ALLEGATO C

DELIBERAZIONE N. 174

DEL 31 MARZO 2011

COMPOSTO DA N. 35 PAGINE

Via Mazzini 117
28887 OMEGNA (VB)
Tel. 0323-868178
Fax 0323-643020

Azienda Sanitaria Locale VCO

Documento programmatico sulla sicurezza

Ai sensi del decreto legislativo 196/2003 – Codice in materia di protezione dei dati personali - art. 34 e regola 19 dell'allegato B.

IL COMMISSARIO IL DIRETTORE SANITARIO IL DIRETTORE AMMINISTRATIVO

Allegato C - Parte integrante e sostanziale della deliberazione n. _____ del _____ composto da numero 35 pagine

Premessa

L'Azienda Sanitaria Locale VCO in ragione dei suoi compiti istituzionali (prevenzione, cura della salute dei cittadini e riabilitazione), tratta con regolarità dati personali e sensibili.

La predisposizione del documento programmatico sulla sicurezza, redatto secondo i criteri dettati dal disciplinare tecnico di cui al D.Lgs 196/03, e s.m.i. riveste pertanto una rilevanza particolare, vista la mole di dati sensibili trattati all'interno delle strutture aziendali. Esso intende definire le politiche di sicurezza in materia di trattamento di dati personali ed i criteri organizzativi per l'attuazione di tali politiche.

L'Azienda, in particolare, si pone i seguenti obiettivi di sicurezza:

- ridurre a livelli ritenuti accettabili i principali rischi di sicurezza a cui il sistema informativo aziendale è sottoposto (ad esempio: rischi di distruzione o perdita, anche accidentale, dei dati; rischi legati all'accesso non autorizzato o a trattamenti non consentiti o con conformi alle finalità della raccolta). La riduzione dei rischi di sicurezza viene perseguita mediante l'attuazione di misure minime di sicurezza e, ove ritenuto opportuno dall'Azienda, anche mediante l'attuazione di misure di sicurezza ulteriori;
- mantenere, compatibilmente con i vincoli di sicurezza sopra enunciati, il massimo livello di usabilità del sistema informativo.

Il Responsabile del trattamento dati è comunque tenuto a trasmettere ai dipendenti, incaricati del trattamento, il presente documento al fine di renderli edotti dei rischi individuati e dei modi per prevenire i danni. Si premurerà altresì di dare immediata comunicazione di ogni aggiornamento dello stesso a seguito di segnalazioni del Responsabile della sicurezza.

Il presente documento viene inoltre pubblicato sul sito intranet aziendale a disposizione di tutti i dipendenti autorizzati all'accesso alla rete aziendale.

Campo di applicazione

Quanto contenuto nel presente documento si applica a tutti i trattamenti effettuati nell'ambito delle attività aziendali su dati idonei a identificare direttamente o indirettamente persone fisiche o entità giuridiche, ivi compresa l'Azienda stessa, con l'ausilio di mezzi elettronici o automatizzati.

Revisioni e aggiornamenti

Il presente documento viene revisionato entro il 31 marzo di ogni anno come da indicazione della normativa vigente.

Elenco dei trattamenti di dati personali (regola 19.1)

L'elenco dei trattamenti di dati personali scaturisce da una indagine interna a seguito di nota Prot. 16182 del 25 febbraio 2009 inviata ai Responsabili (**allegato C-1**) e rinviata agli stessi per le opportune verifiche ed integrazioni .

Descrizione dei compiti e delle responsabilità (regola 19.2)

La distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati è stata effettuata con atto deliberativo n. 1403 del 11.12.2000 nonché da ogni specifica disposizione impartita formalmente dal Responsabile del trattamento.

In qualità di titolare delle banche dati aziendali, il Direttore Generale ha nominato con lettera formale i Responsabili del trattamento dei dati.

Con deliberazione del Direttore Generale n. 738 del 15 dicembre 2005 è stato approvato il *"Manuale aziendale per la sicurezza del trattamento dei dati personali"* ad uso dei Responsabili e degli Incaricati del trattamento dei dati dell'Azienda Sanitaria Locale VCO con l'intento di fornire ai Responsabili ed agli Incaricati del trattamento dei dati, una panoramica sulle responsabilità loro spettanti, sui rischi che incombono nello svolgimento di detti compiti, sulle misure adottate dall'Azienda Sanitaria per prevenire eventi dannosi, e sui profili più significativi della disciplina sulla protezione dei dati personali.

Analisi dei rischi che incombono sui dati e misure di sicurezza (regola 19.3 e 19.4)

In questo capitolo è descritta l'analisi dei rischi derivanti dall'utilizzo degli elaboratori elettronici, con i quali è effettuato il trattamento dei dati, che possono essere accessibili mediante una rete di telecomunicazioni disponibile al pubblico.

Normalmente gli elaboratori non prevedono collegamenti esterni, però per alcune operazioni sono effettuate connessioni all'esterno autorizzate, quali i collegamenti con le Ditte che gestiscono i programmi del Sistema Amministrativo, del Servizio Personale, del Sistema Sanitario, ecc., connessioni via internet, gestione caselle di posta elettronica.

Alcuni elaboratori sono collegati alla rete geografica aziendale, altri sono in rete interna al servizio e non connessa con altre Unità Operative, altri ancora non sono collegati alla rete.

Nell'anno 2010 è stata implementata la nuova rete dati/fonia geografica aziendale basata su un collegamento in fibra ottica tra le sedi principali (Ospedale di Verbania, Ospedale di Domodossola, Sede Centrale di Omegna). Le maggiori sedi distaccate (distretti di Verbania, Domodossola, DSM di Omegna e Domodossola) sono collegate in MPLS a banda larga ad alta velocità; le sedi sub-distrettuali (Omegna Vicolo Mergozzolo, Vanzone, San Maurizio d'Opaglio, San Rocco a Verbania, Villadossola, Pieve Vergonte, Premosello) sono in MPLS a banda larga con capacità trasmissiva a velocità inferiori.

Conseguentemente è attivo anche un collegamento INTERNET a 100 Mbps che viene utilizzato anche per fornire, tramite collegamento VPN dedicate, servizi diretti ad alcune Case di Cura convenzionate (Villa Serena – Orta San Giulio, Lagostina a Omegna, Eremo di Miazzina, Ornavasso).

Alcuni elaboratori hanno connessioni accessibili dall'esterno in modo limitato e protetto. Le persone che possono accedere dall'esterno sono i tecnici delle Ditte preposte all'assistenza alle procedure da remoto, i Consorzi dei Servizi Sociali di Verbania, Omegna e Domodossola, le Strutture Residenziali convenzionate. Le protezioni sono gestite in modo che ogni Ente possa accedere solo alle macchine (server e PC) di propria competenza. Tali collegamenti possono, comunque, presentare rischi di accesso indesiderato o di utilizzo non corretto delle procedure. Le Ditte sono incaricate al trattamento dei dati.

L'analisi dei rischi e l'individuazione ed adozione delle relative misure di protezione e sicurezza sono state effettuate per tutti gli elaboratori elettronici installati presso l'Ente.

ANALISI RISCHI E MISURE DI SICUREZZA RELATIVE ALLE OPERAZIONI E COLLEGAMENTI EFFETTUATI

Elaboratori in rete

Presso l'Azienda è in funzione una rete geografica di elaboratori, realizzata con collegamenti diretti interni via cavo o wireless e tra le sedi attraverso. Tutte le tipologie di collegamento, ma in particolare quelle di tipo wireless e quelle che utilizzano internet, sono protette secondo gli standard più sicuri attualmente disponibili.

Gli elaborati sono utilizzati dal personale dipendente dell'Ente, responsabile del corretto impiego dei computer, il quale è inoltre incaricato del trattamento dei dati personali ed autorizzato all'accesso per la gestione esclusiva delle operazioni connesse alla propria attività lavorativa.

Tutti i PC presenti in Azienda sono dotati di Sistema Operativo che richiede il riconoscimento degli utenti. L'utilizzo dei PC è consentito solo in seguito all'identificazione dell'utilizzatore che avviene tramite idoneo programma (Active Directory) che riconosce l'utente e gli abilita le autorizzazioni che gli sono state assegnate dal suo Responsabile del trattamento dei dati.

ActiveDirectory risiede sul P.D.C. installato presso la S.O.C. I.C.T. ed è replicato sui D.C di sede che validano in locale e consentono il normale svolgimento del lavoro anche nel caso di impossibilità di accesso al P.D.C..

Viene gestito l'aggiornamento centralizzato della soluzione antivirus utilizzata (antivirus, antispyware, host intrusion protection) sugli elaboratori in rete attraverso un software di gestione predisposto a tale scopo. Tale gestione consente non solo l'aggiornamento automatico sugli elaboratori client in rete dell'ultima versione dell'antivirus commercializzata, ma anche la possibilità di monitoraggio degli stessi con possibilità di effettuare analisi statistiche periodiche relative alla sicurezza della rete. Viene inoltre gestita da remoto la rimozione dei virus intercettati.

Operazioni attuate	**Valutazione dei rischi**	**Misure di protezione e sicurezza**
Utilizzo procedure informatiche.	Funzionamento non corretto rispetto allo standard verificato dovuto alla modifica dei parametri di base in modalità diversa da quella prevista dall'Azienda.	Utilizzo delle procedure secondo le caratteristiche intrinseche alle stesse. Connessione e disconnessione nella maniera stabilita dalla procedura. Vietare l'intervento estemporaneo di qualsiasi persona esterna non autorizzata dall'Ente.
	Blocco delle procedure.	Utilizzo delle procedure secondo le caratteristiche intrinseche alle stesse. Connessione e sconnessione nella maniera stabilita dalla procedura.
	Danneggiamento delle apparecchiature e degli	Utilizzo delle procedure secondo le

	archivi informatici.	caratteristiche intrinseche alle stesse. Connessione e sconnessione nella maniera stabilita dalla procedura. Vietare l'intervento estemporaneo di qualsiasi persona esterna non autorizzata dall'Ente.
Operazioni di trattamento dati con collegamento in rete tra il computer server centrale e gli elaboratori client. Essendo la rete privata, funziona a circuito chiuso realizzato mediante allacciamento diretto via cavo.	Quando gli elaboratori vengono utilizzati collegati in rete interna non vi è nessuna connessione con l'esterno. L'accesso è autorizzato solo al personale per la gestione della sua normale attività.	Utilizzo di una password per la connessione alla rete aziendale e utilizzo di una password per l'accesso al Server centrale per la gestione di dati. Tali password devono essere personali e utilizzate solo dalla persona intestataria delle stesse. Devono essere richieste al servizio competente sottoscrivendo apposita modulistica che deve essere firmata dal Responsabile del servizio e dall'intestatario relativo. Le password di accesso alla rete o ai diversi sistemi informatici devono essere modificate spesso o direttamente dalla procedura, se lo consente, o facendo esplicita richiesta al servizio competente.
I Sistemi presenti nell'Ente prevedono la possibilità di intervento da parte della Ditta fornitrice la quale può collegasi alla rete aziendale utilizzando due modalità: - connessione a banda larga tramite un portale che attiva un collegamento VPN SSL - direttamente via modem Tale procedura risulta importante ed utile per l'Ente in quanto consente che gli interventi di manutenzione ordinaria e straordinaria su richiesta siano tempestivi e rapidi .	Possibilità che possa essere attivato da parte delle Ditte esterne un collegamento illecito ai personal computer presenti sulla rete aziendale ed agli archivi contenenti i dati personali degli utenti, anche se le abilitazioni consentono interventi solo sugli archivi di propria competenza.	Per evitare tale rischio, che peraltro è conseguente ad azioni illecite, occorre che il programmatore che richiede l'aggiornamento del programma controlli, passo passo, i collegamenti che sono effettuati dalla Ditta esterna verificando che l'accesso sia limitato esclusivamente alle tabelle del sistema in gestione o al programma. L'accesso tramite portale VPN SSL è effettuato previa autenticatizione ed è normato e verificato da una serie di regole di accesso alla rete aziendale definite a livello di firewall. Le regole di accesso sono definite in modo che le

		Ditte possano accedere solamente ai server dei loro sistemi e non a tutti gli elaboratori in rete. Per quanto riguarda l'accesso via modem, ormai utilizzato solo sporadicamente, è richiesto un sistema di autenticazione, ma non è possibile definire le regole di accesso alla rete aziendale. In questo caso l'intervento viene, di norma, seguito direttamente da un tecnico del CED, che scollega il modem al termine dell'intervento.
	Intrusione ad opera di programmi di cui all'art. 615-quinquies del codice penale che eventualmente siano presenti negli strumenti informatici della Ditta esterna che si collega al Server.	Utilizzo del programma "antivirus" aggiornato.
	Intrusione illecita negli archivi da parte di terzi (pirati informatici) durante il collegamento.	Per l'accesso via portale VPN SSL gli accessi indebiti sono filtrati a livello di firewall e tracciati in un file di log. Per l'accesso via modem si deve limitare il collegamento solo ed esclusivamente al tempo necessario alla Ditta per attuare le modifiche al sistema.
	Violazione e modifica dell'integrità dei dati con programmi contenenti virus informatici.	Utilizzo di un firewall con antivirus integrato per effettuare un controllo antivirus a livello perimetrale. Utilizzo del programma "antivirus" aggiornato. Limitare il collegamento con modem all'esterno solo ed esclusivamente al tempo necessario alla Ditta per attuare le modifiche al sistema . Effettuare controlli periodici (ogni quindici

		giorni) a campione per verificare l'integrità dei dati archiviati. Cancellare, dopo il definitivo utilizzo, i files di testo che contengono dati sensibili. Effettuare salvataggi periodici dei dati archiviati con conservazione del supporto di backup in luogo differente da dove è collocato il computer.
Copia o installazione sul computer di programmi esterni o di archivi attraverso supporti magnetici.	Violazione e modifica dell'integrità dei dati con programmi contenenti virus informatici.	Utilizzo del programma "antivirus" aggiornato. Non installare programmi dei quali non se ne conosce la precisa provenienza e non autorizzati.
	Danneggiamento configurazione delle macchine che può portare ad un utilizzo non efficiente dell'apparecchiatura con conseguenti perdite di tempo.	Utilizzo del programma "antivirus" aggiornato. Non installare programmi non autorizzati.
	Superamento numero licenze acquistate dall'Ente (violazione della legge sulla pirateria informatica).	Non installare programmi non autorizzati.
	Diffusione rapida di virus informatici via rete.	Utilizzo del programma "antivirus" aggiornato. Non installare programmi non autorizzati. Non scaricare programmi o allegati da internet potenzialmente pericolosi o di cui non si conosce l'esatta provenienza. Contattare immediatamente il Servizio competente per adeguato controllo.
Ricerche via Internet e connessioni a siti per attività istituzionali dell'Ente e di ricerca dati.	Intrusione illecita negli archivi da parte di terzi (pirati informatici) durante il collegamento.	Gestione di programmi appositi (firewall) per il controllo di accessi illeciti tramite la rete internet. Non effettuare collegamenti alla rete internet al di fuori di quelli autorizzati.

		Limitare il collegamento ad internet al tempo strettamente necessario. Consentire l'accesso a siti di interesse aziendale a tempo indeterminato, regolamentare l'accesso a siti non istituzionali per un tempo predefinito, vietare l'accesso a tutti gli altri siti. Consentire l'accesso a internet solo a persone autorizzate dal responsabile di struttura.
	Violazione e modifica dell'integrità dei dati con programmi contenenti virus informatici.	Utilizzo del programma "antivirus" aggiornato. Non effettuare collegamenti alla rete internet al di fuori di quelli autorizzati. Effettuare salvataggi periodici dei dati archiviati con conservazione del supporto di backup in luogo differente da dove è collocato il computer. Verificare periodicamente manualmente che non siano presenti nel sistema programmi che non vengono identificati dalla protezione antivirus.
Collegamento alle caselle di posta elettronica per la gestione delle e-mail.	Intrusione illecita negli archivi da parte di terzi (pirati informatici) durante il collegamento.	Non è possibile l'accesso esterno in quanto il server di posta è accessibile solo dall'interno della rete aziendale.
	Violazione e modifica dell'integrità dei dati con programmi contenenti virus informatici o tramite spam.	Utilizzo di un server di posta con antivirus integrato. Gestione dello spamming a livello di sistemi firewall e/o server. Utilizzo del programma "antivirus" aggiornato sul personal computer client. Informativa all'utenza interna (ad es. "Non aprire mail "strane", ma soprattutto non aprire allegati sospetti"). Non trasmettere dati sensibili via e-mail.
Inserimento, modifica, cancellazione dati di qualunque natura (documenti, tabelle, archivi	Perdita dei dati inseriti a causa di malfunzionamenti di parti hardware del	Per evitare il rischio di perdita del lavoro svolto si ritiene indispensabile effettuare salvataggi a

personali, ecc.)	computer o a causa di attacchi di virus informatici che pregiudicano il funzionamento dell'apparecchiatura o a causa di cancellazioni accidentali di dati.	diversi livelli: su floppy disk, su CD-ROM, via rete su altre apparecchiature adibite a tale scopo, con scadenze da stabilire a seconda dei tempi di aggiornamento di tali dati sul computer in uso.

Elaboratori non in rete aziendale ed elaboratori in rete utilizzati in modalità "STAND ALONE"

Non tutti gli elaboratori sono connessi alla rete aziendale. Tali elaboratori vengono utilizzati dal personale del servizio di appartenenza, il quale è autorizzato all'accesso per la gestione esclusiva relativamente alla propria attività lavorativa.

Operazioni attuate	Valutazione dei rischi	Misure di protezione e sicurezza
Utilizzo procedure informatiche.	Funzionamento non corretto rispetto allo standard verificato dovuto alla modifica dei parametri di base in modalità diversa da quella prevista dall'Azienda.	Utilizzo delle procedure secondo le caratteristiche intrinseche alle stesse. Connessione e sconnessione nella maniera stabilita dalla procedura. Vietare l'intervento estemporaneo di qualsiasi persona esterna non autorizzata dall'Ente.
	Blocco delle procedure.	Utilizzo delle procedure secondo le caratteristiche intrinseche alle stesse. Connessione e sconnessione nella maniera stabilita dalla procedura.
	Danneggiamento delle apparecchiature e degli archivi informatici.	Utilizzo delle procedure secondo le caratteristiche intrinseche alle stesse. Connessione e sconnessione nella maniera stabilita dalla procedura. Vietare l'intervento estemporaneo di qualsiasi persona esterna non autorizzata dall'Ente.
Operazioni di trattamento dati locali al servizio senza possibilità di collegamento telematico con altri computer.	Accesso ai dati presenti sul computer da parte di persone non autorizzate al trattamento degli stessi.	Definire su ciascun elaboratore una password di sistema che non consenta l'utilizzo a personale non autorizzato. Le password di accesso ai diversi sistemi informatici devono essere modificate spesso o direttamente dalla procedura, se lo consente, o facendo esplicita richiesta al servizio competente. Deve essere richiesta al servizio competente sottoscrivendo apposita modulistica che deve

		essere firmata dal Responsabile del servizio e dal personale autorizzato.
Copia o installazione sul computer di programmi esterni o di archivi attraverso supporti magnetici.	Violazione e modifica dell'integrità dei dati con programmi contenenti virus informatici.	Utilizzo del programma "antivirus" aggiornato. Non installare programmi dei quali non se ne conosce la precisa provenienza e non autorizzati.
	Danneggiamento configurazione delle macchine che può portare ad un utilizzo non efficiente dell'apparecchiatura con conseguenti perdite di tempo.	Utilizzo del programma "antivirus" aggiornato. Non installare programmi non autorizzati.
	Superamento numero licenze acquistate dall'Ente (violazione della legge sulla pirateria informatica).	Non installare programmi non autorizzati.
	Diffusione rapida di virus informatici.	Non installare programmi non autorizzati. Non scaricare programmi o allegati da internet potenzialmente pericolosi o di cui non si conosce l'esatta provenienza. Contattare immediatamente il Servizio competente per adeguato controllo.
Ricerche via Internet e connessioni a siti per attività istituzionali dell'ente e di ricerca dati. Collegamento alle caselle di posta elettronica per la gestione delle e-mail.	Intrusione illecita negli archivi da parte di terzi (pirati informatici) durante il collegamento via modem.	Gestione di programmi appositi per il controllo di accessi illeciti tramite la rete internet. Non effettuare collegamenti alla rete internet al di fuori di quelli autorizzati. Consentire l'accesso a internet solo a persone autorizzate dal responsabile di struttura. Limitare il collegamento ad internet al tempo strettamente necessario.
	Violazione e modifica dell'integrità dei dati con programmi contenenti virus informatici.	Utilizzo del programma "antivirus" aggiornato. Non effettuare collegamenti alla rete internet al di fuori di quelli autorizzati. Effettuare salvataggi periodici dei dati archiviati con conservazione del supporto di backup in luogo differente da dove è collocato il computer.

		Verificare periodicamente manualmente che non siano presenti nel sistema programmi che non vengono identificati dalla protezione antivirus.
Inserimento, modifica, cancellazione dati di qualunque natura (documenti, tabelle, archivi personali, ecc.)	Perdita dei dati inseriti a causa di malfunzionamenti di parti hardware del computer o a causa di attacchi di virus informatici che pregiudicano il funzionamento dell'apparecchiatura o a causa di cancellazioni accidentali di dati.	Per evitare il rischio di perdita del lavoro svolto si ritiene indispensabile effettuare salvataggi a diversi livelli: su floppy disk, su CD-ROM, con scadenze da stabilire a seconda dei tempi di aggiornamento di tali dati sul computer in uso.

Elaboratori in rete interna al servizio

Presso alcune Unità Operative i computer sono collegati in rete interna via cavo per consentire lo scambio rapido di informazioni tra utenti dello stesso servizio.

Operazioni attuate	Valutazione dei rischi	Misure di protezione e sicurezza
Utilizzo procedure informatiche.	Funzionamento non corretto rispetto allo standard verificato dovuto alla modifica dei parametri di base in modalità diversa da quella prevista dall'Azienda.	Utilizzo delle procedure secondo le caratteristiche intrinseche alle stesse. Connessione e sconnessione nella maniera stabilita dalla procedura. Vietare l'intervento estemporaneo di qualsiasi persona esterna non autorizzata dall'Ente.
	Blocco delle procedure.	Utilizzo delle procedure secondo le caratteristiche intrinseche alle stesse. Connessione e sconnessione nella maniera stabilita dalla procedura.
	Danneggiamento delle apparecchiature e degli archivi informatici.	Utilizzo delle procedure secondo le caratteristiche intrinseche alle stesse. Connessione e sconnessione nella maniera stabilita dalla procedura. Vietare l'intervento estemporaneo di qualsiasi persona esterna non autorizzata dall'Ente.
Operazioni di trattamento dati locali al servizio senza possibilità di collegamento telematico con altri computer.	Accesso ai dati presenti sul computer da parte di persone non autorizzate al trattamento degli stessi. Non vi è nessuna connessione con l'esterno. L'accesso ai dati è consentito solo al personale dell'Ente per la gestione della normale attività.	Definire su ciascun elaboratore una password di sistema che non consenta l'utilizzo a personale non autorizzato. Deve essere richiesta al servizio competente sottoscrivendo apposita modulistica che deve essere firmata dal Responsabile del servizio e dal personale autorizzato. Le password di accesso alla rete interna al servizio o ai diversi sistemi informatici devono essere modificate spesso o direttamente dalla procedura, se lo consente, o facendo esplicita

		richiesta al servizio competente.
Copia o installazione sul computer di programmi esterni o di archivi attraverso supporti magnetici.	Violazione e modifica dell'integrità dei dati con programmi contenenti virus informatici.	Utilizzo del programma "antivirus" aggiornato. Non installare programmi dei quali non se ne conosce la precisa provenienza e non autorizzati.
	Danneggiamento configurazione delle macchine che può portare ad un utilizzo non efficiente dell'apparecchiatura con conseguenti perdite di tempo.	Utilizzo del programma "antivirus" aggiornato. Non installare programmi non autorizzati.
	Superamento numero licenze acquistate dall'Ente (violazione della legge sulla pirateria informatica).	Non installare programmi non autorizzati.
	Diffusione rapida di virus informatici via rete.	Non installare programmi non autorizzati. Non scaricare programmi o allegati da internet potenzialmente pericolosi o di cui non si conosce l'esatta provenienza. Contattare immediatamente il Servizio competente per adeguato controllo.
Ricerche via Internet e connessioni a siti per attività istituzionali dell'ente e di ricerca dati. Collegamento alle caselle di posta elettronica per la gestione delle e-mail.	Intrusione illecita negli archivi da parte di terzi (pirati informatici) durante il collegamento via modem.	Gestione di programmi appositi per il controllo di accessi illeciti tramite la rete internet. Non effettuare collegamenti alla rete internet al di fuori di quelli autorizzati. Limitare il collegamento ad internet al tempo strettamente necessario. Consentire l'accesso a internet solo a persone autorizzate dal responsabile di struttura.
	Violazione e modifica dell'integrità dei dati con programmi contenenti virus informatici.	Utilizzo del programma "antivirus" aggiornato. Non effettuare collegamenti alla rete internet al di fuori di quelli autorizzati. Effettuare salvataggi periodici dei dati archiviati con conservazione del supporto di backup in luogo differente da dove è collocato il computer. Verificare periodicamente manualmente che non siano presenti nel sistema programmi che

		non vengono identificati dalla protezione antivirus.
Inserimento, modifica, cancellazione dati di qualunque natura (documenti, tabelle, archivi personali, ecc.)	Perdita dei dati inseriti a causa di malfunzionamenti di parti hardware del computer o a causa di attacchi di virus informatici che pregiudicano il funzionamento dell'apparecchiatura o a causa di cancellazioni accidentali di dati.	Per evitare il rischio di perdita del lavoro svolto si ritiene indispensabile effettuare salvataggi a diversi livelli: su floppy disk, su CD-ROM, via rete su altre apparecchiature adibite a tale scopo, con scadenze da stabilire a seconda dei tempi di aggiornamento di tali dati sul computer in uso.

Elaboratori di servizi erogati su rete pubblica (Internet)

Presso l'Azienda ci sono diversi server *pubblici* (ovvero quei server che sono raggiungibili dall'esterno della rete aziendale - ed anche da internet). In particolare:

- portale dei servizi dedicati ai Medici di Medicina Generale e Pediatri di Libera Scelta
- server di inoltro posta elettronica

Questi server sono collocati in una parte della rete chiamata DMZ (**demilitarized zone**). Questa porzione di rete è un segmento isolato della LAN (una "sottorete") raggiungibile sia da sottoreti interne che dall'esterno. Nella DMZ sono, però, permesse connessioni esclusivamente *verso* l'esterno: gli host attestati sulla DMZ non possono connettersi alla rete aziendale interna o possono connettersi solo ad alcune risorse specificate nelle regole impostate sul firewall.

Operazioni attuate	**Valutazione dei rischi**	**Misure di protezione e sicurezza**
Fornitura servizi internet tramite portale	Accesso indebito alla rete grazie a software maligno o ad attacchi mirati da parte di hacker informatici	Utilizzo di un firewall che filtri ogni tipo di attacco indebito. Inserimento dei server pubblici nella rete DMZ.
	Accesso indebito per eventuali problemi dovuti a "buchi" nei sistemi software utilizzati (webserver) che consentono l'esecuzione di software indesiderato (virus, malware ecc.).	Utilizzo di una soluzione antivirus integrata (antivirus, antispyware e host intrusion protection) gestita centralmente. Aggiornamento costante dei sistemi utilizzati.
	Salvaguardia dell'Integrità dei dati	Effettuazione salvataggi periodici dell'intero sistema.
Fornitura servizio posta elettronica	Accesso indebito alla rete grazie a software maligno o ad attacchi mirati da parte di hacker informatici	Utilizzo di un firewall che filtri ogni tipo di attacco indebito. Utilizzo di un server aggiuntivo per l'inoltro della posta ed il controllo antispam in rete DMZ.

	Accesso indebito per eventuali problemi dovuti a "buchi" nei sistemi software utilizzati (webserver) che consentono l'esecuzione di software indesiderato (virus).	Utilizzo di un gestore di posta elettronica dotato antivirus integrato costantemente aggiornato. Utilizzo di una soluzione antivirus integrata (antivirus, antispyware e host intrusion protection) gestita centralmente. Aggiornamento costante dei sistemi utilizzati.
	Rischi dovuti alla possibilità di accesso alla posta aziendale a distanza.	Utilizzo di un sistema di accesso con richiesta di autenticazione e crittografia dei dati. Accesso alla posta solo tramite web mail.
	Integrità dei dati	Si effettuano salvataggi giornalieri della configurazione del server di posta e dei dati contenuti nelle caselle di posta elettronica.

ANALISI RISCHI E MISURE DI SICUREZZA RELATIVE ALLE AREE E LOCALI

Aree e locali	**Valutazione dei rischi**	**Misure di protezione e sicurezza**
Locali tecnici centrali CED Tutti gli impianti (elettrici, rete fonia e dati, condizionamento, ecc.) sono stati realizzati secondo le normative vigenti e la loro corretta realizzazione è certificata dalle Ditte fornitrici. La manutenzione ed il controllo degli impianti installati è stato affidato alla Ditta VCO Global Service con Delibera n. 322 del 31 maggio 2001 che effettua verifiche periodiche di funzionamento.	Intrusione illecita di terzi non autorizzati nei locali dove sono presenti computer	Gli elaboratori centrali presenti in questi locali sono accessibili durante l'orario di lavoro solo da personale del CED o da persona autorizzate dal Responsabile del CED o dagli incaricati al trattamenti di dati del CED o da tecnici esterni supportati dalla presenza di personale CED. L'accesso ai computer avviene solo tramite password di amministrazione conosciuta solo dagli incaricati del trattamento. E' inoltre prevista anche la password sullo screen saver che viene attivata automaticamente durante le soste dell'attività lavorativa. I locali tecnici sono sempre chiusi a chiave e vengono aperti solo in caso di necessità lavorative. La sicurezza, sia passiva che attiva, dei locali tecnici del CED è garantita da porte di ingresso tipo REI tagliafuoco. E' previsto un registro di accesso per l'identificazione del personale esterno all'Azienda.
	Incendio – Allagamento	I dati vengono salvati su nastro o su supporto magnetico e sono conservati in archivio. Per il pericolo di allagamento installare i computer in posizione rialzata da terra. La sicurezza, sia passiva che attiva, dei locali tecnici del CED è garantita da: • sistema di sensori di calore collegati ad un allarme presso la portineria centrale della ASL VCO

		✓ sistema di sensori di fumo collegati ad un segnalatore acustico locale
	Mancanza di energia elettrica	I computer centrali sono dotati di gruppi di continuità per assicurare l'erogazione di energia elettrica. La sicurezza, sia passiva che attiva, dei locali tecnici del CED è garantita da un sistema di segnalazione mancanza di tensione che si attiva mandando un segnale di allarme alla portineria centrale della ASL VCO.
Uffici nelle Sedi (principali e secondarie) presenti su tutto il territorio dell'Azienda.	Intrusione illecita di terzi non autorizzati nei locali dove sono presenti computer	Gli elaboratori sono installati all'interno di uffici dove possono accedere e sono autorizzati ad essere presenti durante l'orario di lavoro gli incaricati del trattamento dei vari uffici. L'ingresso negli uffici da parte di altre persone è autorizzato dai Responsabili. L'accesso ai computer avviene solo tramite password personale di accensione come pure l'accesso alla rete e l'accesso ai dati centrali. E' inoltre prevista anche la password sullo screen saver che viene attivata automaticamente durante le soste dell'attività lavorativa. Di giorno, al di fuori dell'orario di lavoro, l'ufficio è chiuso a chiave. Alla sera, al termine dell'orario di lavoro, tutti gli uffici sono chiusi a chiave.
	Incendio – Allagamento	I dati vengono salvati su nastro o su supporto magnetico e sono conservati in archivio. Per il pericolo di allagamento installare i computer in posizione rialzata da terra.
	Mancanza di energia elettrica	I computer centrali sono dotati di gruppi di continuità per assicurare l'erogazione di energia elettrica.

Criteri e modalità di ripristino della disponibilità dei dati (regola 19.5)

In questa sezione si indicano le procedure adottate per il salvataggio dei dati presenti sui server centrali aziendali.

Per quanto riguarda il ripristino degli stessi in caso di danneggiamento o di inaffidabilità della base dati, in tutti i casi è necessario utilizzare il supporto esterno, custodito in cassaforte, e ricaricare i dati presenti nell'ultimo salvataggio secondo le modalità previste per ciascun archivio.

L'aggiornamento alle istruzioni operative e tecniche per la realizzazione di quanto descritto nel seguito sono state trasmesse ufficialmente al personale della s.o.c. I.C.T.

UBICAZIONE CED 1 OMEGNA

NOME SERVER	MODALITA'
CEDDC	Il salvataggio è effettuato tramite server dedicati (CEDDCVH, CEDDCVB, CEDDCDH, CEDDCDO, CEDDCCR)
CEDPROG –PIANTA ORGANICA	Copia giornaliera su CEDBKP Copia periodica su CD
CEDPROG –CREDNET	Copia giornaliera su CEDBKP Copia periodica su CD
CEDPROG – FORMAZIONE	Copia giornaliera su CEDBKP Copia periodica su CD
CEDPROG – UVG	Copia giornaliera su CEDBKP Copia periodica su CD
CEDMAIL	Copia giornaliera su CEDBKP
ISASERVER	Nessuna modalità necessaria
CEDWEB	Copia settimanale su CEDBKP
CEDVIRUS	Nessuna modalità necessaria
CEDBKP	Trasferimento periodico dati su disco esterno o DVD
CEDWWW	Copia periodica su CEDBKP
CEDPORT	Copia periodica su CEDBKP

UBICAZIONE CED 2 OMEGNA

NOME SERVER	MODALITA'
PATIDOK	Backup automatico giornaliero e copia su CEDPROG. Base dati su SAN.
OLIAMM	Salvataggio dati giornaliero automatico su cassetta. Occorre sostituire giornalmente la cassetta. Salvataggio automatico su altro server
PROTOCOLLO	Copia fisica della base dati giornaliera su disco esterno. Salvataggio giornaliero del registro su CD. Automatismo per gestione registro di emergenza in caso di crash del sistema. Backup automatico su CEDBKP Creazione DVD 2 volte al mese
RADIOLOGIA	Salvataggio incrementale dati giornaliero automatico su cassetta. Base dati su SAN. Salvataggio Immagini c/o Server Immagini delle radiologie VB - Domo. Il salvataggio è automatico da programma. Base dati su SAN.
NEFROLOGIA	Salvataggio automatico della base dati su unità disco di rete esterno.
LABORATORIO ANALISI	Il DB server è clusterizzato.

	Il backup viene eseguito automaticamente con Oracle Recovery Manager. Export giornaliero su LABSRV01\d$ Copia automatica su LABSRV01\G$ e su LABSRV06

UBICAZIONE CED VERBANIA OSPEDALE

NOME SERVER	MODALITA'
CEDDCVH	Essendo un backup controller non necessita di salvataggi periodici

UBICAZIONE CED VERBANIA DISTRETTO

NOME SERVER	MODALITA'
CEDDCVB	Essendo un backup controller non necessita di salvataggi periodici

UBICAZIONE CED DOMODOSSOLA OSPEDALE

NOME SERVER	MODALITA'
CEDDCDH	Essendo un backup controller non necessita di salvataggi periodici

UBICAZIONE CED DOMODOSSOLA DISTRETTO

NOME SERVER	MODALITA'
CEDDCDO	Essendo un backup controller non necessita di salvataggi periodici

UBICAZIONE CED CRUSINALLO

NOME SERVER	MODALITA'
CEDDCCR	Essendo un backup controller non necessita di salvataggi periodici

UBICAZIONE ALTRI SERVIZI

NOME SERVER	MODALITA'
ANATOMIA PATOLOGICA	Il salvataggio parte automaticamente tutte le notti. Occorre cambiare giornalmente la cassetta.
RILEVAZIONE PRESENZE	Export giornaliera in locale e copia automatica su altro server di raccolta in altra sede.
ONCOLOGIA	Backup automatico su CEDBKP Cambio della cassetta ogni venerdì.
DIPARTIMENTO DI PREVENZIONE - CRUSINALLO	Copia periodica su altro PC e su CD
DISTRETTI DOMODOSSOLA	Copia su CD
DISTRETTO VERBANIA	Copia giornaliera su altri PC del Distretto Copia periodica su CD

Per tutti i salvataggi è prevista almeno una possibilità alternativa in caso di guasto all'apparecchiatura preposta originariamente (es. in caso di rottura dell'unità a nastro, backup su cd/dvd o disco rigido su altra macchina).

Per quanto riguarda il ripristino dei dati in caso di danneggiamento gli stessi potranno essere recuperati dai supporti prodotti dalle sopraelencate operazioni.

Piano di formazione

La sicurezza in materia di Privacy richiede una manutenzione continua del sistema trattandosi di aspetto organizzativo che ancora non è pienamente parte della cultura dei sistemi più organizzati quali gli enti pubblici.
In questo senso nel corso di questi anni si sono affrontati tematiche apparentemente non direttamente connesse in materia di sicurezza di privacy ma a questa riconducibile pienamente. Gli interventi formativi sono rivolti ai Responsabili e agli Incaricati del trattamento in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per mantenere un aggiornamento sulle misure da assicurare in materia di trattamento dei dati.
La S.O.C. Gestione Attività Supporto Direzionale, sulla base delle indicazioni programmatiche del piano di attività della Direzione Generale e sulla scorta dell'analisi del bisogno formativo nell'ASL VCO deliberato ha attuato la seguente attività formativa:

ATTIVITA' FORMATIVA ATTUATA

Nel corso dell' anno 2008-2010 la S.O. C. GASD ha coordinato, organizzato e realizzato diversi percorsi formativi rivolti ad operatori sanitari ed amministrativi i cui riflessi didattici ed organizzativi sono riconducibili al trattamento dei dati e nell' applicazione della normativa in materia di Privacy.

L'articolazione formativa è stata la seguente:

- "ETHOS" ASL VCO: condividere e diffondere la prospettiva etica nelle II referente del rischio clinico e la gestione delle segnalazioni;
- Comunicazione e gestione delle relazioni professionali nell'équipe di lavoro ;
- La figura dell'operatore sanitario e la responsabilità professionale oggi;

- Segreto d'ufficio e professionale;
- organizzazioni sanitarie;
- Malpractice, aspetti giuridici e consenso informato.

Il percorso ETHOS è stato attivato per tutto il personale del ruolo sanitario ed inserito nel progetto di collaborazione interaziendale fra le AASSRR del Quadrante 2 ed in particolare, per quanto riguarda la materia specifica, fra l' ASL VCO, l' ASO Maggiore della Carità di Novara e le ASL di Novara, Biella e Vercelli.
Attraverso questa iniziativa formativa sono stati affrontati argomenti corollari alla privacy di grande attualità in quanto costituiscono il presupposto fondamentale per la cultura della privacy.
Le altre tematiche che configurano un vero e proprio "progetto formativo" dedicato ad argomenti in materia di privacy hanno interessato a fari livelli operatori e sanitari di strutture aziendali diverse.

ATTIVITA' FORMATIVA PROGRAMMATA

La programmazione formativa in materia di sicurezza dei dati affronterà argomenti nel campo organizzativo-gestionale ed un percorso formativo in materia di sicurezza dei dati in campo clinico sia per il personale del ruolo amministrativo e sanitario, che sarà programmato per il personale del ruolo sanitario.

Sinteticamente qui di seguito si riepilogano le principali iniziative formative programmate:

- Idoneità e gestione dell'operatore sanitario con problematiche psichiatriche rivolto anche a RLS, dirigenti e preposti;

- Amministratore di sostegno, interdizione inabilitazione: aspetti problematici della messa in atto di tali strumenti di tutela ;

- Ruoli e competenze del personale amministrativo: il responsabile del Procedimento Amministrativo ;

- Aggiornamenti su tematiche amministrative di attività distrettuale ;

- Aggiornamenti su aspetti legislativi nel settore socio-sanitario necessari nell'anno a seguito di nuove disposizioni legislative anche con particolare riferimento a responsabilità, ruolo dell'assistente sociale in sanità.

Amministratori di sistema

Il Dirigente Analista e tutti i Collaboratori e gli Assistenti Tecnici Programmatori svolgono mansioni di amministratore di sistema, amministratore di base di dati, amministratore di rete, ciascuno secondo le proprie competenze e le attività assegnate al momento.

Per questo motivo tutti possono, nell'ambito dell'assistenza agli utenti, venire a conoscenza di dati personali/sensibili presenti nelle basi dati aziendali.

Pertanto si è deciso di dare le stesse competenze di amministratore di sistema alle persone di seguito elencate:

NOMINATIVO	QUALIFICA	INCARICO
GAGLIARDI Anna	Dirigente Analista	
CERUTTI Gianfranco	Collaboratore Tecnico Professionale Programmatore	Nota Prot. 20833 del 11/03/2009
GESU' Silvana	Collaboratore Tecnico Professionale Programmatore	Nota Prot. 20863 del 11/03/2009
ROBERTI Fausto	Assistente Tecnico Programmatore	Nota Prot. 20849 del 11/03/2009
ROMAGNOLI Davide	Assistente Tecnico Programmatore	Nota Prot. 81876 del 16/10/2009
RUSSO Silvia	Assistente Tecnico Programmatore	Nota Prot. 20831 del 11/03/2009
SAVINA Stefano	Assistente Tecnico Programmatore	Nota Prot. 20845 del 11/03/2009
SCARIN Chiara	Assistente Tecnico Programmatore	Nota Prot. 20830 del 11/03/2009
MARTORANA Ferdinando	Assistente Amministrativo	Nota Prot. 21281 del 12/03/2009

In adeguamento della normativa emanata dal Garante per la protezione dei dati personali del 27.11.2008 pubblicata sulla Gazzetta Ufficiale n. 300 del 24.12.2008 è stato attivato un sistema informatico per il controllo accessi denominato LogLogic MX2010 (determina Direttore S.O.C. Forniture e Logistica n. 73 del 27 novembre 2009).

Trattamenti affidati all'esterno (regola 19.7)

Tutte le Ditte esterne che effettuano trattamento di dati per conto dell'Azienda devono garantire, tramite idonea documentazione, l'adozione delle misure minime di sicurezza in conformità a quanto previsto nel codice.

L'elenco delle Ditte scaturisce da indagine interna a seguito di nota nota Prot. 19147 del 3/3/2008 inviata ai Responsabili del trattamento di dati personali (**allegato C-2**).

Incarico al trattamento dei dati: Ditte esterne

Nell'ambito dei contratti di manutenzione e assistenza dei sistemi informatici dell'Azienda, le Ditte fornitrici possono venire a conoscenza di dati personali/sensibili presenti nelle basi dati dei sistemi di afferenza.

Pertanto è stato incaricato al trattamento dei dati il legale rappresentante di ciascuna di esse che, a sua volta, ha indicato i nominativi delle persone che operano sulle base dati relative alle procedure fornite. Gli elenchi dei nominativi incaricati vengono costantemente aggiornati in funzione delle variazioni comunicate dalle Ditte.

Cifratura dei dati o separazione dei dati identificativi (regola 19.8)

Dato	Protezione scelta (cifratura/separazione)	Data di effettività	Tecnica adottata	
			Descrizione	**Informazioni utili**
Gestione flussi dati regionali	Cifratura	01.01.2003	I dati vengono trasmessi sulla rete Rupar con l'utilizzo della Posta elettronica Lottus Notes e codificati come previsto dal protocollo di comunicazione della Regione Piemonte. Attraverso un programma apposito è possibile decifrare i dati con l'utilizzo di password idonee	Si veda estratto DPS del CSI Piemonte (**allegato C-3**)
Altri dati	Separazione	Dalla data di attivazione delle diverse procedure	I dati anagrafici sono di norma contenuti in tabelle diverse rispetto a quelle relative ai dati sensibili	

Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali

Con nota Prot. 21304 del 12/03/2009 è stato inviato a tutti i Responsabili del trattamento dei dati personali il protocollo per lo smaltimento di apparecchiature informatiche, come previsto dal Provvedimento del Garante della Privacy – 13 ottobre 2008, di seguito riportato:

PROTOCOLLO PER L'INSTALLAZIONE, LA SOSTITUZIONE PER NON IDONEITA' E LO SMALTIMENTO DI APPARECCHIATURE INFORMATICHE (PC, STAMPANTI ECC.).

Visto quanto previsto dal Provvedimento del 13 ottobre 2008 del Garante della Privacy in materia di regolamentazione e di messa in sicurezza dei dati in caso di reimpiego, riciclaggio o smaltimento di apparecchiature elettriche ed elettroniche, si stabilisce quanto segue:

- L'apparecchiatura da sostituire deve essere mantenuta integra in ogni sua parte fino all'installazione di quella nuova. Solo l'operatore del Sistema Informativo è autorizzato alla rimozione delle componenti fisiche delle stesse (schede interne, hard disk ecc.). Eventuali inadempienze verranno segnalate per iscritto al Responsabile della Struttura per le opportune verifiche/provvedimenti.

- Dopo l'installazione delle nuove apparecchiature la S.O.C. I.C.T. provvederà al recupero dei componenti riciclabili ed allo smaltimento degli hard disk secondo quanto previsto nella normativa sopra citata.

- L'apparecchiatura sostituita potrà essere smaltita solo dopo autorizzazione della S.O.C. I.C.T. che apporrà sulle stesse etichetta adesiva con autorizzazione specifica.

- La confezione della nuova apparecchiatura potrà essere aperta, oltre che dal personale della S.O.C. I.C.T., solo dal fornitore o dal personale della S.O.C. Affari Legali e Patrimoniali per le operazioni di inventario.

- In nessun caso gli utenti finali (impiegati, medici, infermieri, tecnici ecc.) sono autorizzati ad aprire le confezioni e tanto meno ad installare software o documenti di alcun genere.

- Nel caso in cui, al momento dell'installazione, l'apparecchiatura sia trovata fuori dall'imballo, collegata e siano trovati installati software o documenti di qualsiasi genere, l'operatore del S.O.C. I.C.T. provvederà a rimuoverli, senza effettuarne il salvataggio, riportando l'apparecchiatura alle condizioni originali.