Allegato sub 1 alla Deliberazione n. 109 del 21/03/2012

Hanno collaborato alla stesura di questo documento:		
Servizio	Qualifica	Nome cognome

Verifica/approvazione dei Responsabili di coloro che hanno collaborato alla stesura[1]		
Servizio	Qualifica-Nome/Cognome	Firma

stesura			**Verifica/approvazione**	**emissione**
Qualifica	Nome	Firma		
Dirigente	Gerbaudo Damiano (S.C. Informatica & Telecomunicazioni)	_____	Responsabile S.C. Informatica & Telecomunicazioni Ing. Aldo BORGNA _____	Commissario Dr. Giovanni MONCHIERO _____
Collaboratore Prof.le Amm.vo Esperto	Peano Martina (S.C. Servizio Legale)	_____	Per il Responsabile della S.C. Servizio Legale Direttore Amministrativo Dr. Alberto Osenda _____	

L'originale firmato in versione cartacea e la versione elettronica del documento sono conservati presso gli archivi del Rappresentante della Direzione.

SOMMARIO

1. PREMESSA

Il presente elaborato costituisce il Documento Programmatico sulla Sicurezza (D.P.S.).

Scopo del documento è quello di formalizzare, razionalizzare e finalizzare le strategie aziendali relative alle politiche di sicurezza, in materia di trattamento di dati personali, e di definire i criteri organizzativi per la loro attuazione, con particolare riferimento a:

a) protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché procedure per controllare l'accesso delle persone autorizzate ai medesimi locali;
b) procedure per assicurare l'integrità dei dati;
c) procedure per la sicurezza della trasmissione dei dati;
d) elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni.

Nel documento:

- vengono identificate le **risorse da proteggere** che hanno impatti con i problemi di sicurezza e svolgono un ruolo significativo nei processi di trattamento dei dati personali;
- viene illustrata la distribuzione dei **compiti e delle responsabilità** nell'ambito delle strutture preposte al trattamento dei dati;
- viene effettuata un'**analisi dei rischi** che costituisce un punto fondamentale per affrontare in maniera definita e controllata le problematiche di sicurezza;
- si definiscono, inoltre, le **misure di sicurezza** (organizzative, fisiche e logiche), in essere e da adottare, per tutelare le strutture e le risorse preposte al trattamento dati e quindi ai dati stessi;
- vengono elencati **i criteri e le modalità per il ripristino dei dati** in caso di perdita dei dati dovuta, ad esempio, ad un guasto;
- vengono elaborati **criteri e procedure per il trattamento dei rischi residui:** procedere non solo all'eliminazione dei rischi monitorati ma anche alla loro riduzione o in alternativa al trasferimento degli stessi (ove possibile) a terzi.

1.1 RIFERIMENTI DEL DOCUMENTO

Titolo del Documento	**Documento Programmatico sulla Sicurezza dell'Azienda Sanitaria Locale CN1 – Anno 2012**
Numero di versione	**v. 1.00**
Data ultimo aggiornamento	**19/03/2012**
Stato del documento	**In corso**
Luogo di conservazione dell'originale cartaceo e di tutti gli allegati	**Presso il Servizio Legale dell'ASL CN1**
Modalità di distribuzione delle nuove versioni	**On-line sul sito intranet aziendale**

1.2 AMBITO DI APPLICAZIONE

Il presente documento si applica a tutti i flussi informativi che coinvolgono dati personali, sensibili e giudiziari gestiti dall'Azienda per il raggiungimento delle proprie finalità istituzionali.

1.3 TRATTAMENTI EFFETTUATI DALL'AZIENDA

Con il termine "trattamento", ai sensi dell'art. 4, comma 1, lett. a) del D.lgs. 196/03, deve intendersi "*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 dei dati*."

Qualunque trattamento di dati personali da parte dell'AZIENDA SANITARIA A.S.L. CN1, quale organismo sanitario pubblico, è consentito soltanto per lo svolgimento delle funzioni istituzionali (art. 18, comma 2 D.lgs. 196/03), al fine di adempiere a compiti ad essa attribuiti da leggi e regolamenti.

E' possibile effettuare trattamenti relativi a dati diversi da quelli sensibili e giudiziari anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente, fermo restando l'esercizio di funzioni istituzionali.

Le Aziende sanitarie, per le attività amministrative, anche se strumentali alle attività di prevenzione, diagnosi, cura e riabilitazione, trattano i dati sensibili in base al "*Regolamento per il trattamento dei dati personali sensibili e giudiziari di competenza della Regione, delle Aziende Sanitarie, degli enti e agenzie regionali, degli enti vigilati dalla Regione*" adottato dalla Regione Piemonte con D.P.G.R. 11 maggio 2006, n. 3/R e ss.mm.i..

Per quanto concerne il trattamento dei dati idonei a rivelare lo stato di salute per perseguire una finalità di tutela della salute o dell'incolumità fisica dell'interessato l'Azienda necessita del consenso di quest'ultimo preceduto da idonea informativa.

Nel caso in cui l'Azienda persegua finalità di tutela della salute o dell'incolumità fisica di un terzo o della collettività il trattamento viene effettuato sulla base dell'Autorizzazione generale rilasciata dal Garante per la protezione dei dati personali (cfr. Autorizzazione n. 2 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale).

I trattamenti (cfr. allegato A) effettuati dall'AZIENDA SANITARIA LOCALE ASL CN1 si possono suddividere nelle seguenti macro aree:

Tipologia di dati	Descrizione del trattamento
Trattamento di **dati idonei a rivelare lo stato di salute.**	Trattamento di dati per esecuzione delle obbligazioni di cui al **rapporto di cura e assistenza** richiesto. Acquisizione, consultazione, registrazione, aggiornamento dati su cartella clinica cartacea/elettronica o altra documentazione sanitaria. Comunicazione dei dati sanitari ai soggetti legittimati.
Trattamento di **dati personali** di tipo contabile e fiscale di fornitori, persone fisiche e giuridiche, pubbliche amministrazioni, enti e associazioni privati.	Acquisizione, consultazione, registrazione, aggiornamento, cancellazione dati contabili, fiscali relativi a soggetti che hanno o hanno avuto in qualche modo **rapporti anche economici** con l'Azienda.
Trattamenti di dati **personali/giudiziari** inerenti soggetti terzi che vengono a contatto con l'Azienda	Gestione del **contenzioso**
Trattamento di dati **personali/sensibili/giudiziari** relativi a dipendenti e professionisti.	Acquisizione, organizzazione e gestione delle risorse umane ed informative, finanziarie, patrimoniali e materiali – **Gestione del personale -**
Trattamento di dati **personali/sensibili/giudiziari** effettuato dal Servizio Informatica e Telecomunicazioni	**Predisposizione di misure di sicurezza** dei dati trattati e conservati su supporti informatici **Salvataggio e ripristino** di dati su supporti informatici. Funzioni di **Amministratore di sistema**

1.4 REQUISITI MINIMI D.LGS. 196/2003 ALLEGATO B

Nella seguente tabella è riportata la corrispondenza fra le misure richieste nell'allegato B al D.Lgs. 196/2003 e le misure indicate nel presente documento.

RIFERIMENTO ALL. B	MISURA ADOTTATA
Sistema di autenticazione informatica, p.ti 1-11	5.1 MISURE RELATIVE ALL'USO DELLE CREDENZIALI
Sistema di autorizzazione p.ti 12-14	5.2 MISURE RELATIVE ALLA GESTIONE UTENTI
Altre misure di sicurezza p.to 15	5.2 MISURE RELATIVE ALLA GESTIONE UTENTI
Altre misure di sicurezza p.ti 16, 17	5.4 PROTEZIONE CONTRO VIRUS INFORMATICI
Altre misure di sicurezza p.to 18	5.5 POLITICHE PER LA MEMORIZZAZIONE DELLE BANCHE DATI 5.6 POLITICHE DI GESTIONE DEI BACKUP
Ulteriori misure (dati sensibili o giudiziari) p.to 20	5.4 PROTEZIONE CONTRO VIRUS INFORMATICI

Ulteriori misure (dati sensibili o giudiziari) p.to 21	0 POLITICHE DI GESTIONE DEI SUPPORTI DI MEMORIZZAZIONE
Ulteriori misure (dati sensibili o giudiziari) p.to 23	6 CRITERI E MODALITA' PER IL RIPRISTINO DELLA DISPONIBILITA' DEI DATI IN SEGUITO A DISTRUZIONE O DANNEGGIAMENTO
Ulteriori misure (dati sensibili o giudiziari) p.to 24	9 SEPARAZIONE DEI DATI SANITARI

2. ELENCO DEI TRATTAMENTI DI DATI PERSONALI

L'elenco dei trattamenti di dati personali è contenuto nell'Allegato A e Abis.

3. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA'

Il **TITOLARE**[2] del trattamento dei dati personali è l'Azienda nel suo complesso rappresentata dal Commissario pro-tempore il quale esercita un potere decisionale del tutto autonomo sulle finalità e modalità del trattamento dati personali, salvo le deleghe rilasciate in conformità del D.Lgs 196/03.

Con Deliberazioni della Giunta Regionale nr. 6-2338 del 22.07.2011 e nr. 2-3185 del 27 dicembre 2011, è stato nominato Commissario – Legale rappresentante dell'ASL CN1 il Dr. Giovanni MONCHIERO con decorrenza dal 01.08.2011.

3.1 RESPONSABILI INTERNI

I RESPONSABILI[3] **interni** del trattamento dei dati sono i dirigenti e/o funzionari Direttori o Responsabili dei Dipartimenti, Distretti, Strutture Complesse – Strutture Semplici dell'A.S.L. CN1, delle seguenti aree di riferimento:

CODICE RESPONSABILE	AREA DI RIFERIMENTO
	DIREZIONALE – AMMINISTRATIVA
R01	Segreteria e sistema informativo direzionale
R02	Programmazione e politiche di budget
R03	Comunicazione e Bilancio sociale

[2] Art. 4, c. 1, lett. f) D.Lgs 196/2003; *"**titolare**: la persona fisica, la persona giuridica, la 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 e agli strumenti utilizzati, ivi compreso il profilo della sicurezza"*

[3] Art. 4, c. 1, lett. g) D.Lgs 196/2003; *"**responsabile**: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento"*

R04	Servizio Informatica e Telecomunicazioni
R05	Servizio Prevenzione e protezione
R06	Servizio Legale
R07	Direzione amministrativa dei Presidi Ospedalieri
R08	Dipartimento Amministrativo
R09	Dipartimento tecnico – logistico
R10	Dipartimento finanziario
R30	Servizio ispettivo e attività extra-istituzionali del personale
R31	Affari istituzionali
R37	Ufficio Stampa
	DIREZIONALE – SANITARIA
R11	Medicina Lavoro - Medico Competente
R12	Ufficio Qualità
R13	Psicologia
R32	Fisica Sanitaria
R33	Direzione delle professioni sanitarie e coordinamento servizio sociale aziendale
	TERRITORIALE
R14	Distretto di Cuneo – Borgo San Dalmazzo
R15	Distretto di Dronero
R16	Distretto di Mondovì
R17	Distretto di Ceva
R18	Distretto di Savigliano – Fossano
R19	Distretto di Saluzzo
R20	Servizio per le dipendenze patologiche
R21	Farmacia del Presidio Ospedaliero
R21bis	Farmacia Territoriale
R22	Medicina Legale
R23	Dipartimento di prevenzione
R24	Presidio Multizonale Profilassi e Polizia Veterinaria
R36	Unità di Valutazione e di Organizzazione dello Screening – UVOS
	OSPEDALIERA
R25	Sovraintendenza sanitaria dei presidi ospedalieri
R26	Direzione sanitaria di Presidio Savigliano – Saluzzo
R27	Direzione sanitaria di Presidio Fossano – Caraglio
R28	Direzione sanitaria di Presidio Mondovì - Ceva

R29	Cure palliative
R34	Dipartimento interaziendale di Salute Mentale
R35	Dipartimento Materno Infantile

Ogni anno il presente documento modifica tali nomine compatibilmente con il Piano di Organizzazione dell'Azienda ed evidenzia le istruzioni agli stessi impartite.

Detto elenco potrà essere aggiornato, sempre con provvedimento del Legale Rappresentante dell'Azienda, in seguito alle variazioni che interverranno nella normativa in materia di *privacy* o nel Piano di organizzazione dell'A.S.L. e della sua attuazione.

Per quanto concerne le competenze e le aree di pertinenza dei responsabili interni al trattamento dati personali, si richiama l'atto aziendale, approvato con Deliberazione del Direttore Generale n. 485 del 01/10/2010 e ss.mm.ii., il D.P.G.R. n. 3/R dell'11.05.2006 e ss.mm.i.i. avente ad oggetto il "*Regolamento per il trattamento dei dati personali sensibili e giudiziari di competenza della Regione, delle Aziende Sanitarie, degli Enti e Agenzie Regionali, degli enti vigilati dalla Regione*", ed in particolare l'Allegato A - Schede nr. 01 – 02 - 03 e l'Allegato B – Schede dal n. 1 a 41, nonché quanto previsto dal presente documento.

I Responsabili interni devono:

- fornire idonee garanzie del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza;
- attenersi scrupolosamente alle disposizioni previste dal D.Lgs 196/03 e ss.mm.ii., con particolare riguardo a quanto sancito dall'art. 11 e dal titolo V, in materia di "*trattamento dei dati personali in ambito sanitario"* della normativa anzi evidenziata;
- ottemperare alle istruzioni impartite dal Titolare anche con il "Documento programmatico sulla sicurezza dei dati personali" redatto annualmente dall'Azienda;
- segnalare al Direttore Generale le ditte esterne che per natura dell'attività svolta, in base a formale incarico, trattano dei dati personali di titolarità A.S.L. CN1 al fine di procedere alla loro nomina quali responsabili esterni al trattamento dati personali. Le suddette nomine e le eventuali revoche devono essere comunicate alla S.C. Servizio Legale;
- redigere ed aggiornare l'elenco dei responsabili esterni del trattamento afferenti alla propria area di competenza comunicandolo annualmente alla S.C. Servizio Legale;
- nominare gli incaricati esterni al trattamento dei dati personali che si inseriscono nei processi di trattamento dei dati nella struttura organizzativa e provvedere all'aggiornamento dell'elenco degli stessi;
- redigere annualmente la lista degli incaricati dipendenti e non che prestano la loro attività presso la struttura di cui la S.V. è responsabile del trattamento dei dati;
- incaricare per iscritto gli esercenti le professioni sanitarie diversi dai medici, che nell'esercizio dei propri compiti, intrattengono rapporti diretti con i pazienti comunicando loro dati personali idonei a rivelare lo stato di salute (art. 84 D.Lgs 196/2003);
- comunicare l'inizio di nuovi trattamenti di dati personali nonché la cessazione e la modifica dei trattamenti già in essere alla S.C. Servizio Legale al fine di garantire il continuo aggiornamento dell'anagrafe dei trattamenti di dati personali aziendali;

- verificare periodicamente l'esattezza e l'aggiornamento dei dati utilizzati presso ogni struttura organizzativa, nonchè la loro pertinenza, completezza non eccedenza e necessità rispetto alle finalità perseguite;
- mettere in atto tutte le misure necessarie e far rispettare ed applicare, nella struttura di propria pertinenza, la normativa ed i documenti sopra richiamati, da parte degli incaricati aziendali e non al trattamento dati personali;
- curare i rapporti con gli interessati che esercitano i diritti di cui all'art. 7 del D.Lgs 196/2003, avvalendosi della collaborazione della S.C. Legale.

3.2 RESPONSABILITA' DEL SERVIZIO INFORMATICA E TELECOMUNICAZIONI

Il responsabile del Servizio Informatica e Telecomunicazioni assicura, inoltre, l'ingegnerizzazione, la realizzazione e la gestione operativa della struttura informatica aziendale (hardware e software) nel rispetto delle misure di sicurezza del dato elettronico previste dalla normativa vigente (cfr. art. 45 Atto aziendale).

Il suddetto servizio ha altresì funzioni di "amministratore di sistema" (cfr. Provvedimento Garante per la protezione dei dati personali del 27.11.2008 *"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"*).

La S.C. Servizio Informatica e Telecomunicazioni, in particolare, ha fra i suoi compiti quelli di:

1. Abilitare e disabilitare l'accesso degli utenti alla rete dati aziendale (autenticazione)
2. Amministrare i diritti di accesso ai dati degli utenti (autorizzazione)
3. Effettuare copie di salvataggio dei dati e costudirle
4. Copiare, spostare o rimuovere dati dai dischi dei computer aziendali, secondo le necessità
5. Sviluppare o gestire applicazioni software che supportino trattamenti di dati personali e sensibili

Alcuni tecnici S.I.T. rientrano quindi nella figura di amministratore di sistema e dispongono di privilegi che consentono loro di accedere a tutti i dati aziendali, ma sono tenuti a maneggiare i dati esclusivamente al fine di garantire il funzionamento e la sicurezza dei sistemi a loro affidati.

3.3 AMMINISTRATORI DI SISTEMA

In ottemperanza al provvedimento del Garante del 27.11.2008, si allega (allegato D) l'elenco degli amministratori di sistema, suddiviso in due parti: Amministratori interni, dipendenti dell'ASL CN1 e ditte esterne che svolgono tale compito per conto dell'ASL CN1.

3.4 RESPONSABILI[4] ESTERNI.

I Responsabili esterni al trattamento dati personali sono gli enti, le società pubbliche o private e gli altri organismi che per natura dell'attività svolta, in base a formale incarico, operano in

[4] vedi nota 2

collaborazione con l'Azienda e, conseguentemente si inseriscono nei processi di trattamento dei dati di titolarità A.S.L. CN1.
Vengono nominati, su segnalazione dei responsabili interni, dal Direttore Generale all'atto del conferimento dell'incarico e/o della sottoscrizione del contratto.
La nomina deve essere comunicata alla S.C. Servizio Legale.
I responsabili esterni devono

- attenersi alle disposizioni previste dal D.Lgs 196/03 "Codice in materia di dati personali" e ss. mm.ii;
- rispettare ed applicare le misure di sicurezza idonee a salvaguardare la riservatezza. l'integrità e la completezza dei dati trattati, secondo quanto disposto dalla Parte Prima - Titolo V - del Codice sopra indicato e dal relativo allegato B;
- nominare con atto scritto gli incaricati del trattamento secondo le modalità previste dal D.Lgs 196/03;
- mettere in atto tutte le misure necessarie a far rispettare ed applicare, la normativa in questione, da parte degli incaricati aziendali al trattamento dati personali, previa loro formazione in materia;
- farsi autorizzare per la creazione di banche dati dal responsabile interno del trattamento dati del Servizio presso cui si esplica l'attività, se espletata presso la sede dell'Azienda, altrimenti dal titolare del trattamento;
- comunicare al Responsabile interno dei trattamenti dati personali nell'ambito della Struttura/Dipartimento in cui operano, i trattamenti di dati personali che risultino necessari al fine dell'adempimento del contratto, non previsti all'atto della sottoscrizione del medesimo;
- comunicare i dati personali di cui è titolare l'A.S.L. CN1 unicamente a dipendenti di quest'ultima addetti alle Strutture operative abilitate al trattamento di quei dati;
- comunicare "dati personali" al di fuori dell'Azienda esclusivamente solo se previamente autorizzati dal Titolare del trattamento dati nel rispetto della normativa citata;
- informare l'Azienda con frequenza annuale dell'adozione delle misure di sicurezza, in conformità a quanto indicato dal D.Lgs 196/2003, così da evitare rischi di distruzione e perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non necessario per l'espletamento dell'attività affidatagli ovvero inviare una copia del certificato di conformità rilasciato da chi ha curato la progettazione e l'attuazione delle misure minime di sicurezza, nel caso in cui il destinatario abbia affidato a soggetti esterni tali compiti;
- trasmettere al Titolare, non oltre le 24 ore successive dal loro ricevimento, le istanze, ex art. 7 D.Lgs 196/2003, inerenti il trattamento dei dati.

Le istruzioni impartite dal titolare ai responsabili con apposita nota scritta possono essere integrate in base allo specifico trattamento dei dati personali effettuato dai singoli responsabili.

Le nomine, ad oggi, comunicate alla S.C. Servizio Legale sono:

Descrizione sintetica dell'attività esternalizzata	**Trattamenti di dati interessati** **P = personali** **S = sensibili**	**Soggetto esterno**
Prenotazione attività Fisioterapia	P – S	A & C Sistemi s.r.l
Gestione dell'accettazione ospedaliera; Gestione della prenotazione sportello CUP e della gestione cassa di Savigliano, Fossano e Saluzzo	P – S	ACCENTURE S.p.A.
Cure palliative domiciliari per patologie	P –S	ADAS onlus

neoplastiche o degenerative		
Servizio di supporto alla gestione del servizio di radiodiagnostica del presidio ospedaliero di Fossano (cfr. Determinazione del Direttore dell'UOA Gestione acquisti, appalti e contratti dell'ex Asl 17 n. 279 del 10.03.2006)	P – S	ALLIANCE MEDICAL srl
Prot. 21058 del 05/05/09 Affidamento del servizio pluriennale di accoglienza-informazione accompagnamento pubblico, da attuarsi nei presidi ospedalieri dell'Asl CN1 siti in Mondovì, Ceva e Saluzzo; sorveglianza-gestione della sicurezza interna - primo intervento da attuarsi nel presidio ospedaliero dell'Asl CN1 sito in Mondovì (Delibera del Direttore Generale 2080 del 30.10.2008); Affidamento del servizio di supporto all'attività sanitaria dell'ASL CN1 – che consiste nello svolgimento da parte di personale O.S.S. delle attività alberghiere relative alla degenza, compresi l'assistenza ai degenti per la loro igiene personale, il trasporto di materiale vario, la pulizia e la manutenzione di utensili ed apparecchiature – (Delibera del Direttore Amministrativo n. 7 del 14.01.2009 e n. 709 del 29.12.2010); Affidamento del servizio di veicolazione e distribuzione pasti nel nuovo Presidio Ospedaliero di Mondovì; veicolazione ferri chirurgici, provette ed altro materiale sanitario compreso quello farmaceutico (Delibera del Direttore Generale 283 del 17.02.2009; 709 del 29.12.2010 e 36 del 31.01.2011); Affidamento della gestione dei servizi di assistenza socio sanitaria residenziale per anziani non autosufficienti nei nuclei RSA –RAF della casa di riposo di Racconigi (Delibera del Direttore Generale n. 290 del 17/02/2009); Affidamento del servizio pluriennale di ricezione e gestione delle richieste di trasporto provenienti dalle strutture dell'ASL CN1 verso le associazioni di volontariato convenzionate (Delibera del Direttore Amministrativo n. 360 del 10/03/09),	P- S	AMOS s.c.r.l.

Affidamento del servizio annuale di gestione delle camere mortuarie nei presidi dell'ASL CN1 (Delibera del Direttore Generale n. 511 del 30.03.2009 e 709 del 29.12.2010); Affidamento del servizio logistico di movimentazione materiale vario presso i presidi dell'ASL CN1 (Delibera del Direttore Generale 537 del 31/03/09 e 709 del 29.12.2010); Affidamento del servizio di Barellaggio (operatori tecnici) Delibera 536 del 31.03.2009 e 709 del 29.12.2010 Attività amministrativa presso DEA/PS Mondovì, Savigliano (delibera 714 del 27-05-2009) Attività amministrativa presso Laboratori di Analisi Savigliano, Saluzzo, Fossano, Mondovì Ceva e Borgo S. Dalmazzo (delibera 826 del 30-06-09); Affidamento del servizio pluriennale di Call center, Programmazione , screening e gestione agende UVOS a livello provinciale (Delibera del Direttore Generale 8 del 14.01.09; Delibera 572 del 16.04.09); Affidamento del servizio di ricezione, gestione e conservazione relativo all'archivio amministrativo e sanitario per l'Asl CN1 per un periodo di 10 anni a partire 01.01.2010 Delibera Direttore Generale 1112 del 29.12.2010; Affidamento del servizio di gestione degli ausili della protesica (delibera 709 del 29.12.2010); Affidamento gestione ambulatori della libera professione ASL CN1 e ASO S. Croce e Carle in Cuneo (delibere n. 212 del 22.04.2010 e n. 231 del 14.05.2010)		
Screening del cancro del colon retto Deliberazione del Direttore Generale 995 del 02.09.09	P-S	ASSOCIAZIONE TITOLARI DI FARMACIA DELLA PROVINCIA DI CUNEO
Attività di volontariato finalizzata a promuovere la salute e la riabilitazione sociale dei diabetici	P- S	ASSOCIAZIONE DIABETICI Savigliano – Fossano – Saluzzo
Gestione informatizzata dei servizi radiologici (p@ris) di Savigliano	P – S	ATS TECNOLOGIE S.r.l. (ex TEINOS s.r.l.)
Software Quani SDO, Quani PA e Quani SID	P – S	BIM Italia s.r.l.
Gestione dell'attività infermieristico territoriale – SAOADI	P – S	BITELO di Lonni Gualtiero & C. s.a.s.

Gestione sportelli unici socio-sanitari	P-S	CADMO INFOR srl
Fornitura di un sistema gestionale di archiviazione e trasmissione immagini digitali e informatizzazione dei servizi radiologici del presidio	P-S	CARE STREAM HEALTH Italia s.r.l.
Prestazioni di assistenza infermieristica	P-S	CASA DI RIPOSO "S. CUORE"
Prestazioni di assistenza infermieristica	P – S	CASA DI RIPOSO CAV TOSELLI
Prestazioni di assistenza infermieristica	P – S	CASA DI RIPOSO DON DALMASSO
Prestazione assistenza infermieristica – Provv. 484/08	P – S	CASA DI RIPOSO ISTITUTO IMBERTO GRANDIS
Prestazioni amministrative	P - S	CASA DI RIPOSO RIBERI
Servizio di sorveglianza dosimetrica e concentrazione radon indoor	P - S	CENTRO PROTEXIMETRICO PIEMONTESE C.P.P. S.R.L.
Attività di riabilitazione odontoiatrica	P - S	CONSORZIO ODONTOTECNICI LIGURE
Utilizzo personale OSS – provv. 1397/08	P - S	CONSORZIO SOCIO ASSISTENZIALE VALLI GRANA E MAIRA – DRONERO
Trasporti interospedalieri e trasporti protetti	P – S	CROCE BIANCA DI FOSSANO
Servizio trasporto sanitario di emergenza 118	P - S	CROCE VERDE SALUZZO
Anagrafe provinciale assistiti	P	DATA PROCESSING SPA
Servizio di manutenzione software per i sistemi relativi a Gestione Laboratorio Analisi, Gestione Screening mammografico e citologico, Gestione vaccinazioni e anagrafica (Giotto), Gestione flussi dati ricoveri (Argos)	P - S	DEDALUS S.P.A.
Software ELIOT per la gestione del Centro Trasfusionale di Savigliano; Software WINSAP per la gestione dell'Anatomia Patologica di Savigliano	P – S	ENGINEERING SANITA' ENTI LOCALI S.p.A.
Recupero crediti	P –S	EQUITALIA s.p.a
Recupero crediti	P –S	EQUITALIA NORD spa
Screening mammografico "Prevenzione Serena" – provv. 1285 del 30.06.08		ERAD - Torino
Gestione logistica dei farmaci, dei materiali sanitari, economali e di consumo – provv. 1516/08		EUMED srl
Screening del cancro del colon retto Deliberazione del Direttore Generale 995 del 02.09.09	P-S	FARMACIA MANASSERO DANIELA – Margarita
Screening del cancro del colon retto Deliberazione del Direttore Generale 995 del 02.09.09	P-S	FARMACIA PICCITTO UMBERTO - Robilante
Screening del cancro del colon retto Deliberazione del Direttore Generale	P-S	FARMACIA SACRO CUORE dI Bra

995 del 02.09.09		
Screening del cancro del colon retto Deliberazione del Direttore Generale 995 del 02.09.09	P-S	FARMACIE COMUNALI n. 1-2-3 – Cuneo
Software per la gestione dell'attività della Medicina del Lavoro	P – S	FREESOFT sas
Recupero crediti	P-S	GEC
Software per la gestione dell'Anagrafe Aziendale; Software per la gestione del DEA di Savigliano e Mondovì; Software per la gestione del sistema informativo amministrativo contabile; Software per la gestione del CUP Provinciale, Accettazione e Cassa a Mondovì e Cuneo	P-S	GPI s.p.a.
Software per la gestione della reportistica unificata	P	INNOVO s.a.s.
Realizzazione software per la gestione delle cartelle cliniche nefrologiche	P - S	INFOGRAMMA s.r.l
Registrazione ed elaborazione delle ricette farmaceutiche	P-S	INTERDATA s.r.l.
Attività di riabilitazione odontoiatrica	P-S	LABORATORI ODONTOTECNICI Castellano Ivano e Crosio Daniele; Arnaudo Claudio e Peirano Silvio; Ghigo Bruno; Garnero Stefano; Postiglioni Paolo; Giuria Gabriele; Forti & Seoni; Gallarate & Somà; Giusta Andrea; Greguoldo & C**;** Schelenova di Valenti Paola & C
Assistenza sistemistica	P-S	LANSERVICE s.r.l.
Fornitura in noleggio di presidi antidecubito	P - S	MEDI-FM_SERVICE s.r.l.
Sistema di gestione del Centro Trasfusionale di Mondovì	P – S	MESIS s.r.l.
Sistema informatizzato di gestione del personale	P – S	MONDO EDP s.r.l.
Inserimento ricette veterinarie sul sistema informatizzato della Regione P.te	P	CONSORZIO NUOVI ORIZZONTI scs srl
Software per la gestione del datawarehouse sanitario	P-S	OSLO s.r.l.
Servizio di invio e comunicazioni destinate agli utenti Screening Prevenzione serena	P – S	POSTEL spa
Gestione informatizzata della Centrale Operativa 118 – NPI NET	P – S	REGOLA s.r.l.
Servizio di imbustamento e invio comunicazione destinate agli utenti		SELECTA s.p.a.
Registrazione ed elaborazione dei dati contenuti nelle prescrizioni	P - S	S2i ITALIA

farmaceutiche		
Manutenzione software di gestione posta elettronica	P - S	STUDIO STORTI S.r.l.
Software per la gestione della cartella Ostetrico-ginecologica	P – S	TESI IMAGING S.r.l.
Software per la gestione del protocollo e delle delibere	P - S	VALUE TEAM S.p.A. (accorpato Etnoteam s.p.a.)
Noleggio di presidi antidecubito		KCI Medical s.r.l.
Servizio di controllo dosimetrico ambientale e del personale sottoposto a radiazioni ionizzanti	P - S	X – GAMMAGUARD
Servizio di assistenza tecnica e manutenzione delle apparecchiature sanitarie in dotazione alle strutture ospedaliere e sanitarie	P-S	SIEMENS s.p.a.
Servizio di assistenza tecnica e manutenzione delle apparecchiature sanitarie in dotazione alle strutture ospedaliere e sanitarie	P-S	EUROCOLUMBUS s.r.l.
Servizio di assistenza tecnica e manutenzione delle apparecchiature sanitarie in dotazione alle strutture ospedaliere e sanitarie	P-S	Ge HEALTHCARE
Servizio di assistenza tecnica e manutenzione delle apparecchiature sanitarie in dotazione alle strutture ospedaliere e sanitarie	P-S	BIOMEDIN
Servizio di assistenza tecnica e manutenzione delle apparecchiature sanitarie in dotazione alle strutture ospedaliere e sanitarie	P-S	CAREFUSION HEALTH 237
Servizio di assistenza tecnica e manutenzione delle apparecchiature sanitarie in dotazione alle strutture ospedaliere e sanitarie	P-S	ESAOTE
Servizio di assistenza tecnica e manutenzione delle apparecchiature sanitarie in dotazione alle strutture ospedaliere e sanitarie	P-S	HORIBA
Servizio di assistenza tecnica e manutenzione delle apparecchiature sanitarie in dotazione alle strutture ospedaliere e sanitarie	P-S	MAQUET
Servizio di assistenza tecnica e manutenzione delle apparecchiature sanitarie in dotazione alle strutture ospedaliere e sanitarie	P-S	TECNOMEDICA
Servizio di assistenza tecnica e manutenzione delle apparecchiature sanitarie in dotazione alle strutture ospedaliere e sanitarie	P-S	VIGLIA

Servizio di assistenza tecnica e manutenzione delle apparecchiature sanitarie in dotazione alle strutture ospedaliere e sanitarie	P-S	CARL ZEISS

Sono incaricati al trattamento[5]:

- tutti i dipendenti;
- tutti i consulenti aziendali;
- tutti i liberi professionisti con cui l'Azienda intrattiene rapporti ed in generale tutti coloro con cui l'ASL instaura rapporti di lavoro di qualunque tipo, dipendente o autonomo, anche non retribuito o onorario o a tempo parziale o temporaneo, od altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato;
- tutte le ditte esterne che per la natura dell'attività svolta si inseriscono in processi di trattamento dei dati o possano venire a conoscenza, per le mansioni affidate, di dati oggetto del presente regolamento, se chi effettua il trattamento è una persona fisica.

I dipendenti possono trattare, esclusivamente per lo svolgimento delle funzioni istituzionali, i soli dati che affluiscono alla Struttura cui sono addetti. I rispettivi ambiti di trattamento sono individuati nel D.P.G.R. n. 3/R dell'11.05.2006 e ss.mm.i.i. avente ad oggetto il "*Regolamento per il trattamento dei dati personali sensibili e giudiziari di competenza della Regione, delle Aziende Sanitarie, degli Enti e Agenzie Regionali, degli enti vigilati dalla Regione*", nell'atto aziendale (cfr. Determinazione Direttore Generale n. 485 del 01/10/2010) e nel presente Documento Programmatico di Sicurezza.
Per quanto concerne gli altri incaricati l'ambito di trattamento agli stessi consentito è esclusivamente quello necessario per il raggiungimento delle finalità indicate nel contratto dagli stessi sottoscritto.

Le istruzioni impartite agli incaricati dall'Azienda sono allegate al presente documento (allegati B e C).

4. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

La seguente tabella riporta una classificazione dei rischi, secondo le indicazioni del Garante (Guida operativa per redigere il Documento programmatico sulla sicurezza (DPS)), corredata dall'indicazione di una stima di impatto sulla sicurezza dei dati, in "*relazione alla rilevanza e alla probabilità stimata dell'evento (anche in termini sintetici: es., alta/media/bassa)*". Nella colonna "Misure" è inoltre indicato un riferimento al paragrafo in cui sono descritte le misure intraprese a protezione dei rischi.

[5] Art. 4, c. 1, lett. h) D.Lgs 196/2003; *incaricati: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;*

Categoria	Rischi	Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)	Misure
Comportamenti degli operatori	sottrazione di credenziali di autenticazione	B – Può comportare la corruzione di un insieme ristretto di dati	5.2 MISURE RELATIVE ALLA GESTIONE UTENTI
	carenza di consapevolezza, disattenzione o incuria	B	5.1 MISURE RELATIVE ALL'USO DELLE CREDENZIALI 5.6 POLITICHE DI GESTIONE DEI BACKUP 7 INTERVENTI FORMATIVI E INFORMATIVI
	comportamenti sleali o fraudolenti	B	7 INTERVENTI FORMATIVI E INFORMATIVI 5.2 MISURE RELATIVE ALLA GESTIONE UTENTI 5.6 POLITICHE DI GESTIONE DEI BACKUP
	errore materiale	B	5.6 POLITICHE DI GESTIONE DEI BACKUP
Eventi relativi agli strumenti	azione di virus informatici o di programmi suscettibili di recare danno	M – Possono bloccare il funzionamento dei sistemi anche per giorni	5.4 PROTEZIONE CONTRO VIRUS INFORMATICI
	spamming o tecniche di sabotaggio	M	5.4 PROTEZIONE CONTRO VIRUS INFORMATICI
	malfunzionamento, indisponibilità o degrado degli strumenti	M – Può comportare da pochi minuti a più giorni di indisponibilità dei dati	5.3 MISURE RELATIVE AGLI STRUMENTI
	accessi esterni non autorizzati	M	5.3.2 Misure adottate nelle sale server
	intercettazione di informazioni in rete	B	5.3.4 Infrastrutture di rete
Eventi relativi al contesto	accessi non autorizzati a locali/reparti ad accesso ristretto	B	5.1 MISURE RELATIVE ALL'USO DELLE CREDENZIALI 5.2 MISURE RELATIVE ALLA GESTIONE UTENTI 5.3.2 Misure adottate nelle sale server
	sottrazione di strumenti contenenti dati	B	5.3.2 Misure adottate nelle sale server

			5.6 POLITICHE DI GESTIONE DEI BACKUP
	eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc.), nonché dolosi, accidentali o dovuti ad incuria	B	5.6 Politiche di gestione dei guasti 5.6 PROTEZIONE CONTRO VIRUS INFORMATICI Situazione ambientale
	guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)	B	5.3.6.4 Guasto ai sistemi complementari
	errori umani nella gestione della sicurezza fisica	B	5.3.6.5 Errori umani

5. MISURE PER GARANTIRE L'INTEGRITA' E LA DISPONIBILITA' DEI DATI NONCHE' LA SICUREZZA DEI LOCALI CHE LI CONTENGONO

5.1 MISURE RELATIVE ALL'USO DELLE CREDENZIALI

Gli operatori incaricati dei trattamenti sono stati istruiti, sia direttamente, tramite eventi formativi, sia dai propri responsabili, sulla normativa e sulla necessità di mantenere riservate le proprie credenziali di accesso.

Il sistema di autenticazione utilizzato è basato sull'uso di password. Le *credenziali di autenticazione* consistono in un codice per l'identificazione dell'incaricato (nel seguito detto anche *username*) associato a una *parola chiave* riservata conosciuta solamente dal medesimo (nel seguito detta anche *password*).
Nelle istruzioni impartite agli incaricati, è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale.
Ad ogni incaricato sono assegnate individualmente una o più credenziali per l'autenticazione. Esistono credenziali generiche, utilizzate per ragioni pratiche-organizzative da più operatori, ma non hanno alcun permesso sulle risorse di rete; il loro unico scopo è consentire l'accesso alla postazione di lavoro (e non l'accesso ai trattamenti).
Per tutti i domini sono attivate le seguenti regole:

- *Regola di lunghezza*: la password deve essere composta almeno da otto caratteri;
- *Regola di scadenza*: il sistema richiede il cambio della password ogni tre mesi;
- *Regola di unicità*: durante il cambio della password, il sistema rifiuta l'inserimento delle ultime quattro password inserite;
- *Regola di blocco*: il sistema blocca indefinitamente l'account dopo cinque tentativi falliti consecutivi di login;

Tali regole sono automaticamente valide per l'accesso a quegli applicativi per i quali il sistema di autenticazione è già stato integrato con quello del dominio di rete.
Per tutto quanto riguarda gli applicativi che non hanno un sistema di autenticazione integrato, si rimanda alle esplicite dichiarazioni delle ditte fornitrici.

Il codice per l'identificazione non può essere assegnato ad altri incaricati, neppure in tempi diversi. Pertanto si dispone che ogni utente definito nel dominio non venga più cancellato, ma disabilitato nel caso cessi di essere in uso, in maniera tale da evitarne il riutilizzo (D.L. 196/2003 Allegato B, punti 6).
Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;
Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

Attualmente, nel caso dei trattamenti i cui applicativi non siano già integrati con il sistema di autenticazione del dominio di rete, i controlli di accesso previsti sono a due livelli:

- Autenticazione di rete: l'utente per poter lavorare deve connettersi alla rete dati aziendale ed autenticarsi fornendo le proprie credenziali (utente-password) di rete. Questa fase è gestita utilizzando la procedura di autenticazione di dominio del sistema operativo Microsoft Windows 2003, con password a scadenza trimestrale.

- Autenticazione applicativa: l'utente, per poter accedere ad un applicativo ed ai relativi dati deve autenticarsi fornendo ulteriori credenziali, proprie dell'applicativo. In questo modo si garantisce che ogni utente possa accedere alle sole procedure e dati di propria competenza. Anche in questo caso le password hanno scadenza trimestrale.

5.2 MISURE RELATIVE ALLA GESTIONE UTENTI

Attualmente la rete informatica dell'ASL CN1 è suddivisa in 3 domini indipendenti ed interconnessi, risultanti dalle 3 ex ASL 15, 16 e 17.
Ogni utente ha, tramite il proprio profilo, diritto di accesso a determinate aree dati condivise di competenza per la propria attività, mentre tutte le altre aree sono a lui precluse.

5.3 MISURE RELATIVE AGLI STRUMENTI

5.3.1 Collocazione dei server e degli apparati di rete

La struttura logistica del sistema informatico dell'Azienda si basa su 3 macro-aree, i cui centri sono Cuneo, Mondovì e Savigliano, risultanti dall'accorpamento delle ex ASL 15, 16 e 17. Sono in corso attività di integrazione, standardizzazione ed aggiornamento tecnologico, anche al fine di migliorarne la sicurezza.

Ognuna di queste macro-aree prevede dei centri principali, delle sedi periferiche intermedie e delle sedi periferiche minori. Tipicamente i centri principali hanno una infrastruttura informatica importante, con cablaggio strutturato diffuso in tutti i locali ed una sala server attrezzata, mentre le altre sedi possono avere una infrastruttura locale oppure, come per le sedi minori, soltanto le postazioni di lavoro e la rete aziendale.
Va comunque tenuto conto che le maggiori quantità di dati aziendali sensibili si concentra nelle 3 sedi principali, in quanto ivi risiedono i database dei sistemi centralizzati.

La seguente tabella fornisce una visione generale della localizzazione dei dati.

AREA	SEDE	LIVELLO	DATI	LOGISTICA E MISURE DI SICUREZZA
Cuneo	via Boggio	Sede Centrale - Direzione	Sistemi Amministrativi, Sanitari – Territoriali Dati e documenti operativi dei servizi	Sala server Porta tagliafuoco Condizionamento Rilevazione temperatura Gruppi di continuità Gruppo elettrogeno Rilevazione fumi Telecamera
	Villa S. Croce	Sede secondaria	Dati e documenti operativi dei servizi	Sala server Porta tagliafuoco Condizionamento Gruppi di continuità Gruppo elettrogeno Rilevazione fumi Telecamera
	Borgo S. Dalmazzo Poliambulatorio	Sede periferica	Dati e documenti operativi dei servizi	Sala server Porta tagliafuoco Condizionamento Gruppi di continuità Sistema antincendio
	Caraglio	Sede periferica	Dati e documenti operativi dei servizi	Ufficio Gruppo di continuità
	Busca	Sede periferica	Dati e documenti operativi dei servizi	Locale apposito Gruppo di continuità
	Borgo S. D. Servizio Multizonale	Sede periferica	Dati e documenti operativi dei servizi	Locale apposito Gruppo di continuità
Mondovì	Nuovo Ospedale Mondovì	Sede Ospedaliera primaria	Sistemi ospedalieri Anagrafe aziendale assistiti	Sala server Porta tagliafuoco Condizionamento Rilevazione temperatura Gruppi di continuità Gruppo elettrogeno Sistema antincendio Accesso controllato tramite badge
	Ospedale Ceva	Sede Ospedaliera primaria	Dati e documenti operativi dei servizi	Locale Server Porta tagliafuoco Condizionamento Gruppi di continuità Gruppo elettrogeno
	Edificio Gazzera	Sede distretto Mondovì	Dati e documenti operativi dei servizi	Sala server Gruppo di continuità Gruppo elettrogeno
Savigliano	Ospedale Savigliano	Sede Ospedaliera primaria	Sistemi ospedalieri	Sala server Condizionamento Gruppi di continuità

				Gruppo elettrogeno
	Ospedale Saluzzo	Sede Ospedaliera primaria	Solo postazioni e rete	Locale tecnico server Porta tagliafuoco Condizionamento
	Ospedale Fossano	Sede Ospedaliera primaria	Solo postazioni e rete Dati veterinaria	Sala server

In tali sedi sono situati tutti i server che ospitano dati e programmi utilizzati all'interno dell'azienda.

5.3.2 Misure adottate nelle sale server

Le sale server non sono presidiate da personale. Per garantire la sicurezza, l'ingresso alle sale server è protetto da una porta tagliafuoco o metallica, chiusa a chiave. Le chiavi sono custodite presso il Servizio Informatica ed il Servizio Tecnico. Nel caso debba accedervi personale estraneo ai due servizi, esso deve essere identificato ed accompagnato dal personale S.I.T..

In alcune sedi intermedie sono stati installati server per memorizzare localmente i documenti di lavoro degli utenti, migliorando la velocità e agevolando il salvataggio dei dati. Tali server sono stati sistemati in locali appositi oppure in uffici, dove sono custoditi durante le ore di servizio dal personale operante all'interno della struttura, mentre durante le ore notturne i relativi locali rimangono chiusi a chiave ed, in qualche caso, protetti dal sistema di allarme della struttura in cui sono ubicati.

Al fine di garantire la sicurezza dei dati all'interno delle sale server sono state applicate le seguenti misure di sicurezza (non presenti in tutti i locali server):

- mantenimento delle condizioni di temperatura operative, ove necessario mediante impianti di condizionamento o raffrescamento;
- rilevazione e monitoraggio della temperatura;
- protezione dei locali con sistema di allarme e sistema antincendio o di rilevazione fumi;
- revisione degli impianti elettrici e predisposizione a norma di legge con adeguate protezioni impiantistiche;
- installazione di gruppi di continuità (UPS) in grado di garantire agli operatori e/o ai sistemi automatici il tempo necessario per l'espletamento delle operazioni di shut-down anche in caso di black-out totale;
- linea elettrica privilegiata, con gruppo elettrogeno (GE) in grado di alimentare i gruppi di continuità presenti nella sala server e permettere la prosecuzione dell'attività anche in caso di black-out totale.

In linea generale i server e le apparecchiature correlate sono installate in appositi armadi metallici (rack), con collegamenti a regola d'arte, che consentono una elevata stabilità ed affidabilità dei sistemi nel loro insieme.

Al di fuori delle sale e locali server, esistono armadi in cui sono contenute le apparecchiature di rete e le interconnessioni della rete locale di edificio. In generale le apparecchiature possono essere posizionate in appositi locali tecnici dedicati oppure in locali condivisi con altri servizi o nei corridoi. Nei casi in cui non è possibile impedire l'accesso alla zona dell'armadio (corridoi), tale armadio è mantenuto chiuso a chiave.

5.3.3 Caratteristiche di ridondanza e protezione degli apparati

Tutti i server in uso in azienda, con particolare riferimento a quelli su cui sono memorizzati dati sensibili, presentano caratteristiche di ridondanza e fault tolerance, fra le quali:

- Alimentatore ridondato; nella maggior parte dei casi anche sostituibile a caldo;
- Doppia scheda di rete; in alcuni casi, anche in configurazione di load-balancing e fault-tolerance;
- Sottosistema di dischi in configurazione di sicurezza RAID (con la possibilità di sostituire "a caldo" il disco danneggiato), che consente alle macchine di continuare ad operare normalmente pur in presenza di un guasto ad uno dei dischi, senza perdita di dati.

Negli ultimi anni è stata introdotta la tecnologia di “Virtualizzazione” dei server, basata su tecnologia VMware, che consente di svincolare i server virtuali dall’hardware del server fisico su cui stanno eseguendo. Questa tecnologia permette quinidi, in caso di guasto hardware di un server fisico, di far immediatamente ripartire i server virtuali che lo stavano utilizzando su un altro server, a patto che questo abbia sufficienti risorse libere. Questa funzionalità consente di minimizzare il tempo di indisponibilità del server e delle applicazioni che su di esso si basano.

Per quanto concerne la memorizzazione dei server virtuali e dei dati degli applicativi, si è fatto uso di apparati di tipo Storage Area Network (SAN), le cui caratteristiche di affidabilità, ridondanza e resistenza ai guasti sono paragonabili, se non superiori, a quelle dei server. In particolare, si riportano alcune delle principali caratteristiche:

- Alimentatore ridondato (doppio), sostituibile a caldo.
- Collegamento con i server mediante cavi in fibra ottica con tecnologia Fiber Channel.
- Doppio switch ottico per Fiber Channel.
- Doppio percorso fra server e SAN.
- Doppio controller di sistema (Storage Processor).
- Dischi in architettura ridondante (RAID 5), con unità di scorta (Hot Spare) che, in caso di guasto di un disco, può subentrare ripristinando la piena funzionalità nel minimo tempo necessario alla rigenerazione dei dati.

5.3.4 Infrastrutture di rete

Le infrastrutture di rete consentono il collegamento di tutte le unità elaborative del sistema informativo e sono quindi diffuse in tutta l’azienda. L’architettura di rete è basata sulla tecnologia MPLS fornita da Fastweb (Provider), che consente l’interconnessione diretta di ogni sede con tutte le altre.
Il Provider ha fornito i collegamenti richiesti in modalità VPN, in modo da garantire alla rete aziendale l’isolamento dal traffico esterno.
Per le sedi principali (vedi sotto) sono stati previsti collegamenti “ad elevata affidabilità”, che prevedono una linea principale ed una di backup (riserva), da utilizzare in caso di guasto della prima.
Nel corso del 2010 sono stati attivati i collegamenti in fibra ottica per le 3 principali sedi, con linea di riserva su rete alternativa.

I vari livelli sono interconnessi mediante router, mentre, a livello locale, la rete viene distribuita ai singoli utenti mediante switch e hub, utilizzando lo standard Ethernet ed il protocollo TCP/IP.

5.3.5 Protezione della rete aziendale da accessi esterni

Per quanto concerne la connessione della rete dati con reti esterne, sono attivi i seguenti collegamenti:

- Il collegamento con la rete regionale RUPAR
- Il collegamento con Internet

Ogni sede principale (Cuneo, Savigliano e Mondovì) dispone localmente, ad oggi, di entrambi i collegamenti con l'esterno sopra descritti. La rete aziendale interna è protetta da accessi indesiderati dall'esterno mediante firewall, posizionati nelle suddette sedi, sui quali è attivato un sistema di monitoraggio di tutte le connessioni in ingresso.
I firewall attualmente in uso sono dotati di vari sistemi per l'analisi dei dati: Intrusion Detection, Intrusion Prevention, Application Layer Filtering, Web-content filtering, Anti-spam. E' inoltre possibile analizzare il log delle connessioni effettuate ai fini di identificare eventuali anomalie ed eventualmente modificare la programmazione del firewall stesso.
Il firewall consente di realizzare una DeMilitarizedZone (DMZ), che di fatto separa la rete aziendale dai server "esposti" verso Internet (es. sito Web). In questo modo, eventuali attacchi diretti al sito Internet non possono causare accessi indesiderati ai server centrali.
Il firewall stesso consente anche di realizzare delle connessioni VPN (Virtual Private Network), che consentono di collegarsi alla rete da un computer posto all'esterno (tipicamente da Internet), in modalità sicura, proteggendo i dati trasmessi mediante crittografia. Questo consente ai fornitori di software, coi quali è stato stipulato un contratto di manutenzione, di accedere rapidamente ed in sicurezza alla rete dati aziendale dall'esterno utilizzando un collegamento via Internet, per effettuare interventi di manutenzione. Il firewall provvede a restringere l'accesso ai soli sistemi di competenza di ogni fornitore.
Per quanto concerne il sistema di posta elettronica, esso è accessibile, per comodità degli utenti, anche da Internet, in modalità web, senza necessità della VPN. In questo caso però si utilizza il protocollo "https", che introduce uno strato di sicurezza, crittografando i dati trasmessi.

5.3.6 Politiche di gestione dei guasti

In funzione della sensibilità del sistema alla tolleranza ai guasti, sono state definite una serie di misure che coinvolgono le tre componenti di un sistema di elaborazione distribuita: client, server e rete di comunicazione, locale o geografica.

5.3.6.1 *Guasto del client*

In generale, guasti alla componente client non comportano gravi problemi in quanto la sua sostituzione è più immediata e garantita dall'intervento del personale del Servizio Informatica, oltre che dal contratto di manutenzione sulle attrezzature client.

5.3.6.2 *Guasto del server*

Nonostante le misure di tutela fisica e di ridondanza hardware citate in precedenza, sono state previste delle misure per il ripristino o sostituzione del server guasto in tempi ridotti.

In linea generale tutte le attrezzature server sono coperte da contratto di manutenzione dedicato direttamente con la casa produttrice, con tempi di riparazione del guasto che vanno dalle 4 ore lavorative al giorno lavorativo successivo, a seconda della criticità del server.

Per tutti i server dedicati al sistema RIS/PACS dell'Ospedale di Mondovì, è stata prevista un'apposita procedura di ripristino del guasto. Si rimanda a tal proposito ai documenti denominati "Flusso di lavoro PACS v. 2.0", "Flusso di lavoro RIS v. 2.0", "Flusso di lavoro Reparti v. 2.0", tutti consultabili sul sito interno http://webradiologia nella sezione "Manuali".

Per i server dedicati al sistema del Laboratorio Analisi di Mondovì, essendo ospitati all'interno di una infrastruttura di Storage Area Network, le garanzie di sicurezza e disponibilità sono, come già detto predentemente molto elevate. In ogni caso, è state implementata un'architettura applicativa di "Mutual Take Over", in cui ciascuna componente software del sistema è installata su due server e quindi è possibile, in breve tempo, garantire il ripristino della piena operatività anche in caso di guasto di una componente hardware.

Per tutti i server più recenti, situati nelle sale server di Cuneo Via Boggio, Ospedale Mondovì e Ospedale Savigliano, sui quali eseguono applicativi strategici per l'azienda, è stata adottata la tecnologia di virtualizzazione VMware, che consente, in caso di guasto hardware di un server fisico, di riavviare immediatamente l'applicativo su di un altro server fisico.

Per alcuni di essi, quale ad esempio il CUP, è stata realizzata un'architettura "cluster", che consente di proseguire, in caso di guasto, con un sistema di backup identico al sistema primario.

5.3.6.3 *Guasto della rete di comunicazione*

L'infrastruttura di rete geografica (WAN) comprende una serie di collegamenti, alcuni dei quali sono ridondati, almeno per le sedi principali. Tali sedi sono collegate mediante linee in fibra ottica con linea di riserva a 8Mbps.

I restanti collegamenti sono realizzati mediante linee con capacità variabile a seconda del traffico e della zona geografica coperta (linee HDSL da 2 a 8 Mbps, ADSL, wireless 3 Mbps).

Per quanto riguarda le apparecchiature di rete, valgono i seguenti principi generali:

- i router sono di posseduti, gestiti e mantenuti dai provider delle connessioni (Fastweb per collegamenti su rame, BBBell per i collegamenti via radio), secondo opportuni livelli di servizio prestabiliti.
- gli switch sono invece di proprietà dell'A.S.L. CN1, per cui, considerato il tasso di guasto molto basso, vengono mantenuti alcuni apparati e componenti di scorta per la sostituzione rapida del pezzo guasto. Per alcuni switch centro stella è stato anche attivato il contratto di manutenzione.
- Il firewall della sede di Cuneo è costituito da una coppia di apparati con funzione di High Availability, con la quale uno dei due apparati ha ruolo di primario e gestisce il traffico, mentre l'altro funge da "riserva calda" ed in caso di guasto sostituisce il primario.

5.3.6.4 *Guasto ai sistemi complementari*

Gli impianti elettrici sono tutti realizzati secondo le normative vigenti. In caso di guasti agli impianti elettrici esiste la struttura interna Servizio Tecnico, i cui tecnici sono in grado di intervenire in tempi brevi per ripristinare il funzionamento. L'utilizzo generalizzato di UPS per gli apparati centrali come i server consente comunque alcuni minuti di autonomia tali da superare senza interruzione di servizio guasti di breve durata.
Gli impianti di condizionamento delle sale server principali sono stati realizzati con ampio margine e con apparecchiature ridondate, tali da poter supplire ad eventuali guasti di uno dei componenti.

5.3.6.5 *Errori umani*

I dipendenti sono formati sul funzionamento delle apparecchiature e dei programmi da loro utilizzati mediante specifici corsi-giornate formative. I tecnici di manutenzione sono addestrati sulle manovre da effettuare per non danneggiare le apparecchiature o comunque non generare guasti.

5.3.6.6 *Malfunzionamenti software*

Analogamente a quanto previsto per le attrezzature hardware, anche per il software, per i sistemi più critici, sono stati stipulati contratti di assistenza con le ditte fornitrici che prevedono interventi in teleassistenza entro 1 ora dalla segnalazione per situazioni bloccanti.

5.3.7 Situazione ambientale

La provincia di Cuneo è classificata come zona a probabilità sismica bassa. Si vedano in proposito:

- Ordinanza Presidenza del Consiglio dei Ministri n. 3274 del 20 marzo 2003, G.U. n. 105 del 8/05/2003, S.O. n. 72 che fissa i criteri di classificazione;
- D.G.R. Regione Piemonte n. 61-11017 del 17/11/2003, dove Cuneo, Savigliano e Mondovì sono classificate in zona 4, cioè minima.

Gli edifici sede di sale server non sono vicini a nessun corso d'acqua.

5.3.8 Misure di sicurezza per nuove installazioni

Con l'adozione del presente piano di sicurezza, si dispone che tutti i nuovi apparati di categoria server che verranno acquistati o comunque installati e utilizzati dall'azienda, dovranno essere collocati in locali che presentino almeno le seguenti caratteristiche:

- **locali chiusi ad accesso controllato**: l'accesso ai locali nei quali siano ospitati i sistemi di elaborazione o i sistemi di comunicazione dovrà essere interdetto a chiunque, fatta eccezione per il personale autorizzato. Valgono le regole già viste per le attuali sale server.
- **locali dotati di alimentazione elettrica privilegiata**: dovrà essere garantita presenza almeno di un gruppo di continuità in grado di alimentare tutte le apparecchiature necessarie alla continuazione dell'operatività in caso di brevi interruzioni di energia elettrica. In caso di server e apparecchiature fondamentali per l'azienda o vitali per la salute dei pazienti è necessaria la presenza di un gruppo elettrogeno che possa supplire nell'eventualità di un guasto elettrico di durata elevata.
- **locali dotati di opportuno condizionamento**: i locali dovranno possedere condizioni idonee di microclima - in termini di temperatura, polverosità, umidità - e nel caso questo non sia garantibile attraverso misure passive, andranno predisposte le adeguate misure attive di condizionamento;
- **locali dotati di impianto antincendio**: i locali dovranno essere dotati di un adeguato impianto antincendio e possibilmente dovranno essere monitorati in continuo attraverso sensori per la rilevazione precoce degli aumenti di temperatura e di fumo;

Tutti gli apparati attivi di rete andranno collocati in armadi chiusi a chiave che garantiscano valori corretti di temperatura, di polverosità e di umidità.

Tutti i sistemi di elaborazione di categoria server in uso in azienda, non importa se di proprietà, o a qualsiasi altro titolo detenuti e di cui si abbia la responsabilità, devono avere almeno le seguenti caratteristiche:

- per quanto possibile, e in funzione della specifica necessità, andranno privilegiate configurazioni hardware dei server ridondanti che garantiscano la continuità di servizio, per es. doppio alimentatore in configurazione ridondata, configurazione di server in cluster in tecnologia virtuale VMware o analoga, o in alternativa con funzionalità di "Mutual Take Over" o similari, doppia scheda di rete al fine di poter resistere a guasti singoli sulla scheda di rete, ecc…;

- tutte le aree di memoria su disco magnetico destinate a contenere i dati dovranno essere tutelate da misure di ridondanza (mirroring o RAID); ogni server dovrà possedere una unità di backup, a meno di utilizzare un sistema di backup centralizzato, presente nelle sedi di Cuneo, Mondovì e Savigliano.

5.4 PROTEZIONE CONTRO VIRUS INFORMATICI

Le difese contro gli attacchi da parte di virus informatici si basano su due tipi di misure:

- Protezione mediante software antivirus.
- Aggiornamento del software.

La protezione mediante software antivirus è diffusa su tutte le piattaforme elaborative della rete aziendale:

- PC: è installato un antivirus Symantec, che provvede ad effettuare scansioni automatiche ad ogni accensione del PC e ad ogni nuovo file creato, letto o scaricato sul PC.
- Server: ogni server è a sua volta dotato di antivirus Symantec, analogo a quello dei PC, anch'esso aggiornato automaticamente. Fanno eccezione i sistemi Linux, per i quali non è previsto antivirus.
- Mail Server: il prodotto open source Zimbra Connection Suite, utilizzato per la posta elettronica aziendale, è dotato di un modulo antivirus ed uno antispam, che provvedono a controllare tutte le mail in arrivo per verificarne il contenuto. In caso di riscontro di virus o spam, la mail viene scartata dal sistema stesso.
- Firewall: sui Firewall Watchguard (presenti a Cuneo e Mondovì ed in corso di attivazione a Savigliano) sono installati un modulo antivirus ed un modulo antispam, forniti dalla stessa Watchguard, che filtrano i contenuti in transito da Internet verso l'Azienda, al fine di rilevare e bloccare eventuali messaggi dannosi.

Al fine di garantire la massima efficienza della protezione, data l'elevata frequenza con cui vengono generati e diffusi nuovi virus, i suddetti programmi vengono sistematicamente e automaticamente aggiornati, sia con connessioni giornaliere dei server principali alla ditta fornitrice del software antivirus, sia con l'aggiornamento giornaliero dei clients tramite il collegamento ai server.

L'aggiornamento dell'antivirus e dei suoi dati avviene in modo automatico, mediante alcuni server, tipicamente uno o più in ogni sede principale, che provvedono a distribuire a tutti i PC la configurazione antivirus aggiornata all'ultima versione disponibile dal sito del produttore.

L'aggiornamento del software di base Microsoft Windows viene effettuato in modo automatico dove l'infrastruttura di rete lo consente e manualmente altrove.

5.5 POLITICHE PER LA MEMORIZZAZIONE DELLE BANCHE DATI

La politica aziendale riguardo alle banche dati contenenti dati personali è che esse siano memorizzate sulle unità disco dei server o delle Storage Area Network (SAN), in quanto trattasi, come descritto nel par. 5.3.3, di apparecchiature ad elevata affidabilità.

In questo caso, la responsabilità del funzionamento di tali banche dati e dell'effettuazione delle copie di salvataggio è del S.I.T. o, se del caso, del Responsabile esterno.

Qualora, esclusivamente per motivi tecnici (ad es. non disponibilità di server nella sede interessata), non fosse possibile la memorizzazione di una banca dati su server o SAN, previa autorizzazione del S.I.T., si potrà memorizzare tale banca dati in locale su di un PC. In questo caso, la responsabilità dell'effettuazione di copie di salvataggio è del responsabile del trattamento. In generale tale situazione è assolutamente da evitare, in quanto espone i dati a maggiori rischi di perdita o accesso indesiderato.

5.6 POLITICHE DI GESTIONE DEI BACKUP

Le misure di seguito descritte si riferiscono a tutti i dati memorizzati centralmente sui server di rete.

5.6.1 Strategie di backup

In azienda è in uso una precisa strategia di effettuazione dei backup, mirata a garantire la pronta disponibilità dei dati in caso di perdita dovuta a guasti meccanici, errore umano o azione dolosa.

Per ogni area ex ASL 15, 16, 17 esiste quindi una procedura centralizzata di backup basata sui server nei quali sono memorizzati i dati e su apposite unità a nastro DAT standard DDS3 e DDS4 e su cassette LTO2, LTO3 e LTO4.

La procedura viene di norma eseguita giornalmente. Per rendere efficienti, sicure e funzionali le procedure di Backup / Ripristino, vengono archiviate quattro unità nastro al mese con frequenza settimanale, un'unità nastro mensile e una annuale, oltre a quella archiviata giornalmente.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Giorno	*L*	*M*	*M*	*G*	*V*	*S*	*D*	*L*	*M*	*M*	*G*	*V*	*S*	*D*	*L*
N. nastro	*1*	*2*	*3*	*4*	*S1*			*1*	*2*	*3*	*4*	*S2*			*1*

	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Giorno	*L*	*M*	*M*	*G*	*V*	*S*	*D*	*L*	*M*	*M*	*G*	*V*	*S*	*D*	*L*
N. nastro	*1*	*2*	*3*	*4*	*S3*			*1*	*2*	*3*	*4*	*S4*			*Mese*

Riepilogando, per un qualsiasi giorno della settimana sono a disposizione:

- Il backup dei 4 giorni precedenti
- Il backup delle 4 settimane precedenti
- Il backup dei mesi precedenti
- Il backup dell'anno precedente

Il giorno in cui viene fatto il salvataggio settimanale (S1, S2, S3, S4) non è sempre lo stesso, ma ruota di mese in mese per avere un ricircolo delle unità nastro utilizzate.

Le regole di Backup sopra indicate vengono applicate per tutte le postazioni di backup presenti.

Oltre ai Backup ordinari, vengono fatti a necessità backup per procedure particolari, in momenti di cambio di configurazione o prima di aggiornare le procedure

5.6.2 Modalità di esecuzione del backup

Nelle varie postazioni di backup vengono salvati:

- dati (file);

- database (le procedure di backup dei database sono intese come esportazione in locale del database e successiva copia su unità nastro);
- applicativi (dove previsto);
- stato del sistema (WINS, DNS, DHCP, Database SAM ecc…);
- dati e impostazioni di posta elettronica, siti web ecc...

I supporti fisici di backup sono conservati, in generale, in luogo sicuro e diverso da quello dove ha sede il server corrispondente, in maniera tale da minimizzare la probabilità di distruzione contestuale di server e dati di salvataggio.

POLITICHE DI GESTIONE DEI SUPPORTI DI MEMORIZZAZIONE

5.6.3 Procedure per l'archiviazione dei supporti di memorizzazione

I supporti di memorizzazione sui quali vengono effettuate le copie di salvataggio vengono etichettati con le informazioni per consentirne l'identificazione e conservati in locali o armadi chiusi a chiave.

5.6.4 Procedure per la verifica della leggibilità dei supporti di memorizzazione

La verifica dell'integrità dell'informazione memorizzata viene eseguita manualmente dall'incaricato al salvataggio.

5.6.5 Criteri per l'eliminazione dei supporti di memorizzazione obsoleti

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

I supporti di memorizzazione possono essere riutilizzati da altri incaricati se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

6. CRITERI E MODALITA' PER IL RIPRISTINO DELLA DISPONIBILITA' DEI DATI IN SEGUITO A DISTRUZIONE O DANNEGGIAMENTO

Le modalità di ripristino dei dati in caso di distruzione e/o danneggiamento dei medesimi devono prevedere due situazioni:

a) **Distruzione e/o danneggiamento dei dati**
   E' compito del personale del S.I.T. procedere al ripristino dei dati mediante recupero degli stessi dalle copie di salvataggio descritte nel par. 5.6 "POLITICHE DI GESTIONE DEI BACKUP". Le operazioni di ripristino dei dati verranno effettuate con priorità assoluta al fine di garantire la ripresa dell'attività lavorativa nel minor tempo possibile.

b) **Distruzione e/o danneggiamento dei dati in aggiunta alla distruzione e/o danneggiamento delle apparecchiature atte a gestirli**

Siccome il danneggiamento dei dati è contemporaneo al danneggiamento delle attrezzature che ne permettono il trattamento verrà definito dal S.I.T. il piano di lavoro per il ripristino delle attrezzature nel minor tempo possibile.
Le attrezzature danneggiate potranno essere così gestite:

- sostituzione immediata con altra pari o simile a quella danneggiata;
- installazione del sistema di trattamento su altra attrezzatura disponibile in azienda e già in uso per altre applicazioni aziendali;
- predisposizione di attrezzatura di emergenza da sostituirsi non appena riparata e/o acquistata nuova attrezzatura idonea a sostituire quella danneggiata.

Va tuttavia ricordato che i principali sistemi centrali sono migrati verso la tecnologia di virtualizzazione VMware, che, in caso di guasto di un server fisico, consente di riprendere immediatamente ed automaticamente il servizio su di un altro server dello stesso cluster. Questa soluzione copre tutta la casistica di guasti ordinari comuni ai server ed in generale agli apparati elettronici.
Inoltre, la stessa tecnologia consente di effettuare delle copie statiche dei singoli server virtuali, utilizzabili come copia di riserva del server. Questo consentirebbe di "trasportare" tale server su un'altra qualsiasi unità elaborativa (server o anche PC), purchè dotata di risorse sufficienti, e, utilizzando un ambiente di supporto VMware, ripristinare il funzionamento del server originale, allo stato del momento in cui è stata fatta la copia. Questa caratteristica dovrà essere sviluppata all'interno dell'azienda per migliorare ulteriormente le possibilità di ripristino in casi gravi.

7. INTERVENTI FORMATIVI E INFORMATIVI

La presente sezione è dedicata alla previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare.

La formazione è programmata già al momento dell'ingresso in servizio, nonchè in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

ANNO 2009

- Giornata formativa: "*Tutela della salute e protezione dei dati personali – principali prescrizioni e problematiche*", corso rivolto ai Responsabili interni del trattamento dei dati personali tenutosi il 22/10/2009 a Mondovì ed il 05/11/2009 a Savigliano. La documentazione relativa è agli atti del Servizio Legale;
- Incontro formativo – informativo il 27.11.2009 diretto agli operatori amministrativi e sanitari sull'applicazione della normativa in materia di protezione dei dati personali su richiesta del Distretto di Savigliano-Fossano. La documentazione relativa è agli atti del Servizio Legale;
- Incontro formativo per i tecnici informatici sulla natura, ruolo e compiti dell'amministratore di sistema e contestuale lettera di incarico id 717865 del 25.11.2009. La documentazione relativa è agli atti del Servizio Informatica & Telecomunicazione.
- Comunicazione a tutti i dipendenti "incaricati del trattamento dei dati" delle istruzioni approvate nel D.P.S., mediante la loro pubblicazione sulla intranet aziendale (nota prot. 19263 del 29.04.2009; e-mail del 04.05.2009);

- Consegna delle istruzioni a tutti i nuovi dipendenti "incaricati del trattamento dei dati" (Allegato 2), approvate nel D.P.S. all'atto della sottoscrizione del contratto - nota prot. 515903 del 04.05.2009 -;
- Consegna istruzioni specifiche a tutti coloro con cui l'ASL instaura rapporti di lavoro autonomo (Allegato 3), anche non retribuito o onorario o a tempo parziale temporaneo, ed altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato (nota prot. 515903 del 04.05.2009);
- Consegna istruzioni specifiche a tutti i dipendenti che utilizzano il nuovo software di prenotazione CUP Provinciale che gestisce, altresì, l'acquisizione del consenso al trattamento dei dati personali degli utenti che accedono all'Azienda (note prot. n. 666295 del 8/10/2009 e n. 68689 del 28.10.2009).
- Predisposizione istruzioni per il trattamento dei dati di terzi durante l'affidamento di servizi ed acquisizione di beni e nel corso della successiva instaurazione ed esecuzione del rapporto contrattuale (nota prot. 515585 del 30.04.2009);
- Utilizzo della intranet aziendale quale strumento informativo in materia di privacy mediante la creazione di un'apposita sezione dedicata alla suddetta materia nella quale sono stati inserite, previa comunicazione a tutti i fruitori della rete locale, i provvedimenti inerenti l'applicazione della normativa sulla protezione dei dati personali adottati dall'Azienda. Creazione della sezione privacy all'interno dell'area S.C. Servizio Legale
- Predisposizione sul sito internet di una sezione dedicata alla privacy mediante la pubblicazione delle informative di interesse ai sensi dell'art. 13 D.Lgs 196/03.

ANNO 2010

- Giornata formativa: "*Tutela della salute e protezione dei dati personali – principali prescrizioni e problematiche*", corso rivolto ai Responsabili interni del trattamento dei dati personali tenutosi a Cuneo il 09.02.2010;
- "*Privacy ed attività medico-legale inerente gli accertamenti finalizzati al sostegno delle fasce deboli*", specifico intervento nell'ambito del Corso di aggiornamento "Invalidità civile, Handicap e disabilità: aspetti valutativi, organizzativi e procedurali", tenutosi a Borgo San Dalmazzo il 22.10.2010 ed a Savigliano il 29.10.2010.;
- Il "*Codice in materia di trattamento dei dati personali*", specifico intervento all'interno del corso "Aspetti legali dell'attività specialistica ambulatoriale dell'ASL CN1" tenutosi a Cuneo il 09.12.2010;
- "*Aspetti e riferimenti legislativi*" (affrontato le tematiche inerenti il passaggio di informazioni tra SERT e 1) altri servizi pubblici sociali e sanitari, 2) autorità giudiziaria e avvocati 3) soggetto in carico); specifico intervento nell'ambito del corso "Genitorialità e dipendenze patologiche" tenutosi in Savigliano l'11 ed il 25 maggio 2010;
- Comunicazione agli "incaricati del trattamento dei dati" delle istruzioni approvate nel D.P.S., mediante la loro pubblicazione sulla intranet aziendale, nonché delle modalità per identificare gli amministratori di sistema in ottemperanza al punto 4.3 del Provvedimento a carattere generale del Garante per la protezione dei dati personali, rubricato "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alla attribuzioni delle funzioni di amministratore di sistema*" del 27.11.2008 (nota prot. 44092/P del 19.04.2010; e-mail del 19.04.2010);
- Comunicazione ai Responsabili interni del trattamento dei dati personali dell'avvenuto aggiornamento del D.P.S. (nota prot. 43932 del 19.04.2010);

- Trasmissione nomina ai nuovi Responsabili interni del trattamento dei dati personali unitamente alla comunicazione dell'avvenuto aggiornamento del D.P.S. (nota prot. 44124 del 19.04.2010);
- Comunicazione al Responsabile del Personale del rinnovo delle istruzioni da consegnare al personale dipendente e non all'atto della stipulazione del contratto unitamente alla trasmissione della modulistica da consegnare nel caso di modifica dei Responsabili delle "Aree privacy di riferimento" (nota prot. 878041 del 06/05/2010).

ANNO 2011

- Il "*Codice in materia di trattamento dei dati personali*", specifico intervento all'interno del corso "Aspetti legali dell'attività specialistica ambulatoriale dell'ASL CN1" tenutosi a Cuneo il 18.03.2011;
- Giornata formativa "*Tutela della salute e disciplina del trattamento dei dati personali*", corso rivolto ai Coordinatori del comparto, edizioni 14.04.2011 e 04.05.2011.

ANNO 2012

- 09 e 16 febbraio 2012 incontro formativo sulla comunicazione effettuato dalla S.C. Bilancio e Comunicazione sociale ai centralinisti di Mondovì-Ceva con approfondimento sulle "istruzioni privacy" allegate al D.P.S.;
- Giornata formativa "Tutela della salute e disciplina del trattamento dei dati personali", corso rivolto ai Coordinatori del comparto, edizioni 08.06.2012 e un'ulteriore edizione in data da determinare.

Si rinvia, altresì, a quanto previsto dal "Piano di Formazione – Anno 2012" dell'ASL CN1.

La predisposizione di ulteriori opportune azioni informative e formative è altresì di competenza dei responsabili dei trattamenti, che si possono avvalere della collaborazione della S.C. Informatica e Telecomunicazione per gli aspetti tecnici e della S.C. Servizio Legale per gli aspetti giuridici.

8. TRATTAMENTI AFFIDATI ALL'ESTERNO

Riguardo al caso di trattamenti di dati personali affidati, in conformita' al codice, all'esterno della struttura del titolare si veda il par. RESPONSABILI ESTERNI.

9. SEPARAZIONE DEI DATI SANITARI

Le modalità di protezione adottate in relazione alla memorizzazione ed archiviazione di dati idonei a rivelare lo stato di salute e la vita sessuale consistono nella separazione di questi ultimi dai dati identificativi. Tutti gli applicativi che gestiscono trattamenti di dati sensibili in azienda adottano questa tecnica rispetto alla cifratura dei dati per motivazioni economiche, per la minor complessità e migliori prestazioni.
Di conseguenza, la visibilità congiunta dei dati identificativi e dei dati sensibili idonei a rivelare lo stato di salute è possibile solo agli incaricati, sulla base dei profili di autorizzazione, tramite l'utilizzo degli appositi programmi applicativi.

10. ALLEGATI

A. Elenco dei trattamenti dei dati personali;
Abis. Elenco apparecchiature elettromedicali;
B. Istruzioni da consegnare all'atto della sottoscrizione del contratto di lavoro ai dipendenti, incaricati del trattamento;
C. Istruzioni da consegnare agli incaricati esterni del trattamento dati personali;
D. Amministratori di sistema.
E. Regolamento sulle modalità d'uso degli strumenti informativi, di internet e della posta elettronica.

11. DOCUMENTI E REGISTRAZIONI CORRELATI

D.lgs 30.06.2003 n. 196 "Codice in materia di Protezione dei dati personali"

12. LISTA DI DISTRIBUZIONE

RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI

TUTTI I DIPARTIMENTI E STRUTTURE DELL'ASL CN1