunghi Osservatorio Geriatria
guatemala	PC di test Luca
helicswin	applicativo HELICSwin: raccolta dati prevernzione malattia
hemalink	postazione Hemalink monitoraggio analizzatori (Siemens)
igconsulting	Server DSS (IGConsulting) - applicativi controllo di gestione e flussi - MUSA, DART, FAR, FEDORA, DIAMANTER,MERCURIO, NETTUNO
imed	server applicativo iMed
intranetausl	server Intranet (nuovo)
intranetdps	server Intranet DPS
itaca-AS-test	AS test Itaca
itaca-DB-test	DB test Itaca
jboss	Appl. Server JBOSS - Applicativi GPI CONTAB, CESPITI, MAGAZZINO, RICHIESTE,CASSAMAV, SILOR,GEST,STATUS,GALENCIA
jbosstest	Appl. Server JBOSS - Applicativi GPI CONTAB, CESPITI, MAGAZZINO, RICHIESTE,CASSAMAV, SILOR,GEST,STATUS,GALENCIA
jpdfwriter	JPDFWriter: generatore PDF
lamp	Server Linux, Apache, MySQL, PhP procedure DUVRI, fatturazione sat, SCARICO OSSIGENO,SANZIONI, LEGALE,PROTOCOOLI RISERVATI,DISPOSITIVI ,MEDICI,ambulatori MMG e PLS, offerta formativa, gestione trasparenza,persone/uffici,rubrica,anagrafe,formazione ECM,timbrature, pasti mensa,repe-rit,repe-sat, interfaccie web presenze/assenze PUNTO BIANCO PATENTI, CAMPAGNA VACCINALE, CERTIFICATI MEDICI NON SPEDITI, REGISTRO ASSEGNAZIONE PRATICHE, GESTIONE REPERIBILITA', Ossigeno Ospedaliero, Fasce Reddito
lampext	Server Linux, Apache, MySQL, PhP (per esterni), RACCOLTA PRESENZA (REGPAS), ReadHealth (MMG-case della salute)
lamptest	Server Linux, Apache, MySQL, PhP
ldapserver	Server LDAP master, Rap3
logserver	Log server Splunk
mobilitystat	Portale Statistiche Mobilità - PROCEDURA MOBILITA' SOTENIBILE
ocs_otrs	OCS Inventory + OTRS
otrs	server OTRS 3
ocs	OCS Inventory 2.1

paf	Piano Formativo Aziendale
parer	server applicativo Parer
pensioni	Server applicativo Pensioni
pensioninew	Server applicativo Pensioni (nuovo aggiornato)
pentaho	applicativo Pentaho (Server Reportistica RIS)
profis2k8	server applicativo Profis (Roberta Bruschi)
proxyausl	server Proxy Internet
qbox	server Qbox (appropriatezza prescrittiva)
qlik	Reportistica Direzionale PROCEDURE AMMINISTRATIVE E TERRITORIALI
qlikserver	QLIK server - reportistica aziendale
radiance	applicativo Radiance per Emogasanalizzatori (Ditta Laboratorio)
radius	server autenticazione Radius
radius_test	test radius
remotecheckads	server di raccolta dati per remote checking ADS
repobackup	repository dei backup
repository	Repository aziendale di rete
reverseproxy	Reverse Proxy
rispras1	Appl. Server RIS (Elco)
rispras2	Appl. Server RIS (Elco)
risprprint	Integrazioni Elco con sistemi esterni
risprqway	server per il Broker degli ecografi (Refertazione ecografica (polaris <-> ecografi))
risprvoc	riconoscimento vocale RIS
risprweb	application server RIS- WHALE per order Entry
serveriap	Server Applicativo IAP (GESTIONE DATI E NUMERO VERDE REGIONALE)
serverlunghi	Server applicativi Lunghi SOCIALE FIDENZA (ADULTI LiqCA Minori) SAA FIDENZA (SADid LiqSaa Saaprot) Sil Fidenza (Kronos Leonardo Equipe_Sil Sildistr) CARCERE (DisagioPSIcarcere) GraDA Grave Disabilità Acquisita, DISABILI,SPG , Spazio Giovani Osservatorio Dipendenze (AZIENDALE) ,GBA.mdb ,SAA Sud-Est (PVC GDSaa),SAA Vlli Taro e Ceno (UVGtc
sister	Server progetto SISTER (SERT)
sondaggio	Portale Questionario Intranet/Internet (Fabio/Thomas)
susupdate	Susupdate 3
test-auth	test per autenticazione SSH-PAM-LDAP
tsserver	Server Servizi Terminal
tstao	Terminal Server TAO (+Gepadial) DIALISI
urologiafid	server applicativo Urologia (ex benecchi)
vcenter	Virtual Center 5
vcenterserver	Virtual Center 5.5
webtax	server WEBTAX per registrazione call telefoniche
win2k12test	macchina Windows 2012 per i test
win2k3test	macchina Windows 2003 per i test
win2k8test	macchina Windows 2008 per i test
win7test	macchina Windows 7 per i test
win8test	macchina Windows 8.1 per i test
Zimbra64	server posta Zimbra 7 64 bit
spylog	applicativo Spylog monitoraggio temperatura frigoriferi materiale organico laboratorio (DB+AS)

aseng1	AS server Enginnering E-Prescription
aseng2	AS server Enginnering E-Prescription
aseng3	AS server Enginnering E-Prescription
aseng4	AS server Enginnering E-Prescription
aseng5	AS server Enginnering E-Prescription
aseng6	AS server Enginnering E-Prescription
aseng7	AS server Enginnering E-Prescription
baleng	server per il balancing Engineering E-Prescription
portaleosa	AS portale OSA veterinari
avenbridge	macchina proxy per NAT chiamate di rete su VPNAven
gridcontrol	installazione Oracle Griod Control per management DB
f-secure	F-Secure Server + console amministrazione F-Secure
logserverrete	server raccolta log per apparati di rete
wikirit	Wiki Ausl
rizone3	RiZone Software Appliance: applicativo Rittal per monitoraggio armadi sala server
auslbridge	macchina ponte per amministrazione remota
maps	SAM Microsoft per mappatura licenze
dbfeticehtte	server stampa etichette
dbzen2k3	DB Server Zen Sistemi (temporaneo)
snmpmaster	macchina master per monitoraggio server via SNMP
tsserver2k8	serve licenze TS 2008
cosmed	gestione spirometri Omnia Network
pingpolling	polling apparati di rete Lepida
lamp64	server LAMP 64 bit applicativi aziendali
sflow	collector sFlow per monitoraggio qualitativo rete
ambprtest	ambulatoriale Elco di test
piessetest	PIESSE di test (CBIM)
alfrescotest	Alfresco di test
flowdoctest	Flowdoc di test
log80	server Prescizione Oncologica LOG80
intellispace	sw IntelliSpace ECG Philips (mini PACS)
vcproxy	proxy videoconferenza Lepida
siavrtest	ambiente test Vaccinazioni (Onit)
siavr1	application server Vaccinazioni (Onit)
siavr2	application server Vaccinazioni (Onit)
engtest	ambiente di test Engineering E-Prescription
ftparea	area FTP di interscambio

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : T0305

Oggetto : Elenco connessioni VPN

Data Ultima Modifica : 25/03/2015

Di seguito l'elenco dei certificati attivati per le connessioni VPN

Nome Ditta	Indirizzo
3T Telecomunicazioni	Stradello Agostini 3, Parma
A. Demori	Via Portaluppi 15, Milano
Ad Personam	Via Cavestro 14, Parma
ADS	Via del Lavoro 17, Bologna
AHSI	Via delle Industrie 33, Bernareggio (MB)
AICOD	Via Cassio Parmense 3, Parma
Ambulatorio San Moderanno	Via Trieste 108, Parma
ASP Azienda Sociale Sud-Est (Val Parma)	Via Don Orsi 1, Langhirano (PR)
ASP Cav. Marco Rossi Sidoli	Via Duca degli Abruzzi 27, Parma
ASP Sede Legale Fidenza	Viale Berenini 151, Fidenza (PR)
Assistenza Pubblica Parma (118)	Viale Gorizia 2/A, Parma (PR)
AVIS Casale di Mezzani	Via Cantoni 3, Casale di Mezzani (PR)
Axios Informatica	Via Sebastian Bach 7, Bassano del Grappa (VI)
Azienda USL di Bologna	Via Castiglione 29, Bologna
Azienda USL di Padova	Via Casa di Ricovero 40, Cittadella (PD)
Biomerieux	Via di Campigliano 58, Firenze
Carestream	Via al Porto Antico 6, Genova
Casa Anziani Collecchio	Via Aldo Moro 2, Collecchio (PR)
Casa degli Anziani di Sorbolo	Via Beethoven 11, Sorbolo (PR)
Casa di Cura Città di Parma	Piazzale Maestri 5, Parma
Casa per Anziani Fondazione Cav. B. Patrioli	Via Giuseppe Verdi 37, Medesano (PR)
Casa Protetta Ca' Bonaparte	Località Ca' Bonaparte, Neviano degli Arduini (PR)
Casa Protetta Città di Fidenza	Via Esperanto 13, Fidenza (PR)
Casa Protetta Città di Salsomaggiore	Viale Rimembranze 17, Salsomaggiore (PR)
Casa Protetta Don Gottofredi	Strada Ospedale 4, Roccabianca (PR)
Casa Protetta Don Prandocchi Cavalli	Via Don Minzoni 24, Sissa (PR)
Casa Protetta Gino Cavazzini	Via Olari 6, Berceto (PR)
Casa Protetta Lorenzo Peracchi	Via XXIV Maggio 16, Fontanellato (PR)
Casa Protetta Ospedale Dagnini	Viale Matteotti 23, Zibello (PR)
Casa Protetta P. Corsini	Via Micheli 1, Pellegrino Parmense (PR)
Casa Protetta Pavesi Borsi	Via Matteotti 25, Noceto (PR)
Casa Protetta Pellegrino Parmense	Via Sonnino, Pellegrino Parmense (PR)
Casa Protetta San Mauro	Via Guglielmo Marconi 12, Colorno (PR)
Casa Protetta Santa Rita	Via IV Novembre 32, Soragna (PR)
Casa Protetta Selene Conti	Via Donatori Sangue 4, Borgo val di Taro (PR)
Casa Protetta Tommasina Sbruzzi	Via Battisti 42, San Secondo (PR)
Casa Protetta Villa Benedetta	Via Roma 4, Sala Baganza (PR)
Casa Protetta Villa Pigorini	Via IV Novembre 2, Traversetolo (PR)
Casa Protetta Villa San Bernardo	Strada Bodrio 14, Porporano (PR)
Casa Protetta Zanetti	Via Alla Rocca 1, Varsi (PR)
CBIM	Piazzale Volontari del Sangue 2, Pavia
CEDAS Srl	Via Nazionale 102, Borgo Val di Taro (PR)
Centro di Solidarietà l'Orizzonte	Via Testi 4/a, Parma
Centro Fisioterapico Maria Luigia	Strada della Repubblica 47, Parma
CISL Parma	Via Lanfranco 21/A, Parma

Comune di Fidenza	Piazza Garibaldi 1, Fidenza
Comune di Neviano degli Arduini	Piazza IV Novembre 1, Neviano degli Arduini (PR)
Comune di Trecasali	Via Nazionale 44, Trecasali (PR)
Comune di Varsi	Via Roma 13, Varsi (PR)
Comune di Zibello	Via Matteotti 10, Zibello (PR)
Comunità di Servizo e Assistenza Betania	Strada del Lazzaretto 26, parma
Comunità Montana Valli Taro e Ceno	Piazza XI Febbraio 7, Borgo Val di Taro (PR)
Comunità Terapeutica Casa di Lodesana	Via Cabriolo 75, Fidenza (PR)
Consorzio Zenit Casa Protetta Alberi di Vigatto	Strada Alberi, Alberi di Vigatto (PR)
Consorzio Zenit Casa Protetta R. Vasini	Via Nazionale, Fornovo (PR)
CSAMED	Via Grado 26, Cremona
CUP 2000	Via del Borgo di San Pietro 90/c, Bologna (BO)
Data4	Via Strada della Selva 87, San Bonifacio (VR)
Dedalus	Via Giardini 454/B, Modena
Dialcenter	Via P. Zuffardi 5, Fornovo (PR)
Dialpoint	Via Verdi 24, Traversetolo (PR)
ELCO	Piazza della Vittoria 24/B, Savona
ELMEC	Via Pret 1, Brunello (VA)
Engineering Sanità Enti Locali	Galleria del Leone 3, Bologna
ET Medical Devices	Via De Zinis 6, Cavareno (TN)
Exprivia	Via Carlo Esterle 9, Milano
Farmacia di Scurano	Via Mercato 141, Scurano (PR)
Farmacia Leonardi	Via Martiri della Libertà 24, Varano de Melegari (PR)
Farmacia Rosso	Via Roma 25, Bore (PR)
Farmacia Scimonelli	Via Roma 18, Varsi (PR)
Fondazione Alfonso Pallavicino	Via XXV Aprile 6/8, Busseto (PR)
Fondazione Casa di Padre Lino	Viale Caprera 16, Parma
GPI	Via Ragazzi del '99, Trento
Gruppo Galeno	Via Musini Luigi 2, Parma
Gruppo Medico Dedalo	Largo Palli 1/A, Parma
Gruppo Pablo	Via La Grola 5, Parma
Gruppo Partners Associates	Via Pradamano 30, Udine
IG Consulting	Strada Martinara 325/B, Modena
Info Line Srl	Via Colorno 63/A, Parma
Infocert	Corso Stati Uniti 14, Padova
Instrumentation Laboratory	Viale Monza 338, Milano
KDM	Via Roberto Bracco 42/B, Roma
La Traccia	Recinto Il Fiorentini 10, Matera
Laboratori Guglielmo Marconi	Via Porrettana 123, Pontecchio Marconi (BO)
LOG 80	Via Cervese 47, Forlì (FC)
ME.TE.DA.	Via Campania 25, San Benedetto del Tronto (AP)
Medical Software System	Via Chiletti 29/2, San Prospero (MO)
Medicina di Gruppo Berceto	Piazza Micheli 8, Berceto (PR)
Medinf	Via Giardini 454/B, Modena
Newteam Srl	Via Chiesa San Cristoforo 1667, Cesena
Nihon Kohden Italia	Via San Tommaso 78, Bergamo
Noemalife	Via Gobetti 52, Bologna

ONIT	Via dell'Arrigoni 308, Cesena
Ospedale Piccole Figlie	Via Po 1, Parma
Partech	Stradello Ada Negri 6, Parma
Poliambulatorio Dalla Rosa Prati	Via Emilia Ovest 12, Parma
PROGEL	Via Due Ponti 2, Argelato (BO)
Quality Group	Via Enzo Ferrari 23, Arluno (MI)
Rastelli Giovanni (Telecom)	Via Argine 30, Soragna (PR)
Residenza Villa Matilde	Via Bracchi 10, Felino (PR)
Rittal	SP 14 Rivoltana, Vignate (MI)
SAA Langhirano	Piazza Ferrari 5, Langhirano (PR)
Samsung Italia	Via Carlo Donat Cattin 5, Cernusco sul Naviglio (MI)
Santa Lucia Ingegneria Biomedica	Via Vittime della Strada 2, Gragnano Tr. (PC)
Sferacarta Net	Via Bazzanese 69, Casalecchio di Reno (BO)
Siemens	Viale Piero e Alberto Pirelli 10, Milano (MI)
SIOMED	Via Porta Est 17, Venezia
SIRAM	Via Bisceglie 95, Milano
Studio Magdala	Via Crespi 41/A, Bologna
Studio Medico Associato Fidenza	Via Bacchini 18, Fidenza (PR)
Technologic	Lungo Dora Voghera 34, Torino
Università di Modena e Reggio Emilia	Viale A. Allegri 9, Reggio Emilia
Villa Mater Gratiae	Via Madonnina 233bis, Bardi (PR)
Villa Matilde	Via Costa 135, Bazzano (PR)
Zen Sistemi	Via Pizzetti 2, Reggio Emilia

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : P0301

Oggetto : Videosorveglianza

Data Ultima Modifica :Elenco in corso di aggiornamento

Nel rispetto della direttiva 29 aprile 2004, emanata dal Garante per la privacy in materia di installazione ed utilizzazione di impianti di videosorveglianza, l'Azienda USL ha:

Impianti installati in strutture dell'Azienda USL di Parma sia per il controllo dei pazienti ricoverati che per il controllo degli accessi.

STRUTTURA	INDIRIZZO	N° VIDEOCAMERE
Dipartimento di Sanità Pubblica	Via Vasari (PR)	4
Polo Sanitario Vilma Preti	Via Verona (PR)	3
Dipartimento Tecnico e delle Tecnologie	Via Spalato, 2 (PR)	14
Sede SPOI – SPDC – Padiglione Braga	Ospedale Maggiore di Parma	15
SERT	Strada Mercati (PR)	6
Centro Distribuzione Metadone	Via del Taglio (PR)	3
Poliambulatori di Fornovo Taro	Via Solferino – Fornovo Taro	8
Ospedale di Vaio	Via Don Tincati, 5 - Fidenza	31
Casa della Salute di Colorno	Via Suor Maria 3 - Colorno	8
Poliambulatori di via PINTOR	Via Pintor 1 - Parma	8
Colorno I Maggio	Via Roma 16 - Colorno	4
Neuropsichiatria Infantile	Via Bocchi/angolo Via Savani (PR)	4
Centro Autismo	Via La Spezia (PR)	4
Polo Sanitario di Langhirano	Via Roma - Langhirano	7
Ospedale di San Secondo P.se	Via M.V.Mazza - San Secondo	6

Ai Responsabili delle Strutture Aziendali sono state impartite specifiche disposizioni in ordine al corretto utilizzo dei sistemi di videosorveglianza. Sono stati altresì apposti presso ogni punto (videocamera) specifici cartelli riportanti l'informativa "MINIMA" costituita dall'indicazione del titolare del trattamento e la finalità che si intende perseguire. Gli stessi sono stati posizionati prima del raggio d'azione delle telecamere e sono visibili in ogni condizione di illuminazione ed informano se le immagini sono solo visionate o anche registrate. Nei locali delle Strutture aziendali è affissa l'informativa completa, così come prevista dal citato art. 13 del Codice: E' facilmente accessibile agli interessati e contiene il nominativo di un incaricato perchè la fornisca anche (se richiesto) oralmente.

Nome Documento : P0401

Oggetto : Linee di indirizzo per la gestione del dossier sanitario nelle aziende sanitarie di AVEN

Data Ultima Modifica :25/11/2014

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Area Vasta Emilia Nord

Linee di indirizzo per la gestione del dossier sanitario nelle aziende sanitarie di AVEN

Redattori del documento: gruppo responsabili ICT e referenti privacy riuniti in AVEN Data di ultima revisione del documento: 25/11/2014 Stato del documento: Bozza

Sommario

Premessa

Nel corso degli ultimi anni le aziende sanitarie **hanno implementato e innovato i loro sistemi informativi sanitari allo scopo di migliorare l'efficienza e l'efficacia delle cure dei pazienti**; tali innovazioni tecnologiche, in particolare, hanno consentito a più organismi sanitari o a più professionisti di condividere informaticamente i dati di salute di un medesimo individuo e quindi di consultare **in modo più veloce e diretto** la storia clinica dei loro pazienti, con indubbi miglioramenti nel processo di cura dei pazienti stessi.

Tale opportunità, che consente un evidente progresso **nel perseguimento delle finalità di prevenzione, diagnosi, cura e riabilitazione**, deve però **tenere conto di specifiche cautele**, volte a proteggere la riservatezza, la libertà e la dignità dei pazienti.

Infatti, fin dalla iniziale esposizione dei principi generali, il **c.d. Codice Privacy** (D. Lgs. 196/03) sancisce che il trattamento dei dati personali deve svolgersi "*nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali*".

Da tale enunciazione derivano in capo a chi tratta dati personali, e a maggior ragione dati sensibili, come nel caso della aziende sanitarie, una serie di obblighi, non solamente di riservatezza nei confronti dei pazienti e di tutela, protezione e sicurezza dei loro dati, ma anche di garanzia agli utenti della **piena libertà di scegliere**, **sulla base del consenso, se far costituire o meno un documento che raccolga informaticamente la loro storia sanitaria, posta l'ampia sfera conoscitiva che un simile strumento può avere**.

Tale documento, che l'Autorità Garante definisce “dossier sanitario”, costituisce l'oggetto delle presenti Linee di indirizzo.

Scopo del documento e ambito di applicazione

Il presente documento si prefigge lo scopo di indicare alle Aziende Sanitarie afferenti all'Area Vasta Emilia Nord (AVEN) le corrette modalità di gestione del c.d. dossier sanitario, nel rispetto della normativa in materia di trattamento dei dati personali, garantendo in particolare l’aderenza al **principio di pertinenza e non eccedenza del trattamento** nella gestione dei dati sensibili.

In questo documento si sintetizzano le regole per garantire il rispetto dei principi esposti e la realizzabilità tecnica e la sostenibilità organizzativa, nella gestione del c.d. dossier sanitario, sotto il duplice profilo di:

1. modalità e profili di accesso
2. consenso preliminare alla costituzione del dossier sanitario.

Definizioni

Dossier: strumento costituito presso un’unica struttura sanitaria, titolare del trattamento dei dati, al fine di consentire la condivisione logica tra più professionisti dei diversi eventi clinici occorsi ad un assistito, al fine di offrire allo stesso un migliore processo di cura.

Contatto: si intende solitamente per *contatto* il periodo di tempo nel quale un certo paziente è presente presso una certa struttura sanitaria per fini di prevenzione, diagnosi, cura, riabilitazione (ad esempio, un contatto di ricovero andrà dalla data e ora di accettazione fino alla data e ora di dimissione).

In questo documento il concetto di contatto viene esteso a tutte quelle fattispecie in cui il paziente è comunque ***in carico*** ad un certo professionista, o ad una certa équipe, o ad una certa struttura per un episodio o percorso di cura (anche se il paziente non è fisicamente presente).

In questo documento si considerano pertanto sovrapponibili i concetti di contatto/ episodio/percorso di cura/presa in carico.

Oscuramento: modalità tecnica che consente, su richiesta dell’interessato, di non fare confluire nel dossier sanitario alcune informazioni o eventi della sua storia clinica.

Oscuramento dell’oscuramento: modalità tecnica che garantisce che i soggetti che accedono al dossier non possano venire a conoscenza del fatto che l’interessato ha effettuato la scelta di oscurare uno o più eventi della sua storia clinica.

Anonimizzazione: sostituzione dei dati identificativi dell’interessato con un codice, così da non renderlo più riconoscibile all’interno del sistema.

Normativa e documenti di riferimento

1. *Decreto legislativo 196/2003*
2. *Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario - 16 luglio 2009*
3. *Provvedimento Garante Privacy n. 3 del 10/01/2013 “Dossier sanitario e trattamento dei dati personali dei pazienti”*
4. *Provvedimento Garante Privacy n. 340 del 3/07/2014 “Trattamento di dati tramite il dossier sanitario aziendale”*

Contesto organizzativo e scenario tecnico

Gli accessi al dossier sono consentiti per finalità di prevenzione, diagnosi, cura, riabilitazione del paziente e solamente per il periodo di tempo in cui si articola la presa in carico.

In occasione dei suddetti accessi occorre garantire:

- che tutti i professionisti coinvolti nel percorso diagnostico, terapeutico ed assistenziale del paziente (e quindi anche coloro che, ad esempio, siano chiamati a consulenza)

dispongano di tutte le informazioni necessarie per la cura del paziente, ad eccezione di quelle espressamente oscurate dal paziente stesso;

- che altri professionisti che non entrano nel percorso diagnostico, terapeutico ed assistenziale non possano avere accesso alle informazioni che si originano durante tale percorso o a quelle già presenti nel dossier;
- che, terminata la presa in carico ivi compreso il completamento delle attività connesse, i professionisti di cui al punto 1) non possano accedere né alle informazioni relative a quel percorso né ad aggiornamenti della storia clinica del paziente, a meno che non lo abbiano di nuovo in carico.

E' fatto salvo quanto previsto dal paragrafo 5.2.

a)Profili di accesso

Gli accessi alle informazioni del dossier devono essere configurati per garantire il rispetto dei principi di pertinenza e non eccedenza.

Il titolare del trattamento o il responsabile designato dal titolare nel nominare gli incaricati impartisce loro istruzioni in merito alle particolari modalità di creazione e utilizzo del dossier sanitario; il titolare o il responsabile deve inoltre richiedere all'ufficio competente, per ciascun incaricato, l'abilitazione ad accedere al dossier su cui lo stesso è legittimato ad operare, indicando l'ambito delle operazioni consentite. Analogamente, qualora l'incaricato non debba più accedere al dossier – ad esempio per cambio mansione, per trasferimento o per pensionamento - deve essere comunicata la revoca della abilitazione.

b)Altre modalità di accesso ai dati

Pur essendo il modello precedente sufficientemente articolato per coprire un'ampia casistica di situazioni, non è tuttavia possibile prevedere tutte le fattispecie nelle quali i professionisti possano avere necessità, per fini di cura, di accedere alle informazioni cliniche del paziente talora anche a caso non chiuso; si deve pertanto prevedere una modalità di accesso ulteriore che registri **almeno** le seguenti informazioni:

- l'operatore che ha chiesto l'accesso al dossier;
- l'identificativo del paziente del quale si stanno per consultare i precedenti;
- la motivazione per la quale si chiede l'accesso, da individuare tra le seguenti:
  - completamento del percorso diagnostico - terapeutico su un paziente non più in carico (es. paziente dimesso, ma arriva l'istologico oltre il limite temporale prestabilito che determina la chiusura del caso);
  - cura di un paziente per il quale si rende necessario il confronto e la rivalutazione di un caso analogo precedentemente trattato;
  - percorso trapianti;
  - necessità di informazioni sanitarie per fini di cura non altrimenti gestibili informaticamente (es. al medico perviene richiesta di consulenza in formato cartaceo).

Periodicamente l'Azienda provvede ad effettuare controlli in merito alla appropriatezza di questi accessi, come meglio documentato nel prosieguo.

Casistiche particolari e casi di esclusione

Per quanto attiene al conferimento al dossier dei dati che fanno riferimento a vittime di violenza sessuale o pedofilia, a persone sieropositive, a soggetti che fanno uso di sostanze stupefacenti, di sostanze psicotrope o alcool, alle donne che si sottopongono a IVG o che partoriscono in anonimato, ai servizi offerti dai consultori familiari, si rimanda alle scelte specifiche delle singole aziende, che dovranno comunque essere adottate nel rispetto delle disposizioni normative a tutela dell'anonimato, secondo quanto previsto dalle citate Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario - 16 luglio 2009.

Il trattamento di dati personali effettuati attraverso il dossier, perseguendo esclusivamente fini di prevenzione, diagnosi, cura dell'interessato deve essere posto in essere esclusivamente da parte di soggetti operanti in ambito sanitario, con l'esclusione di periti, compagnie di assicurazione, datori di lavoro, associazioni o organizzazioni specifiche e organismi amministrativi anche operanti in ambito sanitario. Analogamente l'accesso è precluso al personale medico nell'esercizio di attività medico legali volte all'accertamento di idoneità o status.

Gestione del consenso

a) Informativa e raccolta del consenso

È necessario che ogni azienda sanitaria dia notizia all'utenza in merito al dossier mediante idonea informativa, di cui a titolo esemplificativo si propone una bozza in appendice. Si lascia alle singole aziende la scelta delle modalità di diffusione ritenute più opportune.

È necessario che le aziende gestiscano **almeno** i seguenti livelli di consenso:

- consenso base al trattamento dei dati;
- consenso preliminare alla costituzione del dossier sanitario;
- consenso ad inserire nel dossier sanitario informazioni precedenti alla sua costituzione.

Il consenso base è il consenso al trattamento dei dati ai fini di cura che il paziente fornisce all'azienda sanitaria e viene raccolto *una tantum*.

Nel caso l'azienda gestisca un dossier è necessario raccogliere il consenso preventivamente alla sua costituzione e rendere il dossier inaccessibile nel momento in cui il paziente revochi il consenso (si veda a questo proposito il paragrafo relativo ai dinieghi).

I consensi possono essere acquisiti informaticamente mediante annotazione e il programma informatico dovrà indicare, oltre nautralmente ai dati anagrafici dell'interessato, se questi rilascia il consenso per se stesso ovvero in qualità di genitore, tutore o amministratore di sostegno

b)Gestione del diniego

Ai tre consensi sopra delineati:

- consenso base al trattamento dei dati;
- consenso preliminare alla costituzione del dossier sanitario;
- consenso ad inserire nel dossier sanitario informazioni precedenti alla sua costituzione

possono corrispondere **tre distinti dinieghi**:

1) diniego al trattamento base dei dati

non viene preso in considerazione nelle presenti Linee di indirizzo, in quanto le decisioni in ordine a tale fattispecie rimangono in capo alla singola azienda (anonimato completo ovvero non erogazione della prestazione sanitaria se non in caso di urgenza).

2) diniego alla costituzione del dossier sanitario

a fronte del diniego sarà possibile:

non costituire il dossier;

qualora il dossier sia lo strumento per la riconsegna dei referti, occorrerà rispettare la volontà del cittadino impedendo ai sanitari di avere accesso ad informazioni diverse da quelle direttamente richieste;

qualora non sia possibile applicare la misura 2) occorrerà gestire la volontà dell'interessato attraverso l'anonimizzazione.

3) diniego ad inserire nel dossier sanitario costituito informazioni precedenti alla sua costituzione
nel caso il paziente abbia dato il consenso alla costituzione del dossier, ma non alla accessibilità ai dati pregressi alla costituzione stessa, il dossier, all'apertura, sarà vuoto e l'aggiunta dei dati sanitari comincerà da quel momento in avanti.

Per le ipotesi di cui ai punti 2) e 3) è opportuno che gli operatori sanitari siano in grado di esplicitare al paziente, anche oralmente e con linguaggio chiaro, che il diniego del consenso potrebbe comportare rischi per la sua salute, in quanto, non potendo accedere ai suoi precedenti sanitari, gli operatori potrebbero non venire a conoscenza di tutte le informazioni necessarie per formulare la migliore strategia diagnostica o di cura e le relative conseguenze da un punto di vista clinico.
Naturalmente analoga comunicazione è già prevista nell'informativa allegata in bozza, conformemente a quanto dettato dal Provvedimento Generale dell'Autorità Garante.

E' inoltre necessario che le aziende gestiscano l'oscuramento e/o l'anonimizzazione del singolo episodio.
L'oscuramento, su alcuni sistemi, sarà ottenuto attraverso il meccanismo della anonimizzazione. Ad esempio, la richiesta di oscuramento di un ricovero pregresso da parte di un paziente potrà essere esaudita spostando il ricovero su di un identificativo anonimo.
Si rimette alle singole aziende la disciplina delle modalità di oscuramento/anonimizzazione/oscuramento dell'oscuramento.

Controlli
Tutti gli accessi al dossier devono essere tracciati. Il servizio aziendale preposto deve effettuare verifiche mirate sugli accessi, sia su richiesta delle direzioni aziendali, sia periodicamente a campione, secondo le determinazioni delle singole aziende.

Qualora l'istruttoria preliminare relativa ai suindicati accessi evidenziasse anomalie, il servizio preposto effettuerà un'analisi più dettagliata. In caso di effettivo riscontro delle stesse, il servizio preposto provvederà a segnalare tali casistiche al responsabile della U.O. o articolazione organizzativa cui afferisce il dipendente che ha effettuato gli accessi esaminati.

Rimane comunque a carico del suddetto responsabile di U.O. comunicare la situazione anomala all'ufficio procedimenti disciplinari, valutando contestualmente il possibile inoltro di denuncia all'autorità giudiziaria, in caso di reati perseguibili d'ufficio, sentiti gli uffici competenti.

Casi d'uso esemplificativi
Di seguito vengono illustrati a titolo esemplificativo, ma non esaustivo, due possibili percorsi di cura nei quali applicare le regole illustrate nelle presenti Linee di indirizzo, nel caso in cui il paziente abbia prestato il suo consenso alla costituzione del dossier e all'inserimento di dati sanitari precedenti alla costituzione.

Ambito di ricovero
Si consideri il seguente tipico percorso di cura chirurgico:
- un paziente viene posto in lista d'attesa per ricovero da uno specialista;
- il paziente – in ambito di prericovero – esegue una serie di analisi ed indagini diagnostiche propedeutiche al ricovero;
- il paziente viene ricoverato per intervento chirurgico in chirurgia;
- il paziente viene operato;

- il paziente transita per qualche giorno dopo l'intervento in una terapia intensiva;
- il paziente ritorna in chirurgia;
- la notte successiva al suo ritorno in chirurgia ha un problema che richiede la consultazione del medico di guardia;
- il giorno successivo viene chiesta una consulenza cardiologica;
- qualche giorno dopo il paziente viene dimesso dal reparto;
- il paziente viene visto ambulatorialmente in postricovero per la rimozione di punti.

Considerazioni analoghe potrebbero essere fatte per percorsi di cura non chirurgici o programmati.

Applicando le regole delle presenti Linee di indirizzo risulta che:

- lo specialista che visita il paziente e lo pone in lista d'attesa ha accessibilità all'intera storia clinica del paziente – aggiornata a quel momento - in quanto nel momento della visita ha in carico il paziente;
- l'équipe di medici del reparto nel quale viene ricoverato ha accessibilità completa alla intera storia clinica – aggiornata a quel momento - in quanto ha in carico il paziente;
- anche il medico di guardia e i consulenti che visitano il paziente mentre è in reparto debbono avere accesso alla intera storia clinica – aggiornata a quel momento;
- gli specialisti ed eventualmente coloro che operano nelle grandi diagnostiche e che hanno in carico il paziente in prericovero e postricovero debbono avere la possibilità di accedere alla storia clinica del paziente – aggiornata a quel momento - mentre hanno il paziente in carico;
- tutti i professionisti sopra citati, una volta che non abbiano più in carico il paziente, non potranno più avere accesso ad aggiornamenti sullo stato di salute del paziente, né alla sua storia clinica;
- nessun professionista potrà avere accesso ai dati di salute del paziente per accessi per i quali non sia stato coinvolto e per i quali non abbia in carico il paziente.

Quindi, tutti i professionisti che hanno in carico un certo paziente possono vedere tutto di quel paziente; a contatto chiuso, completate le diverse pratiche – SDO o altro - non sarà più possibile accedere alla storia clinica del paziente. AD ESEMPIO: nel caso sopra citato del paziente che viene ricoverato in chirurgia e successivamente in cardiologia, ai chirurghi – dopo un certo periodo convenuto dalla dimissione – non sarà più possibile accedere alla storia clinica del paziente, mentre sarà sempre possibile accedere ai dati di cartella a suo tempo da loro stessi redatti.

Ambito ambulatoriale

Si consideri il seguente caso d'uso:

- il paziente viene visto da uno specialista ambulatoriale nell'ambito di una visita programmata.

Applicando le regole della presente linea guida risulta che:

- lo specialista che visita il paziente ha accessibilità all'intera storia clinica del paziente – aggiornata a quel momento - in quanto con la visita lo prende in carico.

Quindi, lo specialista può vedere tutto di quel paziente durante la visita; ma a contatto chiuso, trascorso un certo periodo, non sarà più possibile accedere alla storia clinica del paziente, mentre sarà sempre possibile accedere ai referti ambulatoriali redatti per quel paziente, all'interno della équipe.

Nome documento: P0601

Oggetto: Reperibilità Servizio Risorse Informatiche e Telematiche-1.doc

Dala ultima modifica: 31/03/2015

Servizio Risorse Informatiche e Telematiche

Regolamentazione del servizio di Reperibilità Sistemistica e applicativa erogato dal Servizio Risorse Informatiche e Telematiche dell'Azienda USL di Parma.

Indice generale

Premessa

Il presente documento ha lo scopo di illustrare le caratteristiche di funzionamento del servizio di Reperibilità Sistemistica e applicativa (pronta disponibilità) erogato dal Servizio Risorse Informatiche e Telematiche dell'Azienda USL di Parma.

Il servizio di Reperibilità Sistemistica e applicativa è svolto su base volontaria ed è regolamentato dal presente documento, redatto dal Direttore del Servizio RIT in collaborazione con il Referente Operativo del servizio di reperibilità.

Articolo 1 – Finalità e campo d'applicazione

La presente regolamentazione disciplina le **modalità di attuazione** del servizio di pronta disponibilità da parte del personale tecnico del Servizio Risorse Informatiche e Telematiche dell'Azienda USL di Parma.

Il Servizio di Pronta Disponibilità (PD) è previsto esclusivamente per i settori di attività per i quali è necessario assicurare la continuità dei servizi, compatibilmente con le risorse umane dipendenti dell'Azienda e in forze al Servizio RIT.

Il Servizio di PD ha lo scopo di assicurare **interventi urgenti ed inderogabili, da remoto o on-site**, nelle seguenti circostanze:

- durante le ore di chiusura delle strutture aziendali, in caso di insorgenza di una emergenza, in modo da garantire la presenza di una persona strutturata autorizzata a prendere decisioni;

- durante le ore notturne, prefestive e festive per garantire una maggiore continuità nell' assistenza informatica e infrastrutturale a processi aziendali ritenuti critici.

Il Servizio di PD è applicato ai presidi ospedalieri ed ai presidi territoriali che erogano prestazioni al di fuori normale orario di lavoro (*) su postazioni e/o applicativi resi disponibili dall'Azienda USL.

La pronta disponibilità è finalizzata a garantire:

- la continuità di funzionamento e l'adeguata disponibilità dei servizi a fronte di esigenze/eventi imprevedibili;
- un pronto espletamento delle improvvise necessità dell'Azienda non preventivamente programmabili e non rientranti nella ordinaria e straordinaria manutenzione;

Sono escluse dal servizio di pronta disponibilità tutte le attività cui l'Azienda può adempiere con il ricorso ad una adeguata programmazione dei servizi, anche mediante forme di flessibilità nell'articolazione dell'orario di lavoro, nel rispetto degli accordi specifici in materia.

Articolo 2 – Ruolo Referente operativo della reperibilità

Il Referente del servizio di reperibilità deve occuparsi della gestione dei turni e dell'adesione delle modalità di intervento e di azione al Documento suddetto.

Il ruolo del Referente Operativo dovrà essere quello di interagire fortemente con i Coordinatori dell'Area Tecnologica e degli Ambiti Applicativi, al fine di garantire il flusso e lo scambio delle informazioni, l'attuazione della formazione e l'utilizzo di appositi sistemi di gestione della documentazione a supporto delle attività previste dai servizi e di tracciamento delle problematiche segnalate, aperte e concluse.

Il Referente Operativo dovrà altresì avere e trasmettere un forte senso di collaborazione e disponibilità verso gli altri Servizi aziendali, verso i referenti informatici dell'Azienda ospedaliera, nei confronti dei fornitori esterni, della Regione e degli Enti di emanazione regionale.

Ha il compito di effettuare il monitoraggio e l'audit sulla presenza e sulla completezza della documentazione tecnica a supporto Servizi di reperibilità

Tale attività deve avvenire in collaborazione con tutti i Coordinatori, e consiste nella raccolta e nella verifica della documentazione necessaria al corretto espletamento di tutte le procedure di supporto agli utenti e di continuità operativa.

Articolo 3 – Tipi più comuni di intervento

Le emergenze più comuni a cui deve far fronte il servizio di pronta disponibilità sono essenzialmente:

- problematiche informatiche sull'applicativo di Pronto Soccorso;
- problematiche informatiche sull'applicativo di gestione ricoveri ADT
- problematiche informatiche sulle integrazioni da Anagrafica e ADT verso gli altri sistemi
- problematiche informatiche sul gestionale di radiologia;
- problematiche informatiche sul gestionale di laboratorio;
- problematiche informatiche sul gestionale di stampa delle etichette per prelievi;
- problematiche informatiche sul gestionale CUP;
- segnalazione di guasti e danneggiamenti a sistemi ed impianti tecnologici (es. rete locale, rete geografica, apparati attivi e passivi di rete)

Sono esclusi:

- gli interventi di assistenza e manutenzione, sia ordinaria che straordinaria, di materiale hardware riguardante stampanti, PC, mouse sulla postazione dell'utente
- la risoluzione di blocchi dovuti a malfunzionamenti di programmi di utilità (Libre Office, Office, Acrobat, etc etc) o al loro cattivo utilizzo;
- l'assistenza su applicativi Regionali e/o su applicazioni di vario genere non in carico al Servizio RIT

Articolo 4 – Modalità di svolgimento del servizio di pronta disponibilità

L'addetto in servizio di pronta disponibilità risponde al numero di telefono 334.6536055.

Il servizio di pronta disponibilità può essere attivato dagli operatori della Centrale Operativa o dal centralino di Fidenza, che troveranno sulla intranet, nell'area dedicata, il nominativo e il numero esatto del tecnico RIT reperibile.

Il servizio di pronta disponibilità si espleta durante le ore o le giornate eccedenti l'orario ordinario di lavoro, sulla base del calendario di turnazione annualmente stabilito, con un turno settimanale da lunedì a lunedì. Il servizio di pronta disponibilità è attivo nelle seguenti fasce orarie:

1. giorni feriali: dalle ore 17.00 alle ore 7.30 del giorno successivo;
2. sabati e giorni festivi: dalle ore 7.30 alle ore 7.30 del giorno successivo.

Il Reperibile per raggiungere gli immobili dell'Azienda negli orari di pronta disponibilità, a discrezione utilizzerà mezzi propri oppure mezzi aziendali messi a disposizione dall'azienda in sede centrale; tale utilizzo si intende implicitamente approvato dal Direttore del Servizio RIT attraverso l'adozione aziendale del presente documento. Essendo il personale reperibile "in servizio" dal momento della chiamata, scatta per l'operatore oltre che per l'automezzo la tutela tramite le coperture assicurative Aziendali.

Gli Addetti redigeranno in caso di attivazione, compilando le maschere dell'apposito software predisposto dal SRIT, un rapporto sulle attività svolte. Detto software rilascerà il listato per l'inserimento manuale delle timbrature previa validazione delle stesse da parte del Responsabile del RIT.

Articolo 5 – Compiti degli addetti al servizio di reperibilità.

Il Reperibile, durante il periodo di pronta disponibilità, deve mettersi sempre nella condizione di poter ricevere le chiamate di servizio; in caso di indisponibilità, per malattia o grave impedimento, va data immediata segnalazione al Responsabile del Servizio, che provvede tempestivamente alla sostituzione.

In caso di chiamata, il Reperibile valuterà,in base alle linee guida dell'allegato tecnico e sulla base della propria esperienza professionale, se ritiene necessario recarsi sul posto ovvero se può essere sufficiente impartire indicazioni telefoniche al personale.

Il Reperibile è autorizzato a coinvolgere, secondo le esigenze, a coinvolgere a sua discrezione soggetti esterni (es. fornitori secondo i vincoli espressi nei contratti di manutenzione (*)), Reperibile Servizio Attività Tecniche, Reperibilità sistemistica RIT, Direttori dei Servizi RIT e SAT, Direttore del Dipartimento tecnico, nel caso in cui un intervento non tempestivo possa recare un blocco sostanziale alle attività erogate dall'Azienda;

Art. 6 - Responsabilità delle persone in pronta disponibilità

Per l'ottimale svolgimento del servizio occorre tenere presente i due distinti compiti e responsabilità dell'amministrazione che organizza il servizio di reperibilità e degli addetti al servizio stesso.

L'Amministrazione, attraverso la reperibilità delegata ai funzionari opportunamente individuati, deve assicurare che tutte le condizioni previste siano attivate con la massima efficienza sia dal punto di vista normativo che da quello strutturale.

L'addetto al servizio di reperibilità deve, dal canto suo, una volta ricevuta la consegna e fino alla remissione della stessa, tenere quel comportamento serio, oculato, preciso, diligente ed attento che si richiede ad un incaricato di pubblico servizio.

Qualora la problematica segnalata non rientrasse nelle casistiche descritte, il reperibile è comunque tenuto a farsi carico della problematica e a gestirla in modo da dare una risposta a chi ha segnalato il problema.

Per ogni tipo di segnalazione ricevuta il Reperibile è tenuto alla presa in carico della segnalazione qualunque essa sia; potrà valutare se smistare personalmente la richiesta ai colleghi o spiegare al richiedente come o a chi rivolgersi per risolvere la problematica, sulla base della valutazione di criticità del caso segnalato.

Una volta rientrato in servizio il Reperibile dovrà informare il Referente della reperibilità, della situazione “non convenzionale” verificatasi durante il turno per consentirgli di valutare se il problema segnalato e gestito estemporaneamente andrà o meno inserito all’interno dei percorsi formalizzati di reperibilità. A tal fine l'operatore che ha gestito il Caso dovrà farsi carico di supportare il Referente nella produzione di adeguata documentazione necessaria alla risoluzione futura del problema e ai percorsi formativi della reperibilità.

Art. 7 - Formazione

Ogni “reperibile” viene avviato al servizio attraverso un percorso di formazione programmato.

Il Responsabile del servizio inoltre favorisce l'aggiornamento professionale continuo del personale reperibile e l'addestramento necessario ad effettuare in modo idoneo il servizio di reperibilità a seguito delle progressive modifiche agli impianti, alle strutture, agli applicativi e all'organizzazione.

(*.).Vedi allegato tecnico dettagliato

Nome documento: P0602

Oggetto: Allegato tecnico.doc

Dala ultima modifica: 31/03/2015

Servizio Risorse Informatiche e Telematiche

Allegato tecnico del servizio di pronta disponibilità erogato dal Servizio Risorse Informatiche e Telematiche dell'Azienda USL di Parma.

Premessa

Il presente documento ha lo scopo di illustrare gli aspetti operativi di dettaglio del funzionamento del servizio di pronta disponibilità erogato dal Servizio Risorse Informatiche e Telematiche dell'Azienda USL di Parma.

Dotazione Reperibile

- Badge personale aziendale
- Chiavi e codici delle porte di accesso agli uffici
- Cellulare di Servizio con caricabatterie (sono disponibili due cellulari all'interno della cassaforte del servizio)
- Chiave e codice di accesso alla sala server (viene passata di volta in volta da un reperibile all'altro)
- Chiavi auto aziendali helpdesk
- Portatile personale aziendale
- Certificato VPN (ogni tecnico del servizio ne possiede uno personale)
- Chiavetta USB Tim aziendale (a disposizione di tutti i tecnici)
- Documentazione On-line sulla wikirit al link http://wikirit.ausl.pr.it/index.php/Gestione_della_Reperibilit%C3%A0

Modalità erogazione delle attività

Ogni settimana è reperibile un tecnico per la parte sistemistica e uno per la parte applicativa.

Il "reperibile" prima dell'entrata in servizio deve obbligatoriamente accedere al software di reperibilità presente sulla intranet aziendale al link http://lamp.ausl.pr.it/intra/reperibilita/

utilizzando le proprie credenziali LDAP per selezionare il numero telefonico del cellulare che si è scelto di utilizzare. I numeri verdi sono per i reperibili applicativi e i rossi per i reperibili sistemistici.

Le segnalazioni di malfunzionamento informatico di qualsiasi tipo arrivano solamente al reperibile applicativo che poi valuterà se attivare o meno gli altri colleghi reperibili (RETE, SAT), eventuali fornitori, i Direttori dei Servizi SAT e RIT o il Direttore del Dipartimento Tecnico.

Lo svolgimento dell'assistenza prevede la presa in carico della chiamata da parte del Reperibile, che analizzerà la problematica segnalata e valuterà le modalità operative da seguire per la risoluzione del problema, redigerà la successiva verbalizzazione all'interno del software e procederà a compilare i moduli cartacei per farsi riconoscere la parte economica delle attività svolte (ore ed eventuali km per spostamenti in sedi diverse dall'Ugolino).

Per agevolare e schematizzare sinteticamente le attività il reperibile dovrà seguire lo schema riportato sotto:

2. PRESA IN CARICO DELLA SEGNALAZIONE

La prima cosa che il reperibile deve fare in fase di presa in carico è cercare di identificare il tipo di problematica che ha scaturito la segnalazione seguendo la manualistica a disposizione al link:

http://wikirit.ausl.pr.it/index.php/Gestione_della_Reperibilit%C3%A0

cercando di collocarla all'interno delle 8 casistiche riportate sotto:

3. PROBLEMA APPLICATIVO
4. PROBLEMA INFRASTRUTTURALE (rete LAN,WAN, timbratori)
5. PROBLEMA DI' INTEGRAZIONE TRA APPLICATIVI
6. PROBLEMA SUI CLIENT
7. PROBLEMI AFFERENTI AL MODULO LDAP AZIENDALE
8. PROBLEMA SU DISPOSITIVO ELETTROMEDICALE
9. ALLARME ANTI INTRUSIONE SERVIZIO RIT
10. PROBLEMA SALA SERVER

Una volta inserita la segnalazione all'interno di uno di questi gruppi si passera alla fase 2

1)ANALISI DELLA PROBLEMATICA

Se la problematica ricade nella casistica dei *PROBLEMI APPLICATIVI* il reperibile applicativo, aiutandosi con la propria preparazione/esperienza professionale supporterà l'operatore nei passaggi applicativi collegandosi alla postazione da remoto per verificare se il problema è:

- di un errato/cattivo utilizzo dell'applicativo

- è presente un problema legato al normale funzionamento dell'applicativo stesso

-richiesta di modifiche di funzionalità del software

Nel primo caso si proverà a guidare l'operatore e portare a termine l'attività

Nel secondo caso il reperibile aiutandosi con il modulo fornitori aiuterà il collega a trovare (se presente) il riferimento della ditta che fa supporto al software e gli suggerirà di contattare direttamente la ditta per velocizzare la risoluzione del problema,mettendosi a disposizione per eventuali chiarimenti, nel caso il software non fosse coperto da assistenza H24 si farà carico di segnalare tempestivamente all'area di appartenenza del software la problematica raccolta,spiegando all'operatore che cosa verrà fatto per garantire il ripristino del problema nel minor tempo possibile

Nel terzo caso il reperibile dovrà dare i riferimenti dell'area di competenza al quale fare una eventuale richiesta di modifica.

In ogni caso una volta terminata l'attività il reperibile passerà alla fase 3

Se la problematica ricade nella casistica dei *PROBLEMI INFRASTRUTTURALE* il reperibile applicativo, passerà la chiamata al reperibile sistemistico che procederà all'analisi della problematica avvalendosi della propria esperienza dei manuali e degli strumenti messi a disposizione dall'azienda.

Una volta risolto il problema il reperibile sistemistico dovrà segnalare al reperibile applicativo l'avvenuta risoluzione del problema e dovrà poi passare alla fase 3.

Il reperibile applicativo avrà poi il compito di verificare con l'operatore che ha effettuato la segnalazione il corretto ripristino delle normali attività per poi passare alla fase 3.

Se la problematica ricade nella casistica dei *PROBLEMI DI' INTEGRAZIONE TRA APPLICATIVI* il reperibile applicativo, aiutandosi con la propria preparazione/esperienza professionale e della manualistica a disposizione procederà al tentativo di risoluzione della problematica.

In caso di esito negativo si dovrà segnalare all'operatore della segnalazione l'impossibilità di immediata risoluzione del problema e si suggerirà di procedere con strumenti d'emergenza in attesa della risoluzione, inoltre si farà carico di segnalare tempestivamente all'area di appartenenza, al referente della reperibilità e al responsabile di servizio la problematica raccolta,e l'impossibilità di risolvere la problematica in reperibilità,spiegando all'operatore che cosa verrà fatto per garantire il ripristino del problema nel minor tempo possibile.

In ogni caso una volta terminata l'attività il reperibile passerà alla fase 3

Se la problematica ricade nella casistica dei *PROBLEMA SUI CLIENT* il reperibile applicativo,dovrà capire se l'attività che deve svolgere l'operatore è vincolata tassativamente alla funzionalità del client bloccato.

Nel caso che il client fosse l'unico adibito a tale attività , quindi bloccante il reperibile applicativo passerà la chiamata al reperibile sistemistico che procederà all'analisi della problematica avvalendosi della propria esperienza dei manuali e degli strumenti messi a disposizione dall'azienda.

Se fosse necessario al ripristino il reperibile sistemistico dovrà recarsi sul posto per procedere alla eventuale sostituzione di componenti o del client stesso.

Una volta risolto il problema il reperibile sistemistico dovrà segnalare al reperibile applicativo l'avvenuta risoluzione del problema e dovrà poi passare alla fase 3.

Il reperibile applicativo avrà poi il compito di verificare con l'operatore che ha effettuato la segnalazione il corretto ripristino delle normali attività e si dovrà fare carico di segnalare al responsabile di servizio e al referente della reperibilità del problema raccolto in modo da rendere appena possibile il client in questione "ridondato", cosi da evitare futuri interventi "on-site" per poi passare alla fase 3.

Nel caso che il client non fosse l'unico adibito a tale attività e nelle vicinanze ci fossero postazioni da poter utilizzare per svolgerla sarà compito del reperibile applicativo indicare al collega come poter operare la propria attività sul client funzionante,Inoltre si farà carico di segnalare tempestivamente all'helpdesk la problematica raccolta (che si attiverà aprendo una chiamata appena riprenderanno le normali attività lavorative) spiegando all'operatore che cosa verrà fatto per garantire il ripristino del problema nel minor tempo possibile.

Una volta terminata l'attività il reperibile passerà alla fase 3

Se la problematica ricade nella casistica dei *PROBLEMI AFFERENTI AL MODULO LDAP AZIENDALE* il reperibile applicativo, aiutandosi con la propria preparazione/esperienza professionale e della manualistica a disposizione procederà al tentativo di risoluzione della problematica.

In caso di esito negativo si dovrà segnalare all'operatore della segnalazione l'impossibilità di immediata risoluzione del problema, inoltre si farà carico di segnalare tempestivamente all'area di appartenenza, al referente della reperibilità la problematica raccolta,e l'impossibilità di risolvere la problematica in reperibilità,spiegando all'operatore che cosa verrà fatto per garantire il ripristino del problema nel minor tempo possibile.

Se la problematica ricade nella casistica dei *PROBLEMI SU DISPOSITIVI ELETTROMEDICALI* il reperibile applicativo suggerirà al collega di farsi contattare il reperibile del SAT dal centralino in modo da tracciare la chiamata, mettendosi a disposizione per eventuali chiarimenti, e successivamente procederà ad avvisare il collega del SAT della chiamata arrivata.

Una volta terminata l'attività si passerà alla fase 3

Se la problematica ricade nella casistica della *ALLARME ANTI INTRUSIONE SERVIZIO RIT* la procedura è in carico al SAT/Servizio di sorveglianza ; Il servizio di sorveglianza effettua la verifica del sito e comunica al SAT eventuali irregolarità. Se si riscontrano delle effrazioni reali , il reperibile SAT avvisa immediatamente il reperibile Applicativo. Il disinserimento dell'allarme è affidato alla ditta di sorveglianza che provvederà a ripristinare il regolare funzionamento del dispositivo.

nel caso i colleghi del SAT non dovessero informarci sulla risoluzione del problema sarà compito del reperibile applicativo ricontattarli per poi procedere con le proprie attività .

Una volta terminata l'attività si passerà alla fase 3

Se la problematica ricade nella casistica dei PROBLEMI IN SALA SERVER il reperibile applicativo dovrà verificare se il problema è di **rete interna** alla sala server passerà la chiamata al reperibile sistemistico che procederà all'analisi della problematica avvalendosi della propria esperienza dei manuali e degli strumenti messi a disposizione dall'azienda.

Una volta risolto il problema il reperibile sistemistico dovrà segnalare al reperibile applicativo l'avvenuta risoluzione del problema e dovrà poi passare alla fase 3.

Il reperibile applicativo avrà poi il compito di verificare con l'operatore che ha effettuato la segnalazione il corretto ripristino delle normali attività per poi passare alla fase 3.

Se il problema è la mancanza di **corrente elettrica** il reperibile applicativo , dopo le opportune verifiche attiverà il reperibile del SAT, per il ripristino del guasto inerente la parte elettrica , una volta ripristinato il guasto sarà compito del reperibile applicativo fare le opportune verifiche sui server eventualmente recandosi in loco.

Se il problema è il malfunzionamento **dell'impianto di condizionamento** il reperibile applicativo , dopo le opportune verifiche attiverà il reperibile del SAT per il ripristino del guasto inerente l'impianto di condizionamento, una volta ripristinato il guasto sarà compito del reperibile applicativo fare le opportune verifiche sui server eventualmente recandosi in loco.

Se il problema è un **malfunzionamento sulle macchine** il reperibile applicativo, aiutandosi con la propria preparazione/esperienza professionale e della manualistica a disposizione procederà al tentativo di risoluzione della problematica.

Nel caso ci fossero problemi hardware accertati su una macchina occorre procedere alla apertura di una chiamata alla ditta esterna incaricata alla manutenzione e si procederà ad avvisare via mail il referente dell'area tecnologica, dell'area di competenza della macchina che ha il problema e il capo servizio.

1. CHISURA DELLA SEGNALAZIONE

Al termine di ogni chiamata il tecnico reperibile in ogni caso dovrà rendicontare la propria attività collegandosi al sito http://lamp.ausl.pr.it/intra/reperibilita/ e descrivere in modo esaustivo il tipo di segnalazione ricevuta, l'attività svolta,il tempo impiegato e se la segnalazione è chiusa oppure necessità di ulteriori approfondimenti/attività.

Elenco fornitori

Data Processing

NoemaLife

Elco

Engineering

CUP2000

Philips

Infocert

Dedalus

Lepida

Telecom

HMS

Magdala

Molteni

Dettaglio applicativi in reperibilità

Anagrafica degli Assistiti

ADT

Order entry LIS e RIS

PS

CUP

Laboratorio Analisi

Radiologia

Prescrizione informatizzata dei farmaci di reparto

MPP

Stampa etichette

Integrazioni

Firma digitale di laboratorio e radiologia

Screening mammografico

Sister

Win Simet

Dettaglio strutture in reperibilità

Sede centrale

Ospedale di Vaio

Ospedale S. Maria di Borgotaro

Ospedale di Comunità di San Secondo

Presidi AOSP aziendali

Punti prelievo

Case della Salute:

- Colorno
- Parma Centro
- San Secondo
- Busseto (Claudio Carosino)
- Langhirano
- Collecchio
- Traversetolo
- Monticelli

Felino

Sala Baganza

Medesano

Bedonia

Berceto

Sono in reperibilità anche:

infrastruttura di rete

sala server

Letto, confermato, firmato:

IL DIRETTORE AMMINISTRATIVO
Dott. Marco Chiari

IL DIRETTORE SANITARIO
Dr. Ettore Brianti

IL DIRETTORE GENERALE
Dott.ssa Elena Saccenti

CERTIFICATO DI PUBBLICAZIONE

Il sottoscritto certifica che la deliberazione è stata **affissa all'albo** di questa Azienda Unità Sanitaria Locale **IL GIORNO 28/10/2015** e vi rimarrà in pubblicazione per 15 giorni consecutivi ai sensi e per gli effetti del 5° comma dell'art.37 della L.R.20/12/94 n.50 così come modificato dall'art.12 della L.R.23/12/04 n.29.

La presente deliberazione diventa esecutiva dal primo giorno di pubblicazione, come previsto dalla Legge Regionale sopra indicata.

Lì 28/10/2015 IL FUNZIONARIO

Dott.ssa Maria Cristina Pomi

Per copia conforme all'originale ad uso amministrativo.

IL FUNZIONARIO

Dott.ssa Maria Cristina Pomi

La presente deliberazione pubblicata il _____,**soggetta a controllo** della Giunta Regionale
(Legge 30/12/1991 n. 412 Art. 4 c.8)
Data ricevimento Regione prot. n. _____ del _____
Chiarimenti Regione prot n.. _____ del _____
Richiesta chiarimenti ai servizi/uffici prot. n. _____/_____ del _____
Controdeduzioni Regione _____
Regione annullamento parziale/totale prot. _____ del _____
È divenuta esecutiva in data _____
è stata approvata nella seduta della Giunta Regionale del _____

La presente deliberazione viene trasmessa
· al Collegio Sindacale, ai sensi dell'art. 40, comma 3), della Legge Regionale 20 dicembre 1994, n. 50 il 28/10/2015
· al Consiglio dei Sanitari il
· alla Conferenza dei Sindaci il

ai seguenti uffici/servizi: