Documento Programmatico sulla Sicurezza

Redatto ai sensi dell'articolo 34, comma 1, lettera g) e Allegato B - Disciplinare Tecnico, Regola 19 del Decreto legislativo 30 Giugno 2003 n.196 *"Codice in materia di protezione dei dati personali"*

Anno 2016

Versione n. 1.08 **del: 31 MARZO 2017**

Stato: approvato

Firma del Titolare del trattamento:

1. PREMESSA

Il presente documento viene redatto per adempiere agli obblighi imposti dal Decreto Legislativo 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali" e dall'Allegato B "Disciplinare Tecnico" in materia di misure minime di sicurezza.

1.1. Revisioni e aggiornamento del documento programmatico

Il presente documento redatto, come richiesto dal punto 19 del Disciplinare Tecnico viene redatto dal Titolare e dai Responsabili dei trattamenti dei dati costituisce la base di osservazione e sviluppo per le successive revisioni in relazione agli aggiornamenti secondo quanto disposto dall'art.34 lett. g) e dal punto 19 Allegato B D.Lgs. 196/03. Ove indicato (regola xx.y) viene fatto riferimento alla regola dell'Allegato B D.Lgs. 196/03. Le tabelle con didascalia progressiva numerica (1.1, 2.1 ecc) fanno riferimento a quanto richiesto dal Garante.

1.2. Definizioni

In questo paragrafo sono elencati i termini e le abbreviazioni, di uso comune nell'ambito della sicurezza e della *privacy* e utilizzati nel documento.

Amministratori sistema:	soggetti cui è conferito il compito di sovrintendere alle risorse del sistema operativo (SO) di un calcolatore (mainframe, distribuito, pc...) o di un DBase o di SW di sistema in generale.
Banca di dati (DB):	qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.
Blocco:	conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.
Comunicazione:	il dare conoscenza dei dati personali di uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Credenziali autenticazione:	i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.
Dato anonimo:	dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.
Dato giudiziario:	dato personale idoneo 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.
Dato identificativo:	dato personale che permette l'identificazione diretta dell'interessato.
Dato personale:	Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili direttamente o indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
Dato sensibile:	dato personale idoneo a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
Diffusione:	il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Disciplinare Tecnico:	Documento Programmatico sulla Sicurezza dei dati, previsto dall'articolo 34 del Codice in materia di protezione dei dati personali. Allegato B Decreto Legislativo 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali, recante norme per la determinazione delle
DPS:	Documento Programmatico sulla Sicurezza
Facility Management (FM):	modalità di applicazione delle misure minime di sicurezza ai sensi dell'articolo 33. amministrazione/gestione delle funzionalità. Utilizzo di un computer, di programmi e/o di personale messi a disposizione da un fornitore per un certo periodo di tempo.
Garante:	l'autorità di cui all'articolo 153 D.Lgs. 196/2003
Gruppo:	termine con il quale si indica una holding od un insieme di società di cui una è capogruppo e le altre sussidiarie;
Incaricato:	la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile.
Interessato:	persona fisica, persona giuridica, ente o associazione, cui si riferiscono i dati personali.
Legge:	Decreto Legislativo 30 giugno 2003,n. 196 Codice in materia di protezione dei dati personali.
Misure idonee:	complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza, da determinare anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati ed alle specifiche
Misure minime:	caratteristiche del trattamento, tali da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta.
Outsourcing:	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 3l. indica la delega della gestione di parte/tutte delle attività e infrastrutture ad una società di servizi esterna. Le parti stabiliscono un contratto che definisce il livello di servizio (Service Level Agreement - SLA) richiesto. Il Service Level Agreement (SLA) è un contratto tra un service provider e un cliente, che stabilisce quali servizi verranno erogati e a quale livello (definito secondo parametri misurabili).
Parola chiave:	componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.
Posta elettronica:	messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.
Profilo di autorizzazione:	l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.
Responsabile:	persona fisica, persona giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento dei dati personali ovvero determinati trattamenti individuati nell'atto di nomina;
Reti comunicazione:	i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato.
Servizio di comunicazione:	i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002.
Sistemi	gli apparati elettronici (siano essi personal computer, server, minicomputer, mainframe) utilizzati per il trattamento dei dati.
Sistema di autenticazione:	l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

Sistema di autorizzazione: l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

Strumenti elettronici: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

Titolare: persona fisica, persona giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza; nello specifico il legale rappresentante ASP IIAARR

Trattamento: qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati;

1.3. Struttura organizzativa del gruppo

L'Azienda di Servizi alla Persona, in particolare nella sede amministrativa rappresenta legalmente e gestisce la Casa di Risposo Francesco Pertusati, da Settembre 2012 la RSA S. Croce ed il Centro diurno F. Pertusati, l'Istituto di Riabilitazione S. Margherita, i reparti E e D solventi, l'Hospice ed il Centro Diurno S. Margherita, tutte le strutture ambulatoriali accreditate presso il Sistema Sanitario Regionale Assessorato alla Famiglia e Solidarietà Sociale - Ciclo Diurno e Trattamento Ambulatoriale, nonché quelle accreditate presso l'Assessorato alla Sanità – Ambulatorio di fisiocinesiterapia per esterni e Poliambulatorio di FKT.

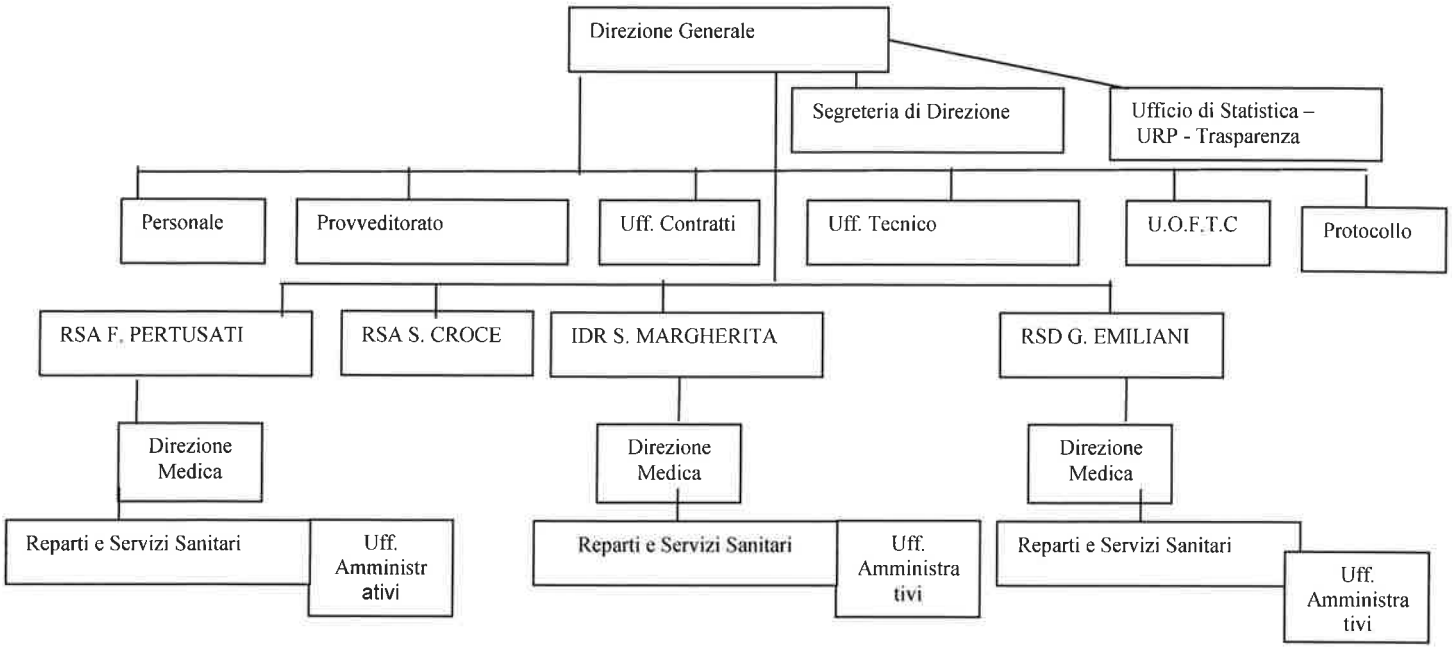
ASP Sede amministrativa e IDR S. Margherita

RSA F. Pertusati
RSD G. Emiliani

La gestione elettronica dei dati e le comunicazioni sono interamente gestite attraverso la adozioni di una rete metropolitana su Protocollo IP. Tale rete collega virtualmente le strutture mediante instradamento attraverso internet di pacchetti TCP/IP e VOIP. Il centro operativo è situato presso l'IDR S. Margherita, ove sono posizionati 4 server. Una macchina con funzione "file server" è temporaneamente adottata presso la RSA F. Pertusati. L'accesso a tale macchina è consentita solo a determinati Host IP

1.4. Struttura organizzativa di ASP IIAARR

La struttura organizzativa di ASP IIAARR è indicata dallo schema seguente:



2.0 STRUTTURA RELATIVA AL TRATTAMENTO DEI DATI PERSONALI

Le attività che competono alle singole funzioni aziendali sono indicate nella tabella seguente:

Finalità perseguita e attività svolta	Categorie di interessati	Ufficio e Responsabile
Protocollazione, registrazione ed Archiviazione di tutte le pratiche trattate dall' ASP	Tutti i soggetti di tutte le categorie che si interfacciano per qualsiasi motivo con l'ASP.	Ufficio Protocollo /Archivio **Scarpa**
Approvazione, smistamento, determinazioni relativamente a tutte le pratiche trattate dall'ASP. Strategia e Management	Tutti i soggetti di tutte le categorie che si interfacciano per qualsiasi motivo con l'ASP.	Direzione Generale e Segreteria **Niutta**
Gestione dati di natura economica e dati anagrafici di fornitori	Aziende ed enti esterni(fornitori)	U.O.F.C **Riccio**
Gestione dati anagrafici per contratti	Aziende ed enti esterni(fornitori)	Contratti/Provveditorato **Noè**
Gestione dati personali e sensibili dei dipendenti	Tutto il personale dipendente	Personale **Rosa**
Gestione dati tecnici	Aziende ed enti esterni(fornitori)	Tecnico **Ghilioni**
Gestione domande e ricovero RSA, IDR, CDI, Ambulatori, debito informativo e quindi Gestione dati personali e sensibili dei dipendenti. Attività connesse con il CUP.	Ospiti e possibili ospiti, tutto il personale dipendente e non	Statistica_Relazioni con il Pubblico - Trasparenza **Magnani**
Gestione dati sensibili di natura medica	Ospiti e dipendenti	Direzione Medica RSA **Segù**
Gestione dati sensibili di natura medica	Ospiti e dipendenti	Direzione Medica RSD **Segù**
Gestione dati per rette	Ospiti	Economato ASP **Pezza,** Russino, Baccalini, Filippi
Gestione dati sensibili di natura medica	Ospiti e dipendenti	Direzione Medica IDR **Rollone**

2.1 Organizzazione Trattamento

Gestione pratiche inerenti al ricovero Gestione domande e ricovero IDR, CDI, Ambulatori, debito informativo	Ospiti e possibili ospiti	Spedalità SM Rollone
Centralino S. Margherita	Ospiti	Certificati di morte ,Elenco ospiti ricoverati
Centralino F. Pertusati	Ospiti	Certificati di morte ,Elenco ospiti ricoverati
Gestione dati salute e stato cognitivo utenti	Ospiti RSD	Animazione/educazione **Cavallotti,**
Gestione dati medici	Ospiti	**Attività sanitaria specifica**
Gestione dati sui farmaci	Reparti/Ospiti	Farmacia Bellotti

Finalità perseguita o attività svolta	Categorie di interessati	Descrizione
Gestione dati di Geriatria, Endocrinologia e Diabetologia	Ospiti	**Attività sanitaria specifica**
Gestione prenotazioni ambulatoriali	Dati pazienti per le prenotazioni delle prenotazioni	**Prenotazioni ambulatoriali**
Gestione di dati inerenti ai parametri bioumorali	Utenti esterni, ospiti, dipendenti	**Esecuzione esami di laboratorio**
Gestione dati Attività di palestra	Ospiti	**Serv. di Riabilitazione ASP Mazzacane**
Gestione pratiche inerenti al ricovero Gestione domande e ricovero IDR, CDI, Ambulatori, debito informativo	Ospiti e possibili ospiti	Spedalità SM **Rollone**
Centralino S. Margherita	Ospiti	Certificati di morte
Centralino F. Pertusati	Ospiti	Elenco ospiti ricoverati
Gestione dati salute e stato cognitivo utenti	Ospiti RSD	Animazione/educazione **Cavallotti,**
Gestione dati medici	Ospiti	**Attività sanitaria specifica**
Gestione dati sui farmaci	Reparti/Ospiti	**Farmacia Bellotti**

Ruolo a fini privacy	Soggetto	Trattamenti
Titolare	ASP	Tutti
Responsabili esterni	Biosistemi	Gestione ospiti e pazienti Contabilità
	Dedagroup	Archiviazione, Protocollazione, gestione del personale
	CLT; ATC Service; P. Marino; Lombardia Informatica S.p.A; Lombardia Gestione S.p.A; Almaviva S.p.A; Milano Bit Media S.p.A. Capgemini Italia S.p.A. ;Hi Tech S.p.A; Insiel Mercato S.p.A; Lutech S.p.A. ; Santer Reply S.p.A. ; Milano Sopra Group ; Telecom Italia Omnicom	Servizi gestione dati e telefonia Manutenzione Hardware Amministrazione di sistema Vedere allegati da 1 a 7 Servizi CUP Accettazione
Incaricati	Tutti i dipendenti, i collaboratori ed i consulenti dell'azienda	

Tutte le disposizioni interne e gli adempimenti prescritti ai fini del D.Lgs. 196/03 sono stati affidati in accordo con quanto indicato nella tabella precedente. In particolare gli incaricati sono stati nominati tramite documentata preposizione al trattamento.

2.2 Sistema informatico

Il sistema EDP di ASP utilizza macchine PC standard, con base operativa Microsoft Windows (marchio registrato dal proprietario). La comunicazione delle informazioni fra le sedi su area metropolitana è attuata mediante protocolli internet standard, sia con servizi di tipo "application" che di tipo "file", come meglio precisato nei paragrafi successivi.

2.2.1 Piattaforma tecnologica

Le piattaforme che compongono il sistema informativo di ASP sono:

2.2.2 Organizzazione rete interna VPN:

Presso le tre sedi sono installate reti locali Ethernet standard, fra loro interconnesse mediante tunnel IP realizzati su linee DSL affidate a router/firewall Netasq (Marchio registrato dal proprietario). I firewall sono configurati in modo da limitare gli accessi agli aventi diritto. L'architettura della rete è mista a priorità client/server, configurazione a stella, Il centro stella è posto in idoneo locale chiuso e climatizzato presso l'IDR S. Margherita.

2.2.3 Distribuzione dei servizi

I dati sono centralizzati su macchine server:
Presso l'IDR S. Margherita, in sala server accessibile mediante chiave, sono installati:

n. 1 server (IP x..103) per dati utenti uffici centrali, base Windows server, gestito unicamente dall'amministratore di sistema

n. 1 server (IP x..100) per contabilità, base Windows server, affidato in gestione a Biosistemi s.r.l.

n. 1 server (IP x..108) per basi dati SW "biosistemi" e programmi sanitari, base Windows server, affidato a Biosistemi s.r.l., Omnicom s.r.l.

n. 1 server (IP x..97) per gestione personale dipendente e protocollo, base Windows server, affidato a Sintecop s.r.l./Dedagroup srl

n. 1 server (IP x..105) per la gestione posta elettronica, base linux, affidato a ATC s.r.l.. nota: i relativi backup sono su disco di rete gestito direttamente dalla società fornitrice; l'amministratore di sistema non ha accesso a questo server.

Gli accessi sono regolamentati mediante verifica delle credenziali degli utenti.

Sono inoltre installati con criterio temporaneo i seguenti:
n. 1 server per gestione flussi utenza residenziale e ambulatoriale, sito in RSA saletta server, autenticazione mediante riconoscimento IP sorgente + accessi ai software mediante riconoscimento credenziali, su base windows XP

n. 1 server per programma pensioni, in sito in sala server dell'Istituto di Riabilitazione Santa Margherita, autenticazione livello software su base sql, su base windows xp professional

2.2.4. Dotazione dei sistemi

I sistemi server che sono sotto la diretta responsabilità di gestione dell'IT di ASP sono dislocati presso la sede dell'IDR e della RSA sono riportati nella tabella seguente.

Servizio (Tecnologia)	IDR S. Margherita	RSA F. Pertusati
Autenticazione (Windows)	X	X
Posta elettronica	X	
Servizi di protocollazione	X	
Navigazione su Internet	X	X
Condivisione file e stampanti (Windows)	X	X
Portale Intranet (Windows)	X	
Gestione del personale	X	
Gestione utenza	X	X
Sistema Gestionale Contabile (Onda)	X	
Salvataggio dei dati	X	X

2.2.5. PC Desktop

La maggior parte dei PC desktop delle sedi ASP IIAARR utilizzano sistema operativo Windows 7 o superiore. I PC Desktop dei reparti, dei magazzini, e delle zone che non hanno elevata produzione a carattere amministrativo, utilizzano Open Office. Quindi la dotazione del software applicativo prevede:

Dotazione standard PC

Ambiente	Prodotto software
Sistema operativo	Windows 7 / XP Professional
Produttività individuale (Office)	Microsoft Office 2000/2003 /Open Office
Browser Internet	Microsoft Internet Explorer
Posta elettronica	Microsoft Outlook Office e MS Outlook Express
Antivirus	NOD 32
Compressore dati	Winzip
Reader di documenti	Acrobat Reader

2.2.6. Posta elettronica

Il servizio di posta elettronica è centralizzato presso l'IDR S. Margherita. Alla data di redazione del presente documento sono in gestione circa 70 caselle postali, che corrispondono ad altrettante utenze ed in accordo con le specifiche credenziali di autenticazione.

2.2.7. Accesso alla rete Internet

L'accesso alla rete Internet in termini di navigazione, download di file *e/o* documenti, utilizzo di protocolli, ecc., è veicolato attraverso Telecom Italia.

2.2.8. Accesso alla rete intranet

Non sono censite le password degli utenti. Queste possono essere impostate con l'ausilio dell'Amministratore di rete, che NON le annota. In caso di smarrimento password questa non è recuperabile e deve essere riassegnata. Le regole password sono come da norme vigenti: minimo 8 caratteri, compresenza di una maiuscola, una minuscola ed un carattere alfanumerico. Le password, su richiesta dell'utente o per esigenze rilevate dall'amministratore di rete, possono essere rinnovate prima della scadenza.

2.2.9. Accessi remoti

L'accesso remoto prevede la autenticazione di rete predisposta dal S.O. Windows server.

2.2.10. Disaster Recovery

Il Disaster recovery è affidato a tecniche avanzate di recupero dati nelle competenze dell'amministratore di sistema, unitamente alle copie di sicurezza periodiche. Queste sono "in chiaro", e contengono quindi dati immediatamente fruibili. Le copie periodiche sono effettuate manualmente su dischi esterni ai server, previste con cadenza settimanale, e su supporti rimovibili e conservati in locale separato, previste con cadenza mensile.

2.3 Ambiente applicativo rete

L'ambiente è Microsoft Windows Server, supporto rete Ethernet cat. 5e/6, standard file systems NTFS.
I server sono configurati per immagazzinamento dati con protezione RAID 5, eccetto il server pensioni (no raid) e quello di posta elettronica (backup su raid 2). Al momento della stesura del presente documento il server x.100 necessita di manutenzione, operando in stato degradato dei dischi, e se ne prevede la sostituzione funzionale con nuovo server, già in dotazione.

2.4 Applicazioni di core business

I dati sono centralizzati su macchine server:

per dati utenti uffici centrali e basi dati SW "biosistemi" per gestione personale dipendente nonché programma "Onda" per contabilità, server sito in sala server dell'Istituto di Riabilitazione Santa Margherita, autenticazione livello utente + accessi ai software, windows server 2003 **e Microsoft Sql Server.**

per SW "Folium e Civilia" (programma protocollo) e SW SIESA "biosistemi" per gestione flussi utenza residenziale e ambulatoriale, sito in idr sala server,autenticazione livello utente + accessi ai software, windows server 2003
n. 1 server per programma pensioni, sito in sala server dell'Istituto di Riabilitazione Santa Margherita, autenticazione livello software su base sql, windows xp professional;

n. 1 server per la gestione posta elettronica, sito in sala server dell'Istituto di Riabilitazione Santa Margherita, autenticazione livello software, windows server 2003; i relativi backup sono su disco di rete gestito direttamente dalla società fornitrice.

Inoltre vi è un server temporaneo in RSA, area Presidenza, SW SIESA "biosistemi" per gestione flussi ricoveri e prestazioni; accesso livello ip address.

2.5. Sicurezza rete

Tutti gli aspetti connessi alla sicurezza dei dati come:

- firewall sono gestiti dai fornitori ATC Service srl e CLT srl

- antivirus per file, antivirus e antispam, patch management, dal fornitore ATC Service

- Il salvataggio dei dati, amministrazione rete e contrasto danni da virus informatici dall'amministratore di sistema.

- il servizio posta elettronica dal fornitore ATC Service srl

3. RILEVAZIONE DEI TRATTAMENTI DI DATI PERSONALI (REGOLA 19.1)

3.1. Classificazione

I dati trattati da ASP vengono classificati secondo la catalogazione derivante dalle definizioni di legge sottoriportate:

dati personali (D.Lgs. 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali, art. 4, comma l.b): qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati od identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

dati identificativi: (D.Lgs. 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali, art. 4, comma l.c): dato personale che permette l'identificazione diretta dell'interessato;

dati sensibili (D.Lgs. 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali, art. 4, comma l.d): dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

dati giudiziari (D.Lgs. 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali, art. 4, comma l.e): dato personale idoneo 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.

3.2. Elenco dei trattamenti: informazioni di base

I trattamenti in carico ad ASP sono definiti nella tabella 1.1. che elenca l'allocazione dei trattamenti ne definisce le caratteristiche, se cartacei o informatici e la più esaustiva Tab.3.3 che utilizza la seguente legenda:

Descrizione sintetica (finalità perseguita o attività svolta)
Contiene la descrizione sintetica degli obiettivi del trattamento.

Descrizione sintetica (categorie di interessati)
Indica la categoria di interessati al trattamento

Natura dei dati trattati (Personali/Sensibili / Giudiziari)
Per ogni trattamento è indicata la specifica presenza o meno di dati sensibili o giudiziari. Tutti i trattamenti indicati nella tabella seguente impattano comunque su dati personali e/o identificativi

Struttura di riferimento
E' indicato il servizio interno ad ASP alla quale fa capo il trattamento.

Altre strutture che concorrono al trattamento
Altre strutture interne o esterne/figure ad ASP che concorrono al trattamento in questione, sia le società esterne che concorrono al trattamento (vengono in tal caso indicate tra parentesi).

Descrizione degli strumenti utilizzati
Si indica l'applicazione o l'insieme di applicazioni (quando si parla di sistema informativo) che viene utilizzato per quel trattamento.

Tabella 1.1. Elenco dei trattamenti - informazioni di base

N° PC	In rete	Archivi Cartacei	Denominazione Ufficio	Sede
1	1	1	Dir.Medica	Gerolamo
1	1	1	Uff. Amministrativo	Gerolamo
1	1	2	Uff Infermieristico	Gerolamo
1	0	2	Serv. Educativo	Gerolamo
1	1	1 (certif di morte)	Centralino	S. Margherita
2	0	1	Serv. Animazione	Pertusati
1	1	1	Centralino	Pertusati
5	1	3	Direzione Medica	Pertusati
4	4	2	Economato RSA	Pertusati
1	1		Magazzino Cucina	Pertusati
1			Luogo di culto	Pertusati
1			Uff. Provvisorio	Pertusati
1	1	1	Sala Medica Segù	Pertusati
1	1	1	sala Medica sez. Gialla	Pertusati
2	2	1	Sala Medica Cabras	Pertusati
1	1	1	Sala Medica Zavaglia	Pertusati
1	1	1	Palestra A	Pertusati
1		1	Palestra B	Pertusati
3	2	3	Direzione Generale	UC
5	5	3	Serv. Endocrino-Nutrizionale	S. Margherita
1	1		Economato IDR	S. Margherita
2	2	2	Contratti	UC
2	2	2	Statistica	UC
5	5	6	Personale	UC
3	3		Uff. Tecnico	UC
2	2		Farmacia	S. Margherita
1	1		Lab Analisi	S. Margherita
2	2		Spedalità	S. Margherita
2	2	1	Pal. Matteotti	S. Margherita
2	2	1	pal s.Margherita	S. Margherita
1	1	1	uff. ticket	S. Margherita
1	1	1	CDC	S. Margherita
1	1	2	CDI	S. Margherita
2	2	1	Sez. B	S. Margherita
2	1		CUP	S. Margherita
2	2	1	GII	S. Margherita
2	2	1	GI	S. Margherita
2	2	1	Amb Geriatr e Prelievi	S. Margherita
2	1	1	Diabetologia	S. Margherita
0	0	4	Provveditore	UC
2	2	1	Sez C	S. Margherita
2	2	1	Serv. di Riabilitazione	S. Margherita
1	1	1	Sala infermieristica GI	S. Margherita
1	1	1	Sala infermieristica GII	S. Margherita
1	1	1	Sala infermieristica GIII	S. Margherita
1	1	1	Sala infermieristica A	S. Margherita
1	1	1	Sala infermieristica B	S. Margherita
1	1	1	Sala infermieristica C	S. Margherita
1	1	1	Hospice	S. Margherita
1	1	1	Hospice	S. Margherita
1	1	1	Beltrami	S. Margherita

N° PC	In rete	Archivi Cartacei	Denominazione Ufficio	Sede
1	1	1	Schifino	S. Margherita
1	1	1	Ricevuti	S. Margherita
1	1	1	Cuzzoni, Maestri, Loria, Mameli	S. Margherita
2	2	1	Cuzzoni, Mameli, Loria, Formica, Loconti,	S. Margherita
1	1	1	Ricevuti	S. Margherita
2	2	1	Rollone, Bocchi	S. Margherita
2	2	1	Pellegrino, Genta, Arcuri, Mazzacane	S. Margherita
3	2	1	, Bressani,	UC
5	5	1	Riccio, Tartarotti, Di Maio, Tavazzani, Ruzza	UC

3.3. Elenco dei trattamenti: descrizione della natura del dato e degli strumenti utilizzati

		Natura dato					
Finalità perseguita o attività svolta	Categorie di interessati	P	S	G	Ufficio e Responsabile	Altri incaricati	Strumenti utilizzati
Protocollazione, registrazione ed Archiviazione di tutte le pratiche trattate dall' ASP	Tutti i soggetti di tutte le categorie che si interfacciano per qualsiasi motivo con l'ASP.	x	x	x	Ufficio Protocollo /Archivio **Scarpa**	Maestri	2 PC in rete SW "Folium" e "Civilia"
Approvazione, smistamento, determinazioni relativamente a tutte le pratiche trattate dall'ASP. Strategia e Management	Tutti i soggetti di tutte le categorie che si interfacciano per qualsiasi motivo con l'ASP.	x	x	x	Direzione Generale e Segreteria **Niutta**	Bernuzzi, Nitrato Izzo	2 PC in rete SW "Folium" e "Civilia", Banche dati in rete
Gestione dati di natura economica e dati anagrafici di fornitori	Aziende ed enti esterni(fornitori)	x			U.O.F.C **Riccio**	Di Maio, Tartarotti, Tavazzani, Ruzza	Software Gestionale "Onda"
Gestione dati personali e sensibili dei dipendenti	Tutto il personale dipendente	x	x		Stipendi **Rosa**	Rosa, Solerte, Alpeggiani, Finotti, Brugnoli, Reccagni, Viscomi	SW personalizzato "Syntecop" e "Gestione Personale" Biosistemi, vecchia e nuova versione
Gestione dati anagrafici per contratti	Aziende ed enti esterni(fornitori)	x			Contratti/Provveditorato **Noè**	Migliazza, Oltremonti	File singoli su file server non condivisi
Gestione dati personali e sensibili dei dipendenti	Tutto il personale dipendente	x	x		Personale **Rosa**	Solerte, Alpeggiani, Brugnoli Reccagni	SW "Gestione Personale" vecchia e nuova versione Biosistemi
Gestione dati tecnici	Aziende ed enti esterni(fornitori)	x			Tecnico **Ghilioni**	Beolchi, Montini, Albano.	File singoli su file server non condivisi
Gestione domande e ricovero RSA, IDR, CDI, Ambulatori, debito informativo e quindi Gestione dati personali e sensibili dei dipendenti. Attività connesse con il CUP.	Ospiti e possibili ospiti, tutto il personale dipendente e non	x	x		Statistica_Relazioni con il Pubblico - CUP **Magnani**	Cavallotti, Pasolini, Suardi, Caselli	Sw "SIESA" biosistemi Sw "SOSIAweb" SW "Gestione Personale" vecchia e nuova versione Biosistemi
Gestione dati sensibili	Ospiti e dipendenti		x		Direzione Medica	Tolentino, Finotti,	File singoli su file

di natura medica					RSA **Segù**	De Paoli, Corradini	server non condivisi, Sw "SIESA" biosistemi, SW "Gestione Personale" vecchia e nuova versione Biosistemi
Gestione dati sensibili di natura medica	Ospiti e dipendenti		x		Direzione Medica RSD **Segù**	Cavallotti T.,	"Gestione Personale" vecchia e nuova versione Biosistemi, dati in locale
Gestione dati per rette	Ospiti	x	x		Economato ASP **Pezza, Locatelli, Baccalini**	Pezza, Russino, Locatelli, Filippi, Baccalini,	Sw "Siesa" biosistemi
Gestione dati sensibili di natura medica	Ospiti e dipendenti		x		Direzione Medica IDR **Rollone**	Bocchi, Pellegrino	Domande di ricovero, cartelle cliniche.
Gestione pratiche inerenti al ricovero Gestione domande e ricovero IDR, CDI, Ambulatori, debito informativo	Ospiti e possibili ospiti	x	x		Spedalità SM **Rollone**	Simone, Bocchi, Reccagni, Brocchetta	Sw "Five" Debito Informativo, domande di ricovero
Centralino S. Margherita	Ospiti	x	x		Certificati di morte	Miranda, Fiammenghi, Aramini, Longhi	Elenco ospiti ricoverati
Centralino F. Pertusati	Ospiti	x	x		Elenco ospiti ricoverati	Ordali, Fusetto	Elenco ospiti ricoverati
Gestione dati salute e stato cognitivo utenti	Ospiti RSD		x		Animazione/educazione **Cavallotti**,	Tutti animatori (elenco a parte)	File locali su PC non in rete. Solo il coordinatore ha 1 PC in rete
Gestione dati medici	Ospiti	x	x		**Attività sanitaria specifica**	Personale sanitario (medico ed infermieristico)	Documenti diversi in locale ed in rete
Gestione dati sui farmaci	Ospiti	x	x		**Farmacia Bellotti**	Naddeo	Sw "Magazzino Farmaci" biosistemi
Gestione dati di Geriatria, Endocrinologia e Diabetologia	Ospiti		x		**Attività sanitaria specifica**	Personale medico specializzato	Documenti diversi in locale ed in rete
Gestione prenotazioni ambulatoriali	Dati pazienti per le prenotazioni delle prenotazioni	x			**Prenotazioni ambulatoriali**	Suardi, Bucci, Caselli	SW CUP Omnicom
Gestione di dati inerenti ai parametri bioumorali	Utenti esterni, ospiti, dipendenti		x		**Esecuzione esami di laboratorio**	Personale specializzato Bonora, Maggi, Signorino, Picci	Documenti diversi in locale
Gestione dati Attività di palestra	Ospiti	x	x		**Serv. di Riabilitazione ASP Mazzacane**	Personale specializzato(FKT, elenco a parte)	Liste attesa fornito da Regione SW CUP

I trattamenti in carico ad ASP sono realizzati attraverso la strumentazione elettronica allegata: Vedere:
Censimento app. informatiche

Ubicazione fisica dei supporti di memorizzazione

Indica la collocazione fisica (sede geografica) dei supporti magnetici utilizzati per la memorizzazione dei dati. Ove indicato come "loro sedi" ci si riferisce alle memorie interne ai singoli sistemi di stampa ASP in dotazione presso ASP. Tutti i dati, per regolamento informatico (da allegare), sono memorizzati sui server nelle rispettive ubicazioni. A questi si aggiungano hard disk rimovibili, in dotazione all'Amministratore di rete, utilizzati per gestire i backup periodici. Tali dischi sono presso il locale server.

Tipologia dei dispositivi di accesso e Modalità di interconnessione

Tutti i dati, per regolamento informatico (da allegare), sono memorizzati sui server nelle rispettive ubicazioni. A questi si aggiunga un hard disk rimovibile, in dotazione all'Amministratore di rete, utilizzato per gestire i backup periodici. Tale disco è presso il locale server quando in uso, altrimenti protetto in armadio chiuso a chiave nell'ufficio IT

I dispositivi di accesso alla rete sono personal computer e telefoni IP, connessi a reti Lan configurate in VMAN.
Telefoni e PC sono segregati e non si "vedono" fra loro in rete. La modalità di connessione prevede sempre la autenticazione utente; eventuali accessi non autorizzati possono accedere all'elenco degli host in rete ma non alle relative risorse.

4. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA' (REGOLA 19.2)

Competenze e responsabilità degli incaricati preposti ai trattamenti

Incaricato	Trattamento	Descrizione compiti e delle responsabilità
Scarpa, Maestri		Registrazione, Protocollazione, Archiviazione e smistamento di tutte le pratiche attive e non presso l'ASP
Riccio, Di Maio, Tartarotti, Tavazzani, Ruzza		Controllo e analisi del bilancio, registrazione fatture, pagamenti
Rosa, Solerte, Brugnoli		Preparazione buste paga dipendenti, calcoli per le pensioni
Noè, Bressani, Oltremonti,		Contratti, affitti, procedure di acquisto, gare ed appalti.
Rosa, Alpeggiani, Solerte, Viscomi, Finotti, Brugnoli, Reccagni		Gestione anagrafiche, curricula, timbrature, ferie, malattie, turni ecc.
Niutta		Direzione Generale, strategia decisionale e amministrativa dell'ente.
Bernuzzi , Nitrato Izzo		Stesura e redazione delibere e determine dell'Organo amministrativo preposto. Provvedimenti su tutte le pratiche attive presso l'ASP.
Ghilioni, Beolchi, Montini, Albano.		Gestione, coordinamento e collaborazione per opere di manutenzione, di ristrutturazione, programmazione tecniche per l'ASP
Magnani, Cavallotti , Graziano		Debito informativo ASP, accreditamenti ASP e liste di attesa ASP. Reclami utenza, anche personali.
Segù, Tolentino, Finotti, De Paoli, Corradini		Pratiche sanitarie ed amministrative per i ricoverati presso la RSA. Gestione anagrafiche, curricula, timbrature, ferie, malattie, turni ecc.
Pezza, Russino, Filippi, Baccalini.		Gestione rette ospiti e acquisti ordinari. Gestione magazzino e personale add. Cucina e centralino.
Ordali, Caselli, Fusetto, Conterio, Miranda, Aramini, Longhi, Di Carlo.		Tenuta elenchi telefonici e elenco nominativi pz ricoverati per reparto e camera.
Brocchetta, Simone, Bocchi, Pellegrino, Reccagni		Pratiche sanitarie inerenti il ricovero e la gestione dei pagamenti con il SSR
Suardi, Pasolini, Caselli		Dati sanitari inerenti le prenotazioni e le distribuzioni dei referti
Cavallotti T. , Negri, Ferraro, Montanari, Pecoraro, Scotti.		Valutazione autonomie di base e capacità cognitive degli utenti per la programmazione di interventi educativi e di modalità comportamentali e relazionali
Personale sanitario: Medico ed infermieristico		Ricovero, diagnosi, assistenza e cura
Bellotti, Naddeo		Gestione richieste di farmaci nominali da parte del Responsabile, Servizio di magazzino
Bonora, Tripodi, Carloni, Picci, Bucci,		Esecuzione esami di laboratorio. Gestione ambulatoriale Service, Decontaminazione ambientale.
Suardi, Caselli, Pasolini		Prenotazioni prestazioni ambulatoriali
Personale Medico ed infermieristico		Prevenzione diagnosi e cura di patologie nel settore precedentemente specificato
Personale medico e fisioterapico		Prevenzione diagnosi e cura (FKT) di patologie nel settore precedentemente specificato

La tabella precedente riassume l'attuale suddivisione delle responsabilità in accordo con quanto previsto nel D.Lgs. 196/03.

4.1. Strutture preposte ai trattamenti

Ufficio e Responsabile Finalità perseguita o attività svolta	Altri incaricati	
Protocollazione, registrazione ed Archiviazione di tutte le pratiche trattate dall' ASP	Ufficio Protocollo /Archivio **Scarpa**	Maestri
Approvazione, smistamento, determinazioni relativamente a tutte le pratiche trattate dall'ASP. Strategia e Management	Direzione Generale e Segreteria **Niutta**	Bernuzzi, Nitrato Izzo
Gestione dati di natura economica e dati anagrafici di fornitori	U.O.F.C **Riccio**	Di Maio, Tartarotti, Tavazzani, Ruzza
Gestione dati personali e sensibili dei dipendenti	Stipendi **Rosa**	Rosa, Solerte, Alpeggiani, Brugnoli, Reccagni, Viscomi, Finotti
Gestione dati anagrafici per contratti	Contratti/Provveditorato **Noè**	Bressani, Oltremonti
Gestione dati personali e sensibili dei dipendenti	Personale **Rosa**	Solerte, Alpeggiani, Brugnoli Reccagni
Gestione dati tecnici	Tecnico **Ghilioni**	Beolchi,Montini, Albano.
Gestione domande e ricovero RSA, IDR, CDI, Ambulatori, debito informativo e quindi Gestione dati personali e sensibili dei dipendenti. Attività connesse con il CUP.	Statistica_Relazioni con il Pubblico - CUP **Magnani**	Cavallotti, Pasolini, Suardi, Caselli. Gabetta
Gestione dati sensibili di natura medica	Direzione Medica RSA **Segù**	Tolentino, Finotti, De Paoli, Corradini
Gestione dati sensibili di natura medica	Direzione Medica RSD **Segù, Xoxi**	Cavallotti T.,
Gestione dati per rette	Economato ASP **Pezza, Filippi, Baccalini**	Pezza, Russino,Filippi, Baccalini,
Gestione dati sensibili di natura medica	Direzione Medica IDR **Rollone**	Bocchi, Pellegrino
Gestione pratiche inerenti al ricovero Gestione domande e ricovero IDR, CDI, Ambulatori, debito informativo	Spedalità SM **Rollone**	Simone, Brocchetta, Pellegrino, Bocchi, Reccagni.
Centralino S. Margherita	Certificati di morte	Ordali, Di Carlo, Miranda, Aramini, Longhi
Centralino F. Pertusati	Elenco ospiti ricoverati	Ordali, Di Carlo, Miranda, Aramini, Longhi
Gestione dati salute e stato cognitivo utenti	Animazione/educazione **Cavallotti,**	Tutti animatori (elenco a parte)
Gestione dati medici	**Attività sanitaria specifica**	Personale sanitario (medico ed infermieristico)
Gestione dati sui farmaci	**Farmacia** **Bellotti**	Naddeo
Gestione dati di Geriatria, Endocrinologia e Diabetologia	**Attività sanitaria specifica**	Personale medico specializzato
Gestione prenotazioni ambulatoriali	**Prenotazioni ambulatoriali**	Suardi, Bucci, Caselli, Gabetta
Gestione di dati inerenti ai parametri bioumorali	**Esecuzione esami di laboratorio**	Personale specializzato Bonora, Maggi, Signorino, Picci
Gestione dati Attività di palestra	**Serv. di Riabilitazione ASP Mazzacane**	Personale specializzato(FKT, elenco a parte)

S. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI (REGOLA 19.3)

5.1. Premessa

L'analisi dei rischi è il processo mediante il quale si identificano le potenziali minacce che incombono sui dati e sui trattamenti in relazione ai mezzi utilizzati; essa costituisce lo strumento principe per impostare ed assicurare la protezione delle risorse informative aziendali.

L'obiettivo principale dell'analisi dei rischi è quello di individuare e quantificare i rischi reali ai quali possono essere soggetti i trattamenti volendo minimizzare le possibilità che si verifichino:

- D trattamenti non consentiti o non conformi con le finalità della raccolta;
- D accessi non autorizzati.
- D danneggiamento o perdita di informazioni

5.2. Modello di analisi

L'analisi dei rischi è indirizzata ad identificare le possibili violazioni dei requisiti di base di sicurezza dei dati in termini di:

D riservatezza	intesa come la garanzia che le informazioni siano accessibili solo alle persone autorizzate, tramite la protezione delle trasmissioni, il controllo degli accessi, ecc.;
D integrità	intesa come la gestione dell'accuratezza e della completezza delle informazioni e delle relative applicazioni, la salvaguardia della esattezza dei dati, la difesa da manomissioni o modifiche non autorizzate, ecc;
D disponibilità	intesa come l'assicurazione che l'accesso ai dati sia disponibile quando necessario, quindi costituisce la garanzia per gli utenti della fruibilità dei dati e dei servizi, evitando la perdita o la riduzione dei dati e dei servizi.

Il grado di copertura fornito dalle misure di sicurezza organizzative, fisiche, logiche e operative già in essere nella ASP, viene determinato attraverso le risorse tecniche della struttura

La valutazione dei rischi è stata effettuata utilizzando i seguenti criteri:

Tabella E: Metrica utilizzata per l'analisi dei rischi

Rischio (cioè pericolosità derivante dall'evento\	Probabilità (cioè possibilità che l'evento si presenti nel tempo\	Gravità
basso	bassa	Bassa
basso	alta	Medio bassa
alto	bassa	Medio alta
alto	alta	Alta

Legenda:
Si intenda per rischio:
- medio: un rischio statisticamente compatibile con la realtà in essere, che merita però osservazione e precise misure preventive.
- basso: un rischio trascurabile, considerato ai fini della determinazione delle misure minime di sicurezza
- medio basso: un rischio che potrebbe essere trascurabile ma con imprevedibilità che suggeriscono una attenzione dedicata
- medio alto: un rischio di probabile verifica, in quanto sussistono condizioni oggettive perché ne occorrano le circostanze (ad es. uso di calcolatori non protetti da password e posto in ambiente non controllato – circostanza accademica non presente nella ASP)
- alto: un rischio di nota evenienza statistica e occorrenza prevedibile

Si intenda per gravità:
- media: un evento risolvibile con risorse normalmente disponibili ma che comporta costi e disagi di natura non ordinaria, con interruzioni di servizio evidenti ma senza conseguenze
- bassa: un evento risolvibile in manutenzione ordinaria, eventualmente dagli stessi utenti finali e senza costi, nessuna interruzione di servizio
- medio bassa: un evento facilmente risolvibile con disagi minimi, brevi interruzioni di servizio
- medio alta: un evento risolvibile, ma con interruzioni di servizio superiori a 24/48 ore, costi straordinari e potenziale danno alla efficienza del sistema che si prolunghi per oltre 48 ore dopo l'emergenza
- alta: evento non completamente risolvibile, con certo danno alla efficienza del sistema successivo alla emergenza di una settimana ed oltre."

5.3 Misure d'azione

Le varie misure di sicurezza sono state classificate secondo la tabella seguente:

Tabella F. Classificazione delle misure di sicurezza

Classe della misura	Livello di applicazione

2. Autenticazione	I sistemi ed i servizi di ASP sono accessibili solo attraverso il superamento di una procedura di autenticazione che prevede l'utilizzo di credenziali associate a li incaricati.
3. Controllo dell'accesso ai dati (autorizzazioni)	L'accesso ai dati è controllato attraverso i profili di autorizzazione definiti al livello del sistema operativo della piattaforma che ospita l'applicazione (Window o ASj400)
4. Controllo dell'integrità dei dati (antivirus, firewall, patch management)	Sono attivi servizi di controllo per la presenza di virus sia nei file system locali dei singoli PC che nei file system condivisi, oltre che sui messaggi di posta elettronica.

5. Backup & Disaster recovery	Sono in atto politiche di backup per i dati. Sono in atto attività indirizzate a ridurre il disservizio in caso di guasto (disaster recovery)
6. Gestione delle politiche di sicurezza	Sono predisposte delle policy di sistema indirizzate alla sicurezza
7. Formazione degli incaricati	E' previsto un piano di formazione e di aggiornamento per gli incaricati di ASP

Ogni classe di misura d'azione è composta da diversi interventi di sicurezza che sono raccolti e dettagliati nel paragrafo seguente.

5.4. Tabella di riepilogo analisi dei rischi

La tabella riepiloga gli eventi considerati nell'analisi dei rischi sopra descritta e ne evidenzia la tipologia di impatto:

Tabella 3.1. Analisi dei rischi

Ambito	Rischio	Probabilità	Gravità	Fattore di Rischio
Comportamento degli operatori	Furto di credenziali di autenticazione	BASSA	ALTA	MEDIO
	Carenza di consapevolezza, disattenzione, incuria	MEDIA	MEDIA	MEDIO
	Comportamenti sleali o fraudolenti	BASSA	ALTA	MEDIO
	Errore Materiale	MEDIA	BASSA	Basso
	Indisponibilità non prevista dall'operatore	MEDIO BASSA	BASSA	Basso
	Strumento non presidiato benché operativo e connesso	BASSA	MEDIO ALTA	Medio bassa
Eventi relativi agli strumenti	Azione di virus informatici o programmi dannosi	MEDIO BASSA	MEDIA	Medio ALTO
	Spamming o altre tecniche di sabotaggio	BASSA	BASSA	BASSA
	Malfunzionamento, indisponibilità o degrado degli strumenti	MEDIO BASSA	BASSA	Bassa
	Accessi esterni non autorizzati	BASSA	MEDIO ALTA	Medio basso
	Intercettazione di informazioni rete	BASSA	MEDIA	Medio BASSA
Eventi relativi al contesto	Accessi non autorizzati a locali/reparti ad accesso ristretto	BASSA	ALTA	MEDIO
	Asportazione e furto di strumenti contenenti dati	MEDIA	BASSA	MEDIO ALTO
	Eventi distruttivi naturali, artificiali, dolosi, accidentali o dovuti ad incuria	BASSA	ALTA	MEDIO
	Guasto ai sistemi complementari (impianto elettrico, climatizzazione)	MEDIA	BASSA	BASSO
	Errori umani nella gestione della sicurezza fisica	BASSA	MEDIO	MEDIO BASSO

1. Sicurezza dei locali e degli apparati	Le aree tecniche di competenza di ASP sono caratterizzate da misure che controllano l'accesso fisico ai locali.

6. MISURE IN ESSERE O DA ADOTTARE (REGOLA 19.4)

6.1. Premessa

In questa sezione vengono presentate le misure di sicurezza fisiche, logiche e organizzative, adottate per tutelare tutte le strutture preposte al trattamento dei dati da tutti i rischi (di tipo ambientale, accessi fisici non autorizzati, attacchi portati agli strumenti elettronici, ecc.) attraverso contromisure tecniche od organizzative; le contromisure tecniche possono essere di tipo logico o fisico.

6.2. Schema riassuntivo delle misure di sicurezza

La tabella seguente riassume le misure di sicurezza adottate o da adottare:

Tabella H

Misura	Titolo	Resp. della adozione	Tipologia
1	Nessuna	n.a.	n.a.
2	Corsi di formazione del personale	Ente – IT	Preventiva
3	Monitoraggio dell'ambiente	Ente – Resp. sicur.	Preventiva
4	Corsi di aggiornamento	Ente – IT	Preventiva
5	Antivirus / Firewall	Fornitori	Preventiva
6	Ignorare l'e-mail non ritenute sicure, comportamenti prudenti	Utenti	Preventiva
7	Cambio password	Utenti amministratori degli elaboratori	
8	Rinnovo continuo dei software, manutenzione degli apparati	Fornitori	Correttiva
9	Controlli sugli accessi informatici, autenticazione credenziali	Ente – IT, Amministratore di rete	Preventiva
10	Copie di sicurezza	Amministratore di sistema	Preventiva
11	Crash recovery	Amministratore di sistema	Correttiva
12	Disaster recovery	Amministratore di sistema	Correttiva
13	Antifurto, grate, controllo accessi e altre misure di sicurezza fisica mediante barriere	Ente – Ufficio Tecnico	Preventiva
14	Antifurto, antincendio, videosorveglianza ed altre misure di sicurezza attiva con controllo elettronico	Fornitori	Preventiva/ Correttiva
15	Revisioni e controlli periodici	Ente	Preventiva
16	Gruppo di continuità, linee dedicate	Ente – Ufficio Tecnico	Preventiva
17	Blocco automatico a tempo dell'elaboratore	Utenti amministratori degli elaboratori	Preventiva
18	Protezione mediante conservazione in luogo protetto	Utente, Ente – IT	Preventiva
19	Intervento di assistenza tecnica	Ente – IT, Amministratore di rete, Fornitori	Correttiva

Legenda tipologia

Preventiva	Misura attuata per contrastare un rischio analizzato
Correttiva	Predisposizione di procedura per contrastare il danno emergente dal verificarsi di una situazione di rischio

6.3. Schede analitiche delle misure di sicurezza adottate

6.3.1 Basso rischio

Per circostanze a basso rischio e bassissimo impatto dannoso non viene adottata nessuna contromisura.

Al momento non vi sono tuttavia circostanze previste e non contrastate. Si rimanda comunque al richiamo operativo allegato al presente documento e pubblicato in bacheca.

6.3.2 Corsi di formazione del personale

Le misure sono adottate al fine di dare conoscenza e sensibilizzare gli incaricati e garantire una corretta adozione delle misure minime di sicurezza.
Sono periodicamente distribuite note relative agli aggiornamenti del Regolamento per l'utilizzo degli elaboratori, questo è pubblicato in bacheca presso il Centralino delle strutture.

6.3.3 Monitoraggio dell'ambiente

Ambiente fisico e informatico, che sempre più vanno considerati integrati quale unica struttura, sono monitorati mediante videosorveglianza e controlli almeno mensili sullo stato di salute degli impianti.
La videosorveglianza comporta la conservazione dei dati per almeno 7.gg. I dati sono accessibili solo agli operatori dedicati.

6.3.4 Corsi di aggiornamento

Periodicamente i sistemi sono aggiornati. Quando le modifiche prevedono variazioni operative, come nella sostituzione o aggiornamento di procedure software, il personale riceve idonea formazione per l'utilizzo delle nuove procedure. La formazione in alcuni casi potrà prevedere che le procedure vengano trasmesse agli operatori dagli utenti esperti.

6.3.5 Antivirus / Firewall

I PC e i server sono protetti mediante Antivirus NOD32. La rete è connessa all'esterno mediante Router-firewall Netasq. Presso l'IDR è stato installato firewall aggiuntivo per limitare accessi a siti indesiderati. La VPN metropolitana è realizzata mediante tunnel IPsec nei quali il reciproco riconoscimento dei router garantisce protezione contro intrusioni indesiderate.

6.3.6. Ignorare l'e-mail non ritenute sicure, comportamenti prudenti

È adottato un "regolamento informatico" , che si riallega insieme alle istruzioni operative di recente revisione, con la finalità di determinare comportamenti, da parte degli operatori, che non sollevino rischi per la sicurezza.
In particolare, è vietato installare software non autorizzato, trasmettere dati all'esterno senza consenso e con procedure diverse da quelle previste, navigare in internet per scopi personali ed in particolare su siti potenzialmente pericolosi. È vietato ogni comportamento contro le leggi vigenti, di cui il responsabile rimane in esclusiva l'utente informatico. È vietato l'utilizzo del PC per dati e con strumenti personali, come lettori multimediali e telefonini, salva espressa autorizzazione. L'ente si riserva ogni diritto su tutti i dati eventualmente rinvenuti sui PC, incluso quello di verifica e controllo senza necessario preavviso, con attività di funzionario dell'Ente o di personale appositamente delegato. È vietato l'uso di cosiddette "chiavette" (unità disco USB) senza preventiva autorizzazione scritta da parte dell'Amministratore di rete. È vietata la occupazione degli spazi disco, anche con particolare riferimento ai server, con dati non autorizzati. È vietata la installazione di software e dati che violino diritti di autore ed altre leggi. Le autorizzazioni devono essere concesse esclusivamente per iscritto. Gli utenti sono tenuti a segnalare la comparsa di messaggi che identificano falle nella sicurezza (antivirus scaduti o non aggiornati, messaggi di errore o applicazioni non funzionanti).

6.3.7 Cambio password

Periodicamente gli operatori sono invitati a modificare la password. Attualmente la procedura non è completamente automatizzata, essendo stata resa automatica solo la scadenza password, ma si prevede la adozione di procedure automatiche.

6.3.8 Rinnovo continuo dei software, manutenzione degli apparati

Hardware e software sono continuamente aggiornati secondo necessità. Laddove le mutate esigenze funzionali o la ridotta funzionalità dei dispositivi in essere lo richiedano è posta in atto la sostituzione.

Gli apparati sono configurati per accogliere attraverso internet gli aggiornamenti automatici.

I fornitori sono contrattualmente impegnati a fornire gli aggiornamenti necessari alle procedure.

6.3.9. Controlli sugli accessi informatici, autenticazione credenziali

Il sistema di autenticazione informatica è quel processo di verifica della rispondenza dell'identità dell'utente, anche in via indiretta, effettuata attraverso l'insieme di strumenti elettronici e procedure con accesso da parte del soggetto tramite l'utilizzo di apposite credenziali, consistenti nella identificazione dell'utente (nome utente) e di una parola chiave (password) di accesso. Le credenziali di autenticazione sono in possesso dell'incaricato e da solo da questi conosciuti ovvero allo stesso unicamente attribuiti.

Ogni utente, nei sistemi informatici resi disponibili, prima di poter eseguire qualsiasi altra operazione deve effettuare un processo di autenticazione.

La fase di autenticazione può essere distinta sulle diverse piattaforme e risorse di rete: questo significa che l'utente può essere chiamato ad autenticarsi diverse volte in funzione della piattaforma e dell'applicazione che deve utilizzare. Per ragioni di maggior sicurezza le credenziali di accesso potrebbero non essere le stesse, per lo stesso utente, sulle diverse risorse.

6.3.10 Copie di sicurezza

Le copie di sicurezza consentono in caso di danno con irrecuperabilità dei dati di recuperare uno stato di servizio del sistema allineato ad un momento precedente, mediante proceduta cosiddetta di RESTORE.

Vantaggi e limiti/svantaggi procedura Restore:

Vantaggi	Limiti / svantaggi
Rappresenta un buon livello di sicurezza e protezione	Non è garantibile a priori la integrità dei dati conservati
Le copie storicizzate sono virtualmente inalterabili	Si perdono gli ultimi aggiornamenti sui dati

I dati sono salvaguardati da server che lavorano per la maggior parte dei casi con funzione RAID5, un dispositivo hardware/software in grado di gestire ridondanza tecnica di informazioni così da garantire la continuità di servizio in caso di guasto di un disco rigido, che costituisce la prima causa, in ordine statistico, di perdita di dati e disservizi.

I dati periodicamente salvati riguardano:

- Dati Ufficio Utenti
- Posta elettronica
- Database applicazioni

Al momento della stesura del presente documento le procedure di salvataggio di sicurezza sono in aggiornamento.

6.3.10.1. Dati Ufficio utenti

I dati ufficio utenti, da regolamento informatico, devono essere memorizzati sulle dedicate unità disco dei server.

La conseguente centralizzazione dei dati riduce il rischio di furto e consente le copie di sicurezza senza la necessità di scandagliare ogni singolo PC. L'utente è direttamente responsabile della conservazione e protezione dei dati eventualmente memorizzati in locale su proprio PC.

La tecnica è "raw copy" di file, che restano così immediatamente disponibili per eventuali immediati recuperi funzionali.

La procedura è disciplinata dall'Amministratore di rete.

6.3.10.2. Dati posta elettronica

La posta elettronica viene duplicata su NAS a mezzo procedura automatizzata a cura e responsabilità del Fornitore, con periodicità prevista almeno settimanale. Le comunicazioni di cui è necessario garantire integrità storica sono soggette a protocollo (e quindi conservazione separata), per cui nessuna ulteriore copia esterna di sicurezza è prevista per i dati di posta.

6.3.10.3 Database applicazioni

Le applicazioni prevedono procedure interne di copie di sicurezza che sono demandate direttamente agli utenti o, laddove previsto, a funzioni automatiche del software, a cura e responsabilità dei fornitori. Tali copie di sicurezza sono ulteriormente duplicate con procedura almeno settimanale. La indicazione dei dati da reduplicare è demandata alla responsabilità dei fornitori. La reduplicazione è demandata a procedura a cura dell'Amministratore di rete.

Quanto indicato è attualmente operativo per tutti i dati con le seguenti eccezioni:

- software pensioni S7: i dati sono ricoverati manualmente mensilmente
- nuovo software stipendi in attesa di attivazione definitiva: non è ancora integrata una politica di protezione dei dati, in quanto ancora in attesa di idonee istruzioni da parte del fornitore.

6.3.11. Crash recovery

Per "crash" di un sistema si intende il crollo di una o più funzionalità di quel sistema.

Si devono distinguere diverse tipologie di crash, secondo l'estensione del disservizio che ne deriva e il supporto funzionale interessato.

Quanto ad estensione il crash può interessare un solo host della rete (un utente o gli utenti di un unico PC), una area della rete, ovvero più hosts, o una struttura virtualmente necessaria al funzionamento dell'intera rete, come un server o un apparato di distribuzione dati connesso ad uno o più server.

Il supporto funzionale può essere distinto in due macro-categorie: hardware o software. Va precisato che un guasto hardware spesso ha incidenze anche sul software.

Non è sempre possibile prevedere le cause di un crash, ma è noto che il cedimento più frequente è dato:

- dal punto di vista hardware: la rottura di un disco fisso
- dal punto di vista software: virus informatici.

Le misure preventive comportano l'adozione di idonei sistemi RAID sui server per la integrità dei dati e la realizzazione di copie di sicurezza.

Inoltre si prevedono procedure di natura correttiva per minimizzare l'incidenza di eventuali guasti, come di seguito dettagliato:

- rilevazione e verifica del disservizio
- attivazione se necessario dell'intervento tecnico volto a risanare disfunzioni hardware (essendo identificato il fornitore di servizi deputato alle riparazioni hardware)
- attivazione delle procedure di recupero dati (a cura dell'Amministratore di rete), al fine di riportare il sistema nel più aggiornato status di funzionamento
- in caso di necessità ricorrere al ripristino dati dalle copie di sicurezza
- in caso di ulteriore necessità pianificare la ricostruzione dei dati necessari

In caso di necessità di recupero dati sono previste le seguenti procedure:

Passo 1. : azione tecnica volta al recupero dei dati al momento del danno, onde attingere alle informazioni più aggiornate.

Passo 2. : in caso di fallimento anche parziale del passo 1 attingere all'ultima copia di sicurezza disponibile

Riallineamento dei dati: se i dati recuperati sono documenti o database destinati ad un servizio di tipo "file" vengono messi immediatamente a disposizione dell'utenza; se i dati recuperati sono relativi a dati "application server", ad es. SQL, questi sono messi a disposizione del fornitore dell'applicativo e il riallineamento è demandato a quest'ultimo

6.3.12. Disaster recovery

In caso di disastro ambientale o calamità:

- tutti i servizi informatici devono essere sospesi
- si provvederà alla esecuzione di copie di sicurezza o di messa in sicurezza delle copie esistenti laddove ancora reperibili
- dopo il cessato allarme si procederà con l'analisi del danno e la valutazione dei necessari interventi
- si adotterà il criterio di intervento di cui al "crash recovery"

6.3.13. Antifurto, grate, controllo accessi e altre misure di sicurezza fisica mediante barriere

Sono previste barriere architettonico/fisiche contro gli accessi non autorizzati

- Gli uffici sono chiudibili a chiave
- I server sono in locale protetto chiuso a chiave
- Eventuali PC accessibili al pubblico non contengono dati sensibili

Nota: per motivi di continuità di servizio talora i PC possono contenere dati destinati ai server. Eventuale perdurare di tale circostanza può comportare videosorveglianza sulla stazione.

6.3.14. Antifurto, antincendio, videosorveglianza ed altre misure di sicurezza attiva con controllo elettronico

Sono in essere presso l'ASP dispositivi di sicurezza attiva. Per i dettagli si rimanda al Manuale per la sicurezza redatto ai sensi della L.626/94

6.3.15. Revisioni e controlli periodici

Con periodicità almeno mensile è verificato il corretto funzionamento dei server.
Viene altresì verificato che le protezioni antivirus siano aggiornate.

6.3.16. Gruppo di continuità, linee dedicate

I server sono alimentati da gruppo di continuità a stato solido in grado di sostenerne il funzionamento per almeno 10 minuti. In caso di mancanza di alimentazione di rete che si protragga oltre 4 minuti, tuttavia, l'alimentazione è garantita da motogeneratore.

6.3.17 Blocco automatico a tempo dell'elaboratore

I server sono configurati per far sì che in caso di assenza dell'operatore per oltre 20 minuti si attivi un salvaschermo disattivabile solo mediante re immissione delle credenziali dai accesso.

6.3.18 Protezione mediante conservazione in luogo protetto

Le copie di sicurezza sono conservate in ufficio chiuso a chiave. I server sono in ambiente chiuso a chiave accessibile solo da altro ambiente anch'esso protetto da porte chiuse a chiave e dagli accessi video-sorvegliati.

6.3.19 Intervento di assistenza tecnica

È in essere un contratto di fornitura di servizi che assicura, in caso di necessità, l'intervento del tecnico entro 24 ore dalla richiesta.

L'amministratore di rete è, in caso di emergenza, rintracciabile 24/24h a mezzo telefono cellulare noto all'Ente.

7. CRITERI E MODALITA' DI RIPRISTINO DELLA DISPONIBILITA' (REGOLA 19.5)

In relazione al punto 23 del Disciplinare Tecnico del D.Lgs 196/03 che delinea la disposizione di legge "di adozione idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a 7 giorni", vengono descritte di seguito le politiche per la garanzia dei dati trattati e della business continuità management approntate da ASP.

7.1. Sinottico misure minime di sicurezza. Cfr. Disciplinare tecnico al.. B D. lgs 196/03

	Descrizione	Stato attuativo
M1	accesso ai dati o al sistema tramite credenziali di autenticazione e procedura di autenticazione	A
M2	credenziali di autenticazione in possesso ed uso esclusivo dell'incaricato	R/P
M3	assegnazione di una o più credenziali di autenticazione individuali per ogni incaricato	A
M4	segretezza delle credenziali di autenticazione e diligente custodia dei dispositivi	A
M5	lunghezza della parola chiave di almeno 8 caratteri con frequenza di modifica almeno ogni 6 mesi (3 sensibili e giudiziari)	A
M6	codice per l'identificazione univoco e non riassegnato	R
M7	disattivazione delle credenziali di autenticazione per mancato utilizzo (oltre 6 mesi) o perdita qualità	R
M8	istruzione agli incaricati per non lasciare incustodito ed accessibile lo strumento elettronico durante una sessione di trattamento	A
M9	custodia copia di credenziali di autenticazione	A/N
M10	presenza di un sistema di autorizzazione	A
M11	profili di autorizzazioni individuati e configurati anteriormente all'inizio del trattamento	A (CARTA)
M12	verifica annuale della validità dei profili di autorizzazione	A
M13	elenco incaricati ed addetti alla gestione o alla manutenzione	A
M14	protezione contro il rischio di intrusione	A
M15	prevenzione della vulnerabilità degli strumenti elettronici e correzione difetti	A
M16	salvataggio dei dati con frequenza almeno settimanale	A
M17	protezione dati sensibili o giudiziari contro l'accesso abusivo	A
M18	custodia, uso e riutilizzo supporti rimovibili	A
M19	garanzia e ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici	R
M20	dichiarazione di conformità interventi effettuati da soggetti esterni	N/R
M21	controllo e custodia da parte degli incaricati della documentazione contenente dati sensibili e giudiziari	A

Legenda Stato Attuativo

Titolo	Descrizione
A	Misura Attuata
P	Misura prevista in corso di attuazione
R	Misura attuata in fase di revisione
N	Misura non prevista

8. PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI PREVISTI

Intervento	Cadenza
Alfabetizzazione informatica	Annuale o secondo necessità
Procedure	Occasionale, ad aggiornamento procedure
Normativa	Occasionale, a variazione norme

9. TRATTAMENTI CARTACEI

La tabella seguente riassume i trattamenti effettuati con strumenti cartacei.

In taluni casi i trattamenti indicati complementano quelli realizzati con strumenti elettronici.

Le note indicate nella colonna "Descrizione delle misure di sicurezza adottate" le note fanno riferimento a quanto indicato nell'Allegato B - Art. 27, 28 e 29 e cioè:

Nota 1: Art. 27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

Nota 2: Art. 28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

Nota 3: Art. 29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato mediante sistema di allarme. Nessuno è ammesso, a qualunque titolo, dopo l'orario di chiusura.

10. ROTTAMAZIONE PC ED AFFINI

Con il provvedimento "Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali" del 13 ottobre 2008, in G.U. n. 287 del 9 dicembre 2008, il Garante richiede che ogni titolare del trattamento deve adottare appropriate misure organizzative e tecniche volte a garantire la sicurezza dei dati personali trattati e la loro protezione anche nei confronti di accessi non autorizzati che possono verificarsi in occasione della dismissione di apparati elettrici ed elettronici (artt. 31 ss. del Codice).

In pratica il Garante esige che siano prevenuti accessi non consentiti ai dati personali memorizzati nelle apparecchiature elettriche ed elettroniche destinate a essere riciclate o smaltite.

Va detto che Le procedure in essere prezzo la ASP prevedono che i dati siano memorizzati solo su server. In caso di rassegnazione delle apparecchiature client viene quindi eseguita la cancellazione dell'utente con eliminazione dei relativi – eventuali – file personali e la generazione di nuovo utente."

In caso di smaltimento o alienazione di apparati contenenti dati, come ad esempio i dischi dei server, questi saranno preventivamente oggetto di "Wiping", ovvero distruzione sistematica delle informazioni magnetiche contenute sulla superficie dei dischi, oppure di distruzione fisica dei supporti o danneggiamento permanente irreversibile mediante microonde o altro.

Quanto a supporti ottici è prevista distruzione fisica indi smaltimento ordinario.

11. LEGGE 18 MARZO 2008 SUI CRIMINI INFORMATICI

Si tratta della "Legge 18 marzo 2008, n. 48 - "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno" che ha introdotto nuovi adempimenti per la sicurezza informatica in quanto ha modificato (art. 10) sia il "Codice in materia di protezione dei dati personali" sia (art. 7) il decreto legislativo 8 giugno 2001, n. 231 (la cosiddetta "Responsabilità amministrativa delle imprese").

Di seguito l'elenco dei reati informatici trattati da questa legge.

- 420: attentato a impianti di pubblica utilità compreso il danneggiamento o la distruzione di sistemi informatici o telematici di pubblica utilità
- 491-bis: falsità in un documento informatico pubblico o privato
- 615-ter: accesso abusivo ad un sistema informatico o telematico
- 615-quater: detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
- 615-quinquies: diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico
- 617-quater: intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
- 617-quinquies: installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche
- 635-bis: danneggiamento di informazioni, dati e programmi informatici
- 635-ter: danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità
- 635-quater: danneggiamento di sistemi informatici o telematici
- 640-quinquies: truffa del certificatore di firma elettronica

Vediamo in dettaglio alcuni di questi reati.

Art. 615 ter Accesso abusivo ad un sistema informatico o telematico: Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni se il fatto è commesso (...) con abuso della qualità di operatore del sistema.

Art. 615-quinquies: diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico: "Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, e' punito con la reclusione fino a due anni e con la multa sino a euro 10.329".

Nota: la norma quindi include non solo il software, ma anche l'hardware, comprendendo tutte quelle apparecchiature e dispositivi il cui funzionamento sia idoneo a danneggiare un sistema informatico, ovvero ad alterarne il funzionamento.

In pratica il "delitto" di cui all'art. 615 quinquies scatta non solo quando ci si procura virus e malware in genere, ma anche nel caso di produzione, importazione, acquisto di dongle, smart card, skimmer e così via, laddove, naturalmente, si prestino ad un utilizzo illecito, al fine appunto di danneggiare o alterare un sistema informatico, ovvero i dati e programmi ivi contenuti.

Articolo 635 - bis: danneggiamento di informazioni, dati e programmi informatici: "Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto e' commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio"

È opportuno che nel capitolo del DPS dedicato alle "Misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità" siano indicati, se già non presenti, per ciascuna di tale tipologia di possibile "crimine informatico" quali misure di sicurezza sono state (o saranno) adottate.

Il titolare deve esercitare, in modo strutturato e periodico, direttamente la sua responsabilità "in vigilando" nei confronti di:

- responsabili interni da lui direttamente (o indirettamente) nominati;
- incaricati (o per meglio dire "classi di incaricati": marketing, risorse umane, sistemi informativi, consulenti esterni, ecc.)
- amministratori di sistema interni;
- responsabili esterni;
- società terze non nominate "responsabili esterni" ma che tuttavia gestiscono in un modo o nell'altro trattamenti del titolare (ad esempio: contitolari, titoli autonomi, outsourcer, ecc.).

Il titolare deve esercitare inoltre, anche qui in modo strutturato e periodico, ma indirettamente la sua responsabilità "in vigilando" nei confronti di:

- (sub)responsabili esterni, cioè responsabili esterni rispetto ai propri responsabili esterni (ad esempio: se il titolare ha nominato la società ABC responsabile esterno per il trattamento dei dati relativo alle buste paghe e la società ABC ha nominato a sua volta la software house "Pinco Pallino" responsabile esterno in qualità di outsourcer dei propri sistemi informativi allora "Pinco Pallino" è un (sub)responsabile esterno rispetto al titolare);
- amministratori di sistema nominati dai responsabili esterni, dai (sub)responsabili esterni, da società terze non nominate "responsabili esterni".

Il titolare può essere chiamato a rispondere (e quindi a dover documentare e dimostrare il suo operato) della sua responsabilità in eligendo, in vigilando e in generale delle due diligence effettuate a diverse categorie di "stakeholder" (termine molto in voga per indicare i "portatori d interessi" ciò coloro che hanno titolo per richiedere che i loro interessi e/o diritti siano garantiti).

Autorità:

- Garante Privacy
- Magistratura, Forze di polizia
- Organismi di vigilanza (ad esempio Banca d'Italia nel caso di intermediari finanziari)

Organismi di controllo interno:

- Consiglio di Amministrazione
- Collegio Sindacale
- Comitati vari di controllo, sicurezza, audit
- Compliance Officer (della società e del gruppo)
- Internai Audit (della società e del gruppo)
- Revisori dei Conti
- Certificatori (1s09001 ed affini)
- Responsabile della Business Continuity (della società e del gruppo)

"Interessati" che intendono esercitare il loro "diritto di accesso":

- Dipendenti,
- clienti,
- fornitori
- e chiunque voglia esercitare tale diritto.

12.0 MODELLO Leg.svo 231

L'ASP adotta il Documento sulle attività da cui possono derivare responsabilità amministrative dell'Azienda ex Decreto Legislativo 231/2001 e sulla proposta di modello organizzativo, nonché il Codice – etico – comportamentali. Il Modello è disponibile agli atti dell'Ente, è affisso nelle bacheche dell'Ente, è pubblicato sul sito web aziendale: www.asppavia.it ed è

13. AMMINISTRATORE DI SISTEMA

Si tratta del provvedimento "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 novembre 2008, in G.U. n. 300 del 24 dicembre 2008

- attività da svolgere
- tempi di completamento previsti
- risorse aziendali dedicate a ciascuna attività
- deliverable per ciascuna attività
- rapporto di fine attività.

13.1.

Lista degli Amministratori di Sistema

L'amministratore di sistema è individuato nella figura del sig. Paolo Marino, sulla fiducia del Rappresentante Legale dell'Ente.

14.0 Progetto SISS

Vedere allegati

SOMMARIO pag