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 DIRETTORE SANITARIO F.F. DI COMMISSARIO (Ai sensi art. 12 comma 5 L.R. n. 10/1995) IL DIRETTORE AMMINISTRATIVO

Allegato A - Parte integrante e sostanziale della deliberazione n. - 169 del 28 MARZO 2012 composto da numero 34 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. 17794 del 13 marzo 2012 inviata ai Responsabili (**allegato A-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.

Nell'anno 2011 è stata predisposta nell'ambito del progetto di Evoluzione del Sistema Informativo Aziendale in particolare nella gestione delle Cartella Clinica Elettronica, una Procedura Operativa (Deliberazione n.422 del 22/08/2011) e conseguente Analisi del rischio (**allegato A-6**).

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 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 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 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 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 sostituzione delle singole procedure di salvataggio precedentemente utilizzate, è stata implementata presso i locali CED della sede di Omegna una soluzione hardware e software che ha permesso di sostituire una parte dei singoli server con una struttura di macchine virtualizzate che si appoggia su uno storage adeguatamente dimensionato.

La nuova configurazione comprende anche la realizzazione di una struttura di disaster recovery remotizzata, in fase di installazione presso l'Ospedale di Verbania.

Il servizio di backup è configurato su Data protector 6.20 installato sul server SRVBCK su libreria nastro LTO Ultrium con 7 nastri LTO5.

Per un maggior dettaglio si vedano gli allegati (**allegato A-4 e allegato A-5**).

La diversa strutturazione della rete dati aziendale consente l'accesso ai dati anche in caso di guasto di uno dei backup controller delle sedi periferiche.

Per quanto riguarda il ripristino dei dati in caso di danneggiamento o di inaffidabilità della base dati occorre, a seconda della configurazione, appoggiarsi alla struttura precedentemente indicata o agli archivi memorizzati sui supporti removibili, custoditi in cassaforte.

Per le macchine virtualizzate è disponibile il backup dell'intero server (programmi e dati), da cui si può partire per ricostruire il server da ricreare e/o la relativa base dati.

Per le macchine non virtualizzate occorre un intervento della ditta esterna che gestisce la procedura da ripristinare per la reinstallazione dei programmi (ove necessaria) ed il recupero dei dati dal backup sulla struttura di disaster recovery o dagli archivi removibili, che vengono creati giornalmente e conservati in cassaforte.

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

Di seguito viene schematizzato la situazione attuale dei serve non virtualizzati.

UBICAZIONE CED 1 OMEGNA

NOME SERVER	MODALITA'
CEDDC	Il salvataggio è effettuato tramite server dedicati (CEDDCVH, CEDDCVB, CEDDCDH)
RPSRV	Export giornaliera in locale e copia automatica su storage centrale.
CEDVIRUS	Nessuna modalità necessaria

UBICAZIONE CED 2 OMEGNA

NOME SERVER	MODALITA'
PATIDOK	Backup automatico giornaliero e copia storage. Base dati su SAN.
OLIAMM	Salvataggio dati giornaliero automatico su cassetta. Occorre sostituire giornalmente la cassetta. Salvataggio automatico su storage.
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.
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 PRESSO 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 storage.
ONCOLOGIA	Backup automatico su CEDBKP Copia periodica su storage
DIPARTIMENTO DI PREVENZIONE - CRUSINALLO	Copia periodica su altro PC, su disco esterno 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 , su disco rigido dello storage o 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 è proseguita affrontando 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 2010-2011 la S.O. C. GASD ha coordinato, organizzato e realizzato nuovi percorsi formativi rivolti sia ad operatori sanitari che amministrativi i cui riflessi informativi ed organizzativi sono stati ricondotti al trattamento dei dati e alla comunicazione appropriata nell' applicazione della normativa in materia di Privacy.

L'articolazione formativa è stata la seguente:

- LA RESPONSABILITÀ PROFESSIONALE DEL MEDICO E DELLA STRUTTURA SANITARIA ILLUSTRATA ALLA LUCE DELLE CASISTICHE CLINICHE PIÙ RICORRENTI
- LO STRESS LAVORO CORRELATO, IL BENESSERE ORGANIZZATIVO E LO SPORTELLO DI ASCOLTO INTERNO
- AUTONOMIA E RESPONSABILITA' INFERMIERISTICA ALLA LUCE DELLA NUOVA CULTURA GESTIONALE
- ANALISI DI PROCESSO DI UNA SEGNALAZIONE DELL'UNITA' RISK MANAGEMENT ASL VCO: L'RCA (ROOT CAUSE ANALYSIS)
- LA COMUNICAZIONE CRITICA CON IL PAZIENTE E I SUOI FAMILIARI
- LA COMUNICAZIONE EFFICACE: LA CAPACITA' DI CONNETTERSI CON L'ALTRO
- ELEVARE LA QUALITÀ DEL LAVORO NELL'AMBITO DELLA RACCOLTA E GESTIONE DEI DATI SANITARI, EPIDEMIOLOGICI, AMMINISTRATIVI E CONTABILI ATTRAVERSO L'UTILIZZO DI MICROSOFT ACCESS - CORSO BASE

- QUALITÀ DEI SERVIZI E BEN ESSERE ORGANIZZATIVO NELLE ORGANIZZAZIONI 'PERSONALITY INTENSITY'
- ETICA, LIFE SKILLS E BEN ESSERE. LE CAPACITÀ CHE AIUTANO A SENTIRSI MEGLIO SUL LAVORO E NELLA VITA.

Queste iniziative formativa hanno consentito di affrontare molti argomenti corollari alla privacy quali momenti utili all'aggiornamento in materia di privacy. Le tematiche hanno interessato a fari livelli operatori e sanitari di strutture aziendali diverse.

ATTIVITA' FORMATIVA PROGRAMMATA

Per l'anno in corso, 2012, a programmazione formativa in materia di sicurezza dei dati prevede di attivare un ampio percorso in modalità E-learning rivolto a tutto il personale dipendente dell'ASL VCO ovvero sia il personale sanitario che amministrativo.

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

- Corso FAD sulla Privacy rivolto anche a tutto il personale dipendente dell'ASL;
- Etica, life skills e ben essere. Le capacità che aiutano a sentirsi meglio sul lavoro
- Riedizione dell'iniziativa formativa riguardo a ruoli e competenze del personale amministrativo: il responsabile del Procedimento Amministrativo ;
- Aggiornamenti su tematiche amministrative di attività aziendale ;
- La consultazione anagrafica del personale dipendente in web sul sito aziendale Intranet"-

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 A-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 A-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.

Allegati

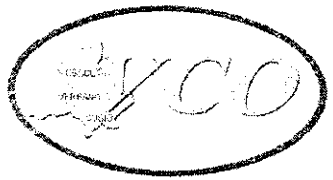
A-1 – Elenco dei trattamenti di dati personali (regola 19.1)
A-2 – Trattamenti affidati all'esterno (regola 19.7)
A-3 – Cifratura dei dati o separazione dei dati identificativi (regola 19.8)
A-4 – Criteri e modalità di ripristino della disponibilità dei dati (regola 19.5)
A-5 – Criteri e modalità di ripristino della disponibilità dei dati (regola 19.5)
A-6 – Analisi dei rischi che incombono sui dati e misure di sicurezza (regola 19.3 e 19.4)

STRUTTURA COMPLESSA I.C.T. GESTIONE DELLE TECNOLOGIE INFORMATICHE DI COMUNICAZIONE E DEL SISTEMA INFORMATIVO

ELENCO TRATTAMENTI DATI PERSONALI

Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture anche esterne che concorrono al trattamento	Eventuale Banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
	S	G						
CORRISPONDENZA verso l'esterno e verso servizi interni	X		I.C.T.	nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	I.C.T.	Personal computer	(*)
PROTOCOLLAZIONE DOCUMENTI DI COMPETENZA	X		S.G.	Strutture Aziendali	ARCHIFLOW	I.C.T.	Personal computer	(*)
DIAPASON ON LINE	X		S.C. AMMINISTRAZIONE DEL PERSONALE	Strutture Aziendali	DIAPASON ON LINE	S.C. AMMINISTRAZIONE DEL PERSONALE	Personal computer	(*)
OLIAMM			I.C.T.	Strutture Aziendali	OLIAMM	I.C.T.	Personal computer	(*)
BOZZE ATTI DELIBERATIVI E DETERMINE			I.C.T.	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	I.C.T.	Personal computer	(*)

(*) Rete aziendale protetta tramite Antivirus e Firewall con collegamento a Internet e alla RUPAR mediante validazione degli accessi a livello utente



STRUTTURA COMPLESSA I.C.T. GESTIONE DELLE TECNOLOGIE INFORMATICHE DI COMUNICAZIONE E DEL SISTEMA INFORMATIVO

ELENCO TRATTAMENTI DATI PERSONALI

Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture anche esterne che concorrono al trattamento	Eventuale Banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
	S	G						
FLUSSI INFORMATIVI REGIONALI	X		I.C.T.	Nessuna	CARTELLA DATI INVIATI	I.C.T.	Personal computer	(*)
TUTTI GLI ARCHIVI AZIENDALI PER ASSISTENZA E MANUTENZIONE	X		Strutture aziendali	Strutture aziendali	TUTTE	Strutture aziendali	Personal computer	(*) (**)

(*) Rete aziendale protetta tramite Antivirus e Firewall con collegamento a Internet e alla RUPAR mediante validazione degli accessi a livello utente

(**) **N.B.** la S.C. C.E.D./Sistema Informativo interviene su tutti i trattamenti di dati aziendali a fini manutentivi e statistici.

Data: 13.03.2012

Firma del Responsabile trattamento dati personali
(Dr.ssa Anna Gagliardi)

ASL

STRUTTURA COMPLESSA UROLOGIA

ELENCO TRATTAMENTI DATI PERSONALI

Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture anche esterne che concorrono al trattamento	Eventuale Banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
	S	G						
CORRISPONDENZA verso l'esterno e verso servizi interni	X		UROLOGIA	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	UROLOGIA	Personal computer	(*)
ESAMI DI LABORATORIO	X		LABORATORIO ANALISI	Strutture Aziendali	DNLAB - DNWEB	C.E.D.	Personal computer	(*)
REFERTI RADIOLOGICI (1)	X		RADIOLOGIA	Nessuna	CD ROM / PROGETTO M.I.S.S.I.L.E. FORNITO DALLA RADIOLOGIA	UROLOGIA	Personal computer	(*)
RELAZIONI CLINICHE (2)	X		UROLOGIA	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	UROLOGIA	Personal computer	(*)
CARTELLA CLINICA	X		D.S.O.	Strutture Aziendali	PATIDOK / PHI	C.E.D.	Personal computer	(*)

(*) Rete aziendale protetta tramite Antivirus e Firewall con collegamento a Internet e alla RUPAR mediante validazione degli accessi a livello utente
(1) I CD RELATIVI AGLI ESAMI RADIOLOGICI DEI PAZIENTI RICOVERATI ALLA DIMISSIONE VENGONO CUSTODITI NELL'ARCHIVIO DELLA RADIOLOGIA
(2) ~~LE RELAZIONI CLINICHE (SCHEDA DI DIMISSIONE) NON HANNO ARCHIVIO INFORMATICO IN QUANTO NON SALVABILI IN PATIDOK~~

Data: 14/03/12

Firma del Responsabile trattamento dati personali
(Dott. Danilo Minocci)

ASL

STRUTTURA COMPLESSA LABORATORIO ANALISI

ELENCO TRATTAMENTI DATI PERSONALI

Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture anche esterne che concorrono al trattamento	Eventuale Banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
	S	G						
CORRISPONDENZA verso l'esterno e verso servizi interni	X		LABORATORIO ANALISI	nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	LABORATORIO ANALISI	Personal computer	(*)
OLIAMM			LABORATORIO ANALISI	Strutture Aziendali	OLIAMM	C.E.D.	Personal computer	(*)
ACCETTAZIONE, ANALISI E REFERTAZIONE ESAMI DI LABORATORIO	X		LABORATORIO ANALISI	Reparti ospedalieri – Centro Polifunzionale Cannobio – Distretti – Case di cura esterne	DNLAB - DNWEB	C.E.D.	Personal computer	(*)
FLUSSI EPIDEMIOLOGIA	X		LABORATORIO ANALISI	NESSUNA	MICRONET	SERVER FARM CSI PIEMONTE - TORINO	Personal computer	(*)
MONITORAGGIO DEI PAZIENTI IN TERAPIA ANTICOAGULANTE	X		LABORATORIO ANALISI	NESSUNA	TAO	SITO INTERNET	Personal computer	(*)

(*) Rete aziendale protetta tramite Antivirus e Firewall con collegamento a Internet e alla RUPAR mediante validazione degli accessi a livello utente

Data: ANNO 2012

Firma del Responsabile trattamento dati personali
(Dott. Nino Cappuccia)

ASL

STRUTTURA COMPLESSA PEDIATRIA

ELENCO TRATTAMENTI DATI PERSONALI

Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture anche esterne che concorrono al trattamento	Eventuale Banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
	S	G						
CORRISPONDENZA verso l'esterno e verso servizi interni	X		PEDIATRIA	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	PEDIATRIA	Personal computer	(*)
ESAMI DI LABORATORIO	X		LABORATORIO ANALISI	Strutture Aziendali	DNLAB - DNWEB	C.E.D.	Personal computer	(*)
REFERTI RADIOLOGICI	X		RADIOLOGIA	Nessuna	CD ROM / PROGETTO M.I.S.S.I.L.E. FORNITO DALLA RADIOLOGIA	PEDIATRIA	Personal computer	(*)
RELAZIONI CLINICHE	X		PEDIATRIA	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	PEDIATRIA	Personal computer	(*)
CARTELLA CLINICA	X		D.S.O.	Strutture Aziendali	PATIDOK / PHI	C.E.D.	Personal computer	(*)
GESTIONE ACCESSI DI PRONTO SEOCCORSO	X		SET. 118/PRONTO SOCCORSO	Strutture Aziendali	FIRST AID	C.E.D.	Personal computer	(*)
CERTIFICATO DI ASSISTENZA AL PARTO	X		SET. 118/PRONTO SOCCORSO	Strutture Aziendali	CEDAP	SERVER FARM CSI PIEMONTE - TORINO	Personal computer	(*)

(*) Rete aziendale protetta tramite Antivirus e Firewall con collegamento a Internet e alla RUPAR mediante validazione degli accessi a livello utente

Data: 13-3-2012

Firma del Responsabile trattamento dati personali
(Dott. Andrea Guala)

non è Pediatria
ma Ostetricia

ASL

S.O.C. IGIENE E SANITA' PUBBLICA

ELENCO TRATTAMENTI DATI PERSONALI

Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture anche esterne che concorrono al trattamento	Eventuale Banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
	S	G						
CORRISPONDENZA verso l'esterno e verso servizi interni	X		SISP	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	SISP	Personal computer	(*)
GESTIONE VACCINAZIONI	X		SISP	Nessuna	ASTER	C.E.D.	Personal Computer	(*)
MALATTIE INFETTIVE	X		SISP	Nessuna	GeMINI 3.3	SISP	Personal Computer	(*)

(*) Rete aziendale protetta tramite Antivirus e Firewall con collegamento a Internet e alla RUPAR mediante validazione degli accessi a livello utente

Data: 15/03/2012

Firma del Responsabile f. f. trattamento dati personali
(Dott. Gianmartino Biollo)

ASL
AZIENDA SANITARIA LOCALE DEL VERBANO CUSIO OSSOLA

STRUTTURA COMPLESSA OCULISTICA

ELENCO TRATTAMENTI DATI PERSONALI

Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture anche esterne che concorrono al trattamento	Eventuale Banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
	S	G						
CORRISPONDENZA verso l'esterno e verso servizi interni	X		OCULISTICA	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	OCULISTICA	Personal computer	(*)
REFERTI RADIOLOGICI	X		RADIOLOGIA	Nessuna	CD ROM / PROGETTO M.I.S.S.I.L.E. FORNITO DALLA RADIOLOGIA	OCULISTICA	Personal computer	(*)
ESAMI DI LABORATORIO	X		LABORATORIO ANALISI	Strutture Aziendali	DNWEB	C.E.D.	Personal computer	(*)
RELAZIONI CLINICHE	X		OCULISTICA	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	OCULISTICA	Personal computer	(*)
CARTELLA CLINICA	X		D.S.O.	Strutture Aziendali	PATIDOK / PHI	C.E.D.	Personal computer	(*)
ESAMI DIAGNOSTICI (FAG/ICG, PERIMETRIA, ERG/PEV)	X		OCULISTICA	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	OCULISTICA	Personal computer	(*)

(*) Rete aziendale protetta tramite Antivirus e Firewall con collegamento a Internet e alla RUPAR mediante validazione degli accessi a livello utente

Data: 20 MAR. 2012

Firma del Responsabile trattamento dati personali
(Dott. Renzo Bordin)

ASL 14

DIREZIONE SANITARIA OSPEDALIERA

ELENCO TRATTAMENTI DATI PERSONALI

Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture anche esterne che concorrono al trattamento	Eventuale Banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
	S	G						
CORRISPONDENZA verso l'esterno e verso servizi interni	X		D.S.O.	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	D.S.O.	Personal computer	(*)
PROTOCOLLAZIONE DOCUMENTI DI COMPETENZA	X		S.G.	Strutture Aziendali	ARCHIFLOW	C.E.D.	Personal computer	(*)
OLIAMM			D.S.O.	Strutture Aziendali	OLIAMM	C.E.D.	Personal computer	(*)
BOZZE ATTI DELIBERATIVI E DETERMINE			D.S.O.	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	D.S.O.	Personal computer	(*)
PROCEDURA ACCETTAZIONE RICOVERI E DAY HOSPITAL	X		D.S.O. – UFFICI ACCETTAZIONE	Strutture Aziendali	ADT – ADTWEB	C.E.D.	Personal computer	(*)
LIBERA PROFESSIONE	X		D.S.O. SEDE DOMODOSSOLA	G.E.F.	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	D.S.O. SEDE DOMODOSSOLA	Personal computer	(*)

ASL 14

DIREZIONE SANITARIA OSPEDALIERA

ASSISTENZA SPECIALISTICA AMBULATORIALE

CORRISPONDENZA verso l'esterno e verso servizi interni	X	X	A.S.A	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	A.S.A	Personal computer	(*)
ARCHIFLOW "PROTOCOLLO INFORMATICO "	X	X	S.G.	Strutture Aziendali	ARCHIFLOW	C.E.D.	Personal computer	(*)
OLIAMM			A.S.A	Strutture Aziendali	OLIAMM	C.E.D.	Personal computer	(*)
BOZZE ATTI DELIBERATIVI E DETERMINE			A.S.A	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	A.S.A	Personal computer	(*)
STIPENDI MEDICI SPECIALISTICI AMBULATORIALI	X		A.S.A	Strutture Aziendali		SERVER FARM CSI PIEMONTE - TORINO	Personal computer	(*)
DIAPASON ON LINE MEDICI SPECIALISTI AMBULATORIALI	X		S.C. AMM.ZIONE DEL PERSONALE	Strutture Aziendali	DIAPASON ON LINE	S.C. AMMINISTRAZIONE DEL PERSONALE	Personal computer	(*)
PRENOTAZIONE VISITE ED ESAMI STRUMENTALI E CONSUNTIVAZIONE	x		A.S.A	Strutture Aziendali	SGP	C.E.D.	Personal computer	(*)

(*) Rete aziendale protetta tramite Antivirus e Firewall con collegamento a Internet e alla RUPAR mediante validazione degli accessi a livello utente

Data:

Firma del Responsabile trattamento dati personali
(Dott. Francesco Garufi)

n.b. si è provveduto a depennare la voce Terapia Alimentare in quanto tale attività non è più di competenza della Direzione Sanitaria Ospedaliera ma fa capo alla SOC Medicina

ASL

AZIENDA SANITARIA LOCALE DEL VERBANO CUSIO OSSOLA

STRUTTURA COMPLESSA SERVIZIO PREVENZIONE E PROTEZIONE

ELENCO TRATTAMENTI DATI PERSONALI

Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture anche esterne che concorrono al trattamento	Eventuale Banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
	S	G						
CORRISPONDENZA verso servizi interni ed esterna	X		S.P.P.	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	S.P.P.	Personal computer	(*)
ARCHIFLOW "PROTOCOLLO INFORMATICO "	X	X	S.G.	Strutture Aziendali	ARCHIFLOW	I.C.T.	Personal computer	(*)
DIAPASON ON LINE	X		RISORSE UMANE	Strutture Aziendali	DIAPASON ON LINE	RISORSE UMANE	Personal computer	(*)
OLIAMM (Ordini magazzino economale)			S.P.P.	Strutture Aziendali	OLIAMM	I.C.T.	Personal computer	(*)
BOZZE ATTI DELIBERATIVI E DETERMINE			S.P.P.	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	S.P.P.	Personal computer	(*)
PIANTA ORGANICA 2011	X		RISORSE UMANE	Alcune strutture aziendali	ARCHIVIO INFORMATICO MICROSOFT ACCESS	I.C.T.	Personal computer	(*)
DOCUMENTI DI VALUTAZIONE DEL RISCHIO			S.P.P.	Nessuna	ARCHIVIO INF.TICO: CARTELLA DOCUMENTI	S.P.P.	Personal computer	(*)
DOCUMENTI DI VALUTAZIONE RISCHIO			S.P.P.	Strutture Aziendali	Sito Intranet	I.C.T.	Personal computer	(*)

ASL

STRUTTURA COMPLESSA NEUROPSICHIATRIA INFANTILE

ELENCO TRATTAMENTI DATI PERSONALI

Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture anche esterne che concorrono al trattamento	Eventuale Banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
	S	G						
CORRISPONDENZA verso l'esterno e verso servizi interni	X		S.C. NPI	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	S.C. NPI – SEDE VERBANIA	Personal computer	(*)
REGISTRO EPIDEMIOLOGICO INFORMATIZZATO NPI	X		S.C. NPI	TUTTE LE ASL PIEMONTESI	NPINet	SERVER FARM CSI PIEMONTE - TORINO	Personal computer	(*)
GESTIONE DATI UTENTI DEL SERVIZIO	X		NPI	Nessuna	MS OFFICE	S.C. NPI	Personal computer	(*)

(*) Rete aziendale protetta tramite Antivirus e Firewall con collegamento a Internet e alla RUPAR mediante validazione degli accessi a livello utente

Data: 19/3/2012

Firma del Responsabile f.f trattamento dati personali
(Dr.ssa Tiziana Martelli)

REGIONE PIEMONTE ASL VCO
DIRETTORE RESPONSABILE F.F.
SOC NEUROPSICHIATRIA INFANTILE 3301
Dott.ssa Tiziana MARTELLI
002990

ASL

STRUTTURA COMPLESSA S.E.R.T.

ELENCO TRATTAMENTI DATI PERSONALI

Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture anche esterne che concorrono al trattamento	Eventuale Banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
	S	G						
CORRISPONDENZA verso l'esterno e verso servizi interni	X	X	S.E.R.T.	Nessuna	ARCHIVIO INF.TICO: CARTELLA DOCUMENTI	S.E.R.T.	Personal computer	(*)
ARCHIFLOWEB "PROTOCOLLO INFORMATICO "	X	X	S.G.	Strutture Aziendali	ARCHIFLOWEB	I.T.C.	Personal computer	(*)
OLIAMM			S.E.R.T.	Strutture Aziendali	OLIAMM	I.T.C.	Personal Computer	(*)
BOZZE ATTI DELIBERATIVI E DETERMINE			S.E.R.T.	Nessuna	ARCHIVIO INF.TICO: CARTELLA DOCUMENTI	S.E.R.T. I.T.C.	Personal computer	(*)
FILE F	X		S.E.R.T.	Nessuna	MS ACCESS	S.E.R.T. I.T.C.	Personal computer	(*)
ESAMI DI LABORATORIO	X		Dipartimento dei Laboratori	Strutture Aziendali Sanitarie	DNWEB	S.E.R.T.	Personal computer	(*)
PRENOTAZIONE VISITE	x		D.S.O. e Dipartimento Territoriale	Strutture Aziendali	SGP	C.E.D.	Personal computer	(*)
REGISTRAZIONE PAZIENTI E GESTIONE AMMINISTRATIVA	X	X	S.E.R.T.	Nessuna	SPIDI	SERVER FARM CSI PIEMONTE – TORINO	Personal computer	(*)
FILE C	X		S.E.R.T.	Nessuna	SPIDI	S.E.R.T. - SERVER FARM CSI PIEMONTE – TORINO	Personal computer	(*)

(*) Rete aziendale protetta tramite Antivirus e Firewall con collegamento a Internet e alla RUPAR mediante validazione degli accessi a livello utente

ASL

STRUTTURA COMPLESSA S.E.R.T.

ELENCO TRATTAMENTI DATI PERSONALI

Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture anche esterne che concorrono al trattamento	Eventuale Banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
	S	G						
DOCUMENTAZIONE PER INSERIMENTI UTENTI IN STRUTTURE RESIDENZIALI	X	X	S.E.R.T.	NESSUNA	MS OFFICE	S.E.R.T. (SEDI DI DOMODOSSOLA, VERBANIA, GRAVELLONA TOCE)	Personal computer	(*)
DOCUMENTAZIONE RELATIVA INSERIMENTI LAVORATIVI C/O COOP. SOCIALI	X		S.E.R.T.	NESSUNA	MS OFFICE	S.E.R.T. (SEDI DI DOMODOSSOLA, VERBANIA, GRAVELLONA TOCE)	Personal computer	(*)
RELAZIONI ATTIVITA' CERTIFICATIVA OVE RICHIESTA DAGLI UTENTI O DA AVENTI DIRITTO	X	X	S.E.R.T.	Nessuna	MS OFFICE	S.E.R.T. (SEDI DI DOMODOSSOLA, VERBANIA, GRAVELLONA TOCE)	Personal computer	(*)
DEFINIZIONE E REALIZZAZIONE DEL PROGRAMMA TERAPEUTICO E SOCIO-RIABILITATIVO	X	X	S.E.R.T.	NESSUNA	MS OFFICE	S.E.R.T. (SEDI DI DOMODOSSOLA, VERBANIA, GRAVELLONA TOCE)	Personal computer	(*)

(*) Rete aziendale protetta tramite Antivirus e Firewall con collegamento a Internet e alla RUPAR mediante validazione degli accessi a livello utente

ASL

STRUTTURA COMPLESSA S.E.R.T.

ELENCO TRATTAMENTI DATI PERSONALI

Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture anche esterne che concorrono al trattamento	Eventuale Banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
	S	G						
DEFINIZIONE E REALIZZAZIONE PROGRAMMA TERAPEUTICO E SOCIO-RIABILITATIVO IN ALTERNATIVA ALLA PENA (RELAZIONI E COMUNICAZIONI)	X	X	S.E.R.T.	NESSUNO	MS OFFICE	S.E.R.T. (SEDI DI DOMODOSSOLA, VERBANIA, GRAVELLONA TOCE)	Personal computer	(*)
FASCICOLO PERSONALE DI FAMILIARI CHE PARTECIPANO AD UN GRUPPO PSICOEDUCATIVO	X		S.E.R.T.	Nessuno	MS OFFICE	S.E.R.T. (SEDI DI DOMODOSSOLA, VERBANIA, GRAVELLONA TOCE)	Personal computer	(*)

(*) Rete aziendale protetta tramite Antivirus e Firewall con collegamento a Internet e alla RUPAR mediante validazione degli accessi a livello utente

Data: 22/03/2012

Firma del Responsabile trattamento dati personali
(Dr.ssa Anna Maria Buzio)

ASL

STRUTTURA COMPLESSA GESTIONE DELLE RISORSE ECONOMICHE E FINANZIARIE

ELENCO TRATTAMENTI DATI PERSONALI

Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture anche esterne che concorrono al trattamento	Eventuale Banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
	S	G						
CORRISPONDENZA verso l'esterno e verso servizi interni	X		G.E.F.	nessuna	ARCHIVIO INF.TICO: CARTELLA DOCUMENTI	G.E.F. C/O settore segreteria o	Personal computer	(*)
ARCHIFLOW "PROTOCOLLO INFORMATICO "	X	X	S.G.	Strutture Aziendali	ARCHIFLOW	C.E.D.	Personal computer	(*)
DIAPASON ON LINE	X		S.C. AMMINISTRAZIONE DEL PERSONALE	Strutture Aziendali	DIAPASON ON LINE	S.C. AMMINISTRAZIONE DEL PERSONALE	Personal computer	(*)
OLIAMM (partitario clienti. partitario fornitori)			G.E.F. (settore contabilità entrate, settore contabilità spese)	Strutture Aziendali	OLIAMM	Ufficio Responsabile S..G.	Personal Computer	(*)
BOZZE ATTI DELIBERATIVI E DETERMINE			G.E.F. (settore segreteria)	Nessuna	ARCHIVIO INF.TICO: CARTELLA DOCUMENTI	G.E.F.	Personal computer	(*)
ANAGRAFE TRIBUTARIA (ACCESSO IN SOLA LETTURA)	X		S.G.	Strutture Aziendali	S.I.A.T.E.L.	AGENZIA DELLE ENTRATE (SITO INTERNET)	Personal computer	(*)

(*) Rete aziendale protetta tramite Antivirus e Firewall con collegamento a Internet e alla RUPAR mediante validazione degli accessi a livello utente

Data:

Firma del Responsabile f.f. trattamento dati personali
Referente Dr.ssa Manuela Succi

ASL

AZIENDA SANITARIA LOCALE DEL VERBANO CUSIO OSSOLA

STRUTTURA COMPLESSA MEDICO COMPETENTE

ELENCO TRATTAMENTI DATI PERSONALI

Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture anche esterne che concorrono al trattamento	Eventuale Banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
	S	G						
CORRISPONDENZA verso servizi interni ed verso l'esterno	X		MEDICO COMPETENTE	nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	MEDICO COMPETENTE	Personal computer	(*)
ARCHIFLOW "PROTOCOLLO INFORMATICO "	X	X	MEDICO COMPETENTE	Strutture Aziendali	ARCHIFLOW	MEDICO COMPETENTE	Personal computer	(*)
OLIAMM			MEDICO COMPETENTE	Strutture Aziendali	OLIAMM	C.E.D.	Personal computer	(*)
BOZZE ATTI DELIBERATIVI E DETERMINE			MEDICO COMPETENTE	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	MEDICO COMPETENTE	Personal computer	(*)
GESTIONE CARTELLA SANITARIA DIPENDENTI ASL E AZIENDE CONVENZIONATE	X		MEDICO COMPETENTE		ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	3 SEDI CON ARCHIVIO CARTACEO E C/O LA SEDE DI VERBANIA E DOMODOSSOLA ANCHE INFORMATICO	Personal computer	(*)

(*) Rete aziendale protetta tramite Antivirus e Firewall con collegamento a Internet e alla RUPAR mediante validazione degli accessi a livello utente

Data: 21/03/2012

Firma del Responsabile trattamento dati personali
(Dott. Giorgio Gambarotto)

ASL

AZIENDA SANITARIA LOCALE DEL VERBANO CUSIO OSSOLA

STRUTTURA COMPLESSA GESTIONE DELLE FORNITURE E DELLA LOGISTICA

Prot. N° 20005 Del 22 MAR. 2012

ELENCO TRATTAMENTI DATI PERSONALI

Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture anche esterne che concorrono al trattamento	Eventuale Banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
	S	G						
CORRISPONDENZA con Ditte e verso servizi interni	X		PROVV. ECONOMATO	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	PROVV. ECONOMATO	Personal computer	(*)
ARCHIFLOW "PROTOCOLLO INFORMATICO"	X	X	S.G.	Strutture Aziendali	ARCHIFLOW	C.E.D.	Personal computer	(*)
DIAPASON ON LINE	X		AMMINISTRAZIONE DEL PERSONALE	Strutture Aziendali	DIAPASON ON LINE	S.C. AMMINISTRAZIONE DEL PERSONALE	Personal computer	(*)
OLIAMM (Approvvigionamenti, Contabilità parziale, Cespiti parziale)			PROVV. ECONOMATO	Strutture Aziendali	OLIAMM	C.E.D.	Personal computer	(*)
BOZZE ATTI DELIBERATIVI E DETERMINE			PROVV. ECONOMATO	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	PROVV. ECONOMATO	Personal computer	(*)

(*) Rete aziendale protetta tramite Antivirus e Firewall con collegamento a Internet e alla RUPAR mediante validazione degli accessi a livello utente

Data: 22 MAR. 2012

Firma del Responsabile trattamento dati personali
(Dott. Federico Bonisoli)

AZIENDA SANITARIA LOCALE - SEDE DI OMEGNA - C.O.C.A.

IL DIRETTORE
STRUTTURA COMPLESSA FORNITURE E LOGISTICA
(Dott. Federico BONISOLI)

ASL

STRUTTURA COMPLESSA RECUPERO E RIABILITAZIONE FUNZIONALE

ELENCO TRATTAMENTI DATI PERSONALI

Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture anche esterne che concorrono al trattamento	Eventuale Banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
	S	G						
CORRISPONDENZA verso l'esterno e verso servizi interni	X		S.C. R.R.F.	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	S.C. R.R.F.	Personal computer	(*)
CONSUNTIVAZIONE PRESTAZIONI PER PAZIENTI RICOVERATI IN ALTRI REPARTI OSPEDALIERI, ADI, RSA, AMNULATORIALI, DOMICILIARI	x		S.C. R.R.F.	Strutture Aziendali	SGP	C.E.D.	Personal computer	(*)
CARTELLA CLINICA INFORMATIZZATA PER PAZIENTI DEGENTI, AMBULATORIALI ESTERNI, PAZIENTI DOMICILIARI, ADI	X		Direzione Sanitaria Ospedaliera	Strutture Aziendali Sanitarie	PATIDOK / PHI	C.E.D.	Personal computer e PRAIM (thin client)	(*)
ESAMI DI LABORATORIO	X		Dipartimento dei Laboratori	Strutture Aziendali Sanitarie	DNLAB - DNWEB	C.E.D.	Personal computer	(*)

(*) Rete aziendale protetta tramite Antivirus e Firewall con collegamento a Internet e alla RUPAR mediante validazione degli accessi a livello utente

Data: 20 MARZO 2012

Firma del Responsabile f.f. trattamento dati personali
(Dott.ssa Marina Buttè)

ASL

S.O.C. SERVIZIO VETERINARIO AREA B

ELENCO TRATTAMENTI DATI PERSONALI

Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture anche esterne che concorrono al trattamento	Eventuale Banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
	S	G						
CORRISPONDENZA verso l'esterno e verso servizi interni	X		VETERINARIO AREA B	A - C	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI E-VET	VETERINARIO AREA B PROTOCOLLO	Personal computer	(*)
SISTEMA INFORMATIVO VETERINARIO			VETERINARIO AREA B	VETERINARIO AREA A C	E-VET	ASL CN1	Personal Computer	(*)
SERVIZI VETERINARI – MARCHE AURICOLARI BOVINI			VETERINARIO AREA A	VETERINARIO AREA B C	E-VET	ASL CN1	Personal Computer	(*)
SCAMBIO, IMPORTAZIONE ED ESPORTAZIONE			VETERINARIO AREA B	VETERINARIO AREA A C	TRACES (EXTRA CE) SINTESI (CE)	APPLICATIVO WEB	Personal Computer	(*)
ANAGRAFE ZOOTECNICA			VETERINARIO AREA A	VETERINARIO AREA B – C	ANAGRAFE ZOOTECNICA NAZIONALE	APPLICATIVO WEB	Personal Computer	(*)

(*) Rete aziendale protetta tramite Antivirus e Firewall con collegamento a Internet e alla RUPAR mediante validazione degli accessi a livello utente

Data: 19/03/2012

Firma del Responsabile F.F. trattamento dati personali
(Dott.ssa Giovanna Lasagna)

ASL 14

DIREZIONE SANITARIA OSPEDALIERA

ASSISTENZA SPECIALISTICA AMBULATORIALE

Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture anche esterne che concorrono al trattamento	Eventuale Banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
	S	G						
CORRISPONDENZA verso l'esterno e verso servizi interni	X	X	A.S.A	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	A.S.A	Personal computer	(*)
ARCHIDOC "PROTOCOLLO INFORMATICO "	X	X	S.G.	Strutture Aziendali	ARCHIDOC	SOC I.C.T. OMEGNA	Personal computer	(*)
OLIAMM			A.S.A	Strutture Aziendali	OLIAMM	SOC I.C.T. OMEGNA	Personal computer	(*)
BOZZE ATTI DELIBERATIVI E DETERMINE			A.S.A	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	A.S.A	Personal computer	(*)
STIPENDI MEDICI SPECIALISTICI AMBULATORIALI	X		A.S.A	Strutture Aziendali		SERVER FARM CSI PIEMONTE - TORINO	Personal computer	(*)
DIAPASON ON LINE MEDICI SPECIALISTI AMBULATORIALI	X		S.C. AMM.ZIONE DEL PERSONALE	Strutture Aziendali	DIAPASON ON LINE	S.C. RISORSE UMANE	Personal computer	(*)
PRENOTAZIONE VISITE ED ESAMI STRUMENTALI E CONSUNTIVAZIONE	x		A.S.A	Strutture Aziendali	SGP	SOC I.C.T. OMEGNA	Personal computer	(*)

(*) Rete aziendale protetta tramite Antivirus e Firewall con collegamento a Internet e alla RUPAR mediante validazione degli accessi a livello utente

Data: 20/3/2012

Firma del Responsabile trattamento dati personali
(Dott. Francesco Garufi)

A.S.L. V.C.O.
Azienda Sanitaria Locale
del Verbano Cusio Ossola

STRUTTURA COMPLESSA GESTIONE DEGLI AFFARI LEGALI E PATRIMONIALI

ELENCO TRATTAMENTI DATI PERSONALI

Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture anche esterne che concorrono al trattamento	Eventuale Banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
	S	G						
CORRISPONDENZA verso servizi interni	X		**ALP**	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	**ALP**	Personal computer	(*)
ARCHIDOC "PROTOCOLLO INFORMATICO "	X	X	S.G.	Strutture Aziendali	ARCHIDOC	C.E.D.	Personal computer	(*)
DIAPASON ON LINE	X		AMMINISTRAZIONE DEL PERSONALE	Strutture Aziendali	DIAPASON ON LINE	S.C. AMMINISTRAZIONE DEL PERSONALE	Personal computer	(*)
BOZZE ATTI DELIBERATIVI E DETERMINE			**ALP**	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	**ALP**	Personal computer	(*)
CARICO INVENTARIALE PROTESI E AUSILI	X		**DISTRETTO -**	Nessuna	OLIAMM Ordini	**CED**	Personal computer	(*)
CORRISPONDENZA RELATIVA A CONTENZIOSO	X	X	**ALP - Settore Legale -**	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	**ALP - Settore Legale -**	Personal computer	(*)
MEMORIE CAUSE PENDENTI	X	X	**ALP - Settore Legale -**	Nessuna **LEXTEL**	ARCHIVIO INFORM.: CARTELLA	**ALP - Settore Legale -**	Personal computer	(*)

A.S.L. V.C.O.
Azienda Sanitaria Locale del Verbano Cusio Ossola

STRUTTURA COMPLESSA GESTIONE DEGLI AFFARI LEGALI E PATRIMONIALI

					DOCUMENTI SUITE AVVOCATO **LEXTEL - archivio telematico connesso a PCT -**			
DOCUMENTI RISK MANAGEMENTI	X		**ALP** **- Settore Legale -**	**MARSH S.P.A.** Viale Bodio, 33 20158 Milano	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI Database del Software DISSERVIZIO	**ALP** **- Settore Legale -**	Personal computer	(*)
GESTIONE EVENTI POTENZIALMENTE AVVERSI, SINISTRI E CORRISPONDENZA RELATIVA	X	X	**ALP** **- Settore Legale -**	**Studio Tecnico Ravinale** C.so Vittorio Emanuele II, 68 10121 Torino **Regione Piemonte** **MARSH S.p.A.** Via Cavour, 1 10123 Torino **MARSH S.p.A.** Via Dante 134 26100 Cremona **MARSH S.p.A.** di Brescia Palazzo Symbol Via Cefalonia, 55 25124 Brescia **VAIANO SRL** Via C. Colombo 7 Torino **FARO Assicurazione ora in LCA e quindi gestita da Commissario Liquidatore**	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI e Database del Software DISSERVIZIO	**ALP** - Settore Legale - **Studio Tecnico Ravinale** di Torino **Regione Piemonte** - Torino **MARSH S.p.A.** di Torino **MARSH S.p.A.** di Cremona **MARSH S.p.A.** di Brescia **VAIANO SRL** di Torino **FARO Assicurazione** di Genova	Personal computer	(*)

A.S.L. V.C.O.
Azienda Sanitaria Locale
del Verbano Cusio Ossola

STRUTTURA COMPLESSA GESTIONE DEGLI AFFARI LEGALI E PATRIMONIALI

				Piazza Piccapietra 73/1 Genova **COMITATO GESTIONE SINISTRI** Presso ASL NO (annualità 2010) **COMITATO GESTIONE SINISTRI** presso A.O.U: "Maggiore della Carità) di Novara (annualità 2011 e **2012)** **STUDIO IES** Via M. Staglieno, 10/11 16129 Genova **LLOYD's SINDACATO NEW LINE** c/o Italian Underwriting Srl Via Borgonuovo, 7 20121 Milano **BRIT SINDACATO LLOYD's** c/o LLOYDI's Rappresentanza per il'Italia Corso Garibaldi, 86 20100 Milano **ITALIAN UNDERWRITING SRL** Via BOorognuovo 7 20121 Milano **MCS S.r.l.** Vicolo Conti, 4 26013 Crema **STUDIO BOLTON & ASSOCIATI** Galleria San Babila 4/a 20122 Milano **CRAWFORD & COMPANY ITALIA SRL** Galleria San Babile, 4/a 20122 Milano		**COMITATO GESTIONE SINISTRI – ASL NO** COMITATO GESTIONE **SINISTRI – A.O.U. "Maggiore della Carità"** di NO **STUDIO IES** – Genova **ITALIAN UNDERWRITING** – Milano **LLOYD'S Rappresentanza per l'Italia** - Milano **ITALIAN UNDERWRITING** – Milano MCS - Crema **STUDIO BOLDON & ASSOCIATI** – Milano **CRAWFORD & COMPANY SRL** – Milano **INA ASSITALIA** –		

A.S.L. V.C.O.
Azienda Sanitaria Locale
del Verbano Cusio Ossola

STRUTTURA COMPLESSA GESTIONE DEGLI AFFARI LEGALI E PATRIMONIALI

				INA ASSITALIA Agenzia di Verbania P.zza San Vittore, 5 28921 Verbania Intra **REALE MUTUA ASSICURAZIONI** Agenzia di Vercelli Via F. Borgogna, 8 13100 Vercelli **UNIPOL ASSICURAZIONI** Agenzia di Omegna Via IV Novembre, 106 28887 Omegna VB **S.S. RISK MANAGEMENT** della ASL "VC" **SS.OO.CC. interne** che detengono la documentazione clinico sanitaria/ oppure alle quali viene affidata l'analisi di alcune problematiche.		Verbania **REALE MUTUA** - Vercelli **UNIPOL** – Omegna **SS.OO.CC. interne** interessate		
GESTIONE ORDINANZE INGIUNZIONI L.R.35/96 E CORRISPONDENZA RELATIVA	X		**ALP** **- Settore Legale -**	**EQUITALIA SERVIZI S.P.A.** Via Benedetto Croce 124 – Roma **E Singoli CONCESSIONARI**	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI e Sito internet EQUITALIA SERVIZI SPA Programma Stato della Riscossione	**ALP** **- Settore Legale -** **EQUITALIA SERVIZI S.P.A.** Via Benedetto Croce 124 – Roma **E Singoli CONCESSIONARI**	Personal computer	(*)
GESTIONE RECUPERO CREDITI VARIA NATURA E CORRISPONDENZA RELATIVA	X		**ALP** **- Settore Legale -**	**EQUITALIA SERVIZI S.P.A.** Via Benedetto Croce 124 – Roma **E Singoli CONCESSIONARI** **Strutture interne: REF**	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI e	**ALP** **- Settore Legale -** **EQUITALIA SERVIZI S.P.A.**	Personal computer	(*)

A.S.L. V.C.O.
Azienda Sanitaria Locale del Verbano Cusio Ossola

STRUTTURA COMPLESSA GESTIONE DEGLI AFFARI LEGALI E PATRIMONIALI

					Sito internet **EQUITALIA SERVIZI** Programma Stato della Riscossione	Via Benedetto Croce 124 – Roma **E Singoli CONCESSIONARI Strutture Interne: REF**		
GESTIONE PARERI LEGALI	X		**ALP - Settore Legale**	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	**ALP - Settore Legale**	Personal computer	(*)
CONTRATTI E VERBALI DI GARA PUBBLICA	X		**ALP**	Nessuna	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	**ALP**	Personal computer	(*)

(*) Rete aziendale protetta tramite Antivirus e Firewall con collegamento a Internet e alla RUPAR mediante validazione degli accessi a livello utente

Data: **21 marzo 2012**

Firma del Responsabile trattamento dati personali
(Dr.ssa Cinzia Meloda)

ASL

S.O.C. SERVIZIO VETERINARIO AREA A

ELENCO TRATTAMENTI DATI PERSONALI

Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture anche esterne che concorrono al trattamento	Eventuale Banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
	S	G						
CORRISPONDENZA verso l'esterno e verso servizi interni	X		VETERINARIO AREA A	B-C	ARCHIVIO INFORMATICO: CARTELLA DOCUMENTI	VETERINARIO AREA A PROTOCOLLO	Personal computer	(*)
SISTEMA INFORMATIVO VETERINARIO			VETERINARIO AREA A	VETERINARIO AREA B C	SIV ARVET	C.E.D. SERVER FARM CSI PIEMONTE – TORINO	Personal Computer	(*)
SERVIZI VETERINARI – MARCHE AURICOLARI BOVINI			VETERINARIO AREA A	VETERINARIO AREA B C	ARVET ANAGRAFE ZOOTECNICA NAZIONALE	SERVER FARM CSI PIEMONTE – TORINO APPLICATIVO WEB IZS TERAMO	Personal Computer	(*)
SCAMBIO, IMPORTAZIONE ED ESPORTAZIONE			VETERINARIO AREA A	VETERINARIO AREA B C	TRACES	APPLICATIVO WEB CEE	Personal Computer	(*)
ANAGRAFE ZOOTECNICA			VETERINARIO AREA A	VETERINARIO AREA B C	ANAGRAFE ZOOTECNICA NAZIONALE	APPLICATIVO WEB IZS TERAMO	Personal Computer	(*)

(*) Rete aziendale protetta tramite Antivirus e Firewall con collegamento a Internet e alla RUPAR mediante validazione degli accessi a livello utente

Data: 20/3/2012

Firma del Responsabile F.F. trattamento dati personali
F.To **(Dott. Germano Cassina)**

ASL

AZIENDA SANITARIA LOCALE DEL VERBANO-CUSIO-OSSOLA

S.O.C. IGIENE E SANITA' PUBBLICA

ELENCO TRATTAMENTI DATI PERSONALI

S.S. EPIDEMIOLOGIA

Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture anche esterne che concorrono al trattamento	Eventuale Banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
	S	G						
ANALISI DEMOGRAFICA ED EPIDEMIOLOGICA	X		S.S. EPIDEMIOLOGIA	Nessuna	MADE	SERVER FARM CSI PIEMONTE - TORINO	Personal Computer	(*)
INDAGINI EPIDEMIOLOGICHE – STATISTICHE SANITARIE	X		S.S. EPIDEMIOLOGIA	Nessuna	EPI INFO, EPIDATA	MS ACCESS	Personal Computer	(*)
STATISTICHE RICOVERI OSPEDALIERI	X		S.S. EPIDEMIOLOGIA	Nessuna		S.S. EPIDEMIOLIGIA	Personal Computer	(*)
BANCA DATI MORTALITA'	X		S.S. EPIDEMIOLOGIA	Nessuna	MS ACCESS	S.S. EPIDEMIOLOGIA	Personal Computer	(*)

(*) Rete aziendale protetta tramite Antivirus e Firewall con collegamento a Internet e alla RUPAR mediante validazione degli accessi a livello utente

Data: 15/3/2012

Firma del Responsabile trattamento dati personali
F.to **(Dott. Paolo Ferrari)**

ASL

STRUTTURA COMPLESSA GESTIONE DELLE RISORSE ECONOMICHE E FINANZIARIE

+ELENCO ATTIVITA' ESTERNALIZZATE

Attività esternalizzata	Descrizione sintetica	Dati personali, sensibili o giudiziari interessati	Soggetto esterno (indicare denominazione ed indirizzo)	Descrizione dei criteri per l'adozione delle misure
RICERCA PRENOTAZIONI X UTENTE				
RICERCA ANAGRAFICA ASSISTITI ASL VCO				
STATISTICHE X CODICI BIANCHI DEA (ADT-WEB)				
CONSULTAZIONE ANAGRAFICA PERSONALE DIPENDENTE				

Data:

Firma del Responsabile f.f. trattamento dati personali
(D.ssa Manuela Succi)

ASL 14

DIREZIONE SANITARIA OSPEDALIERA

ELENCO ATTIVITA' ESTERNALIZZATE

Attività esternalizzata	Descrizione sintetica	Dati personali, sensibili o giudiziari interessati	Soggetto esterno (indicare denominazione ed indirizzo)	Descrizione dei criteri per l'adozione delle misure
ARCHIVIAZIONE CARTELLE CLINICHE	CONSERVAZIONE ED ARCHIVIAZIONE CARTELLE CLINICHE PAZIENTI RICOVERATI NELLE STRUTTURE OSPEDALIERE ASL 14	DATI DI NATURA SANITARIA	ITAL ARCHIVI SRL CENTRO DIREZIONALE . STRADA 6 PALAZZO E2 – ASSAGO ITAL ARCHIVI – LOCALE DEPOSITO - VILLAMAGGIORE - LACCHIARELLA	PER L'ARCHIVIAZIONE: RACCOLTA DELLE CARTELLE CLINICHE IN FALDONI CHIUSI PER IL TRASPORTO A LACCHIARELLA PER LA RICHIESTA AD USO COPIA RICHIESTA PAZIENTE: INVIO ALL'ASL ATTRAVERSO CORRIERE IN BUSTE CHIUSE SIGILLATE.
DIAGNOSTICA	ESAMI DI LABORATORIO	DATI PERSONALI E SENSIBILI	STRUTTURE ESTERNE SIA CONVENZIONATE CHE NON CONVENZIONATE E CENTRI DI RIFERIMENTO REGIONALI	ASSUNZIONE DI RESPONSABILITA' DELLA TUTELA DELLA PRIVACY DA PARTE DELL'ENTE ESTERNO
DIAGNOSTICA	RISONANZA MAGNETICA, PRESTAZIONI DI MEDICINA NUCLEARE	DATI PERSONALI E SENSIBILI	STRUTTURE ESTERNE SIA CONVENZIONATE CHE NON CONVENZIONATE	ASSUNZIONE DI RESPONSABILITA' DELLA TUTELA DELLA PRIVACY DA PARTE DELL'ENTE ESTERNO

Data:

Firma del Responsabile trattamento dati personali
(Dott. Francesco Garufi)

N.B: si è provveduto ad integrare la diagnostica con le prestazioni di medicina nucleare e l'indicazione del soggetto esterno essendo generica comprende tutte le diverse strutture a cui ci si appoggia

ASL TERRITORIALE

STRUTTURA COMPLESSA ASSISTENZA SPECIALISTICA AMBULATORIALE

ELENCO ATTIVITA' ESTERNALIZZATE

Attività esternalizzata	Descrizione sintetica	Dati personali, sensibili o giudiziari interessati	Soggetto esterno (indicare denominazione ed indirizzo)	Descrizione dei criteri per l'adozione delle misure
STIPENDI MEDICI SPECIALISTI AMBULATORIALI	ELABORAZIONE E STAMPA TABULATI PER STIPENDI MENSILI	TUTTI I DATI RELATIVI AGLI STIPENDI: DATI ANAGRAFICI DATI FISCALI DATI PREVIDENZIALI DATI PROFESSIONALI DATI SINDACALI DATI ECONOMICI ALTRI EVENTUALI DATI PER CASI PARTICOLARI	CSI PIEMONTE C.so Unione Sovietica n. 216 – Torino	CONTRATTO ASL14 VCO – CSI PIEMONTE
CONSUNTIVAZIONE	SERVIZIO DI CONSUNTIVAZIONE PRESTAZIONI SPECIALISTICHE	DATI ANAGRAFICI DATI SANITARI DATI ECONOMICI	PROMOZIONE LAVORO VCO CORSO MONETA - DOMODOSSOLA	TRASMISSIONE REGOLAMENTO AZIENDALE DI TUTELA DELLA PRIVACY CON NOTA PROT. 824 DEL 11/09/2003
CALL CENTER	ATTIVITA' DI PRENOTAZINE, SPOSTAMENTO, DISDETTA PRESTAZIONI SPECIALISTICHE AMBULATORIALI	DATI ANAGRAFICI DATI SANITARI DATI ECONOMICI	**** Associazione temporanea di impresa : PROMETEO SRL STRADA CAVALLI 41 BAVENO E AZZURRA SOC. COOPERATIVA arl VIA DELL'INDUSTRIA 1 PIEDIMULERA	

Data: 20/03/2012

Firma del Responsabile trattamento dati personali
(Dott. Francesco Garufi)

ASL

STRUTTURA COMPLESSA RECUPERO RIABILITAZIONE FUNZIONALE

ELENCO ATTIVITA' ESTERNALIZZATE

Attività esternalizzata	Descrizione sintetica	Dati personali, sensibili o giudiziari interessati	Soggetto esterno (indicare denominazione ed indirizzo)	Descrizione dei criteri per l'adozione delle misure
CONSUNTIVAZIONE PRESTAZIONI PER PAZIENTI AMBULATORIALI	SERVIZIO DI CONSUNTIVAZIONE PRESTAZIONI SPECIALISTICHE (MEDICHE E DEI TECNICI DELLA RIABILITAZIONE DELLA S.C. R.R.F. DELLE TRE SEDI: DOMODOSSOLA, VERBANIA, OMEGNA)	DATI ANAGRAFICI DATI SANITARI DATI ECONOMICI	PROMOZIONE LAVORO VCO CORSO MONETA - DOMODOSSOLA	TRASMISSIONE REGOLAMENTO AZIENDALE DI TUTELA DELLA PRIVACY CON NOTA PROT. 824 DEL 11/09/2003

Data: 20 MARZO 2012

Firma del Responsabile f.f. trattamento dati personali
(Dott.ssa Marina Buttè)

ASL GENERALE

STRUTTURA COMPLESSA LABORATORIO ANALISI

ELENCO ATTIVITA' ESTERNALIZZATE

Attività esternalizzata	Descrizione sintetica	Dati personali, sensibili o giudiziari interessati	Soggetto esterno (indicare denominazione ed indirizzo)	Descrizione dei criteri per l'adozione delle misure
ESAMI DI LABORATORIO	INVIO A LABORATORI ESTERNI CAMPIONI ETICHETTATI PER L'ESECUZIONE DI ESAMI NON ESEGUIBILI PRESSO LA ASL14 VCO	DATI SENSIBILI	OSPEDALE MAGGIORE - NOVARA OSPEDALE SANT'ANNA – TORINO OSPEDALE SAN MATTEO - PAVIA	CONTRATTO A CURA DELLA DIREZIONE SANITARIA OSPEDALIERA

Data: anno 2012

Firma del Responsabile trattamento dati personali
(Dott. Nino Cappuccia)

ALLEGATO A-3
COMPOSTO DA 24 PAGG.

Misure adottate presso la server Farm CSI a garanzia di quanto previsto al punto 19.4 (Allegato B D.Lgs.196/2003)

PREMESSA

Nel seguente documento, estratto dal Documento Programmatico sulla Sicurezza (DPS) del CSI Piemonte, vengono descritte le misure tecnico-organizzative, predisposte dal CSI Piemonte, al fine di ridurre al minimo i rischi di distruzione o perdita anche accidentale dei dati personali, di accesso non autorizzato, non consentito o non conforme alle finalità del trattamento.
In particolar modo, sono di seguito descritte le modalità di protezione delle aree e dei locali (sicurezza fisica) nonché le misure di sicurezza adottate per la trasmissione dei dati con specifico riferimento alla rete RUPAR e i criteri a garanzia dell'integrità e della disponibilità dei dati.

1. CRITERI

In questo capitolo sono esposte più dettagliatamente le principali prescrizioni da osservare a garanzia del rispetto dei requisiti di Legge.

~~4.~~1.1 OBIETTIVI GENERALI

Formattati: Elenchi puntati e numerati

Con l'obiettivo di ridurre al minimo i seguenti principali **rischi**:

- distruzione o perdita, anche accidentale, dei dati;
- *accesso, comunicazione e trattamento* di dati non consentito o non conforme alle finalità della raccolta;
- conservazione per un periodo di tempo superiore necessario agli scopi della raccolta o inferiore a quello prescritto dagli obblighi di legge;
- raccolta non autorizzata;
- *diffusione* non autorizzata di dati, know-how e prodotti gestiti e/o realizzati presso il CSI;
- utilizzo dei servizi aziendali disponibili in modo illecito e non finalizzato alle attività aziendali;
- introduzione di elementi (fisici o logici p.e. virus informatici) potenzialmente deterioranti i servizi resi;
- incauto accollo di responsabilità di terzi derivanti da forniture ai Clienti (es. servizi di rete)

devono essere garantite, a seconda delle responsabilità definite, le seguenti attenzioni:

- progettare, allestire e gestire applicazioni e servizi conformemente alle necessità implicite ed esplicite di sicurezza ivi comprese note ed indicazioni da fornire all'Utenza;
- verificare tutti gli aspetti contrattuali relativi alle forniture prestate da CSI verso i Clienti per le responsabilità relative agli aspetti di Sicurezza;
- analogamente prevedere che per le operazioni svolte per conto CSI, si articolino ed esplicitino le opportune responsabilità a carico dei Fornitori;

- custodire il materiale cartaceo relativo ai *dati personali* in armadi o cassetti chiusi a chiave, in modo comunque non accessibile da persone non autorizzate[1];
- utilizzare convenientemente le password individuali di accesso ai *dati personali*;
- subordinare l'accesso, la comunicazione o la modifica dei *dati personali ad una specifica autorizzazione*;
- limitare l'accesso agli *incaricati* per i *dati sensibili*;
- attivare le protezioni da danneggiamento;
- effettuare i salvataggi con cadenze regolari;
- usare programmi antivirus;
- controllare gli accessi ai locali aziendali e all'uso delle apparecchiature e dei servizi.

Le modalità di svolgimento delle Attività del CSI sono conformi a quanto descritto dalle procedure del Sistema Qualità pertanto: **operazioni non descritte in esso e di pertinenza della Sicurezza devono essere esplicitamente autorizzate dal Responsabile del Trattamento dati CSI Piemonte.**

~~Si rimanda al par. 7.6 per la descrizione del~~

1.2 CRITERI TECNICI ED ORGANIZZATIVI DI SICUREZZA FISICA

1.2.1 OBIETTIVI DELLA SICUREZZA FISICA

Il ruolo della sicurezza fisica è quello di proteggere le persone che operano sui sistemi, le aree e le componenti del sistema informativo ed i beni del CSI Piemonte, assicurando altresì il pieno rispetto della legge (D.Lgs.196/2003).

I Criteri relativi al controllo dell'accesso fisico alle diverse aree del CSI Piemonte sono finalizzati a definire:

❖**La Sicurezza di area** che ha il compito di prevenire accessi fisici non autorizzati, danni o interferenze con lo svolgimento dei servizi IT. I Criteri si riferiscono:

- alle protezioni perimetrali dei siti
- ai controlli fisici all'accesso
- alla sicurezza dei locali del Centro di Calcolo (ospitanti in particolare server e apparecchiature di trasmissione dati) rispetto a danneggiamenti accidentali o intenzionali
- alla protezione fisica dei supporti.

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

[1] La custodia è da intendersi estesa ai documenti da avviare al macero

1.2.2 RESPONSABILITA'

La responsabilità della Sicurezza Fisica è del Responsabile dei Servizi Generali Aziendali (RSPP), mentre la messa in opera e supervisione della stessa appartiene all'Unità Organizzativa "Sicurezza Sedi e Gestione Sale Multimediali".
L'Unità organizzativa "Sicurezza Sedi e Gestione Sale Multimediali" con considerazione dei servizi pubblici gestiti da CSI Piemonte:

- definisce ed aggiorna una specifica procedura di controllo accessi;
- segue progettazione, startup e mantenimento in efficienza dei sistemi di sicurezza fisici.

La responsabilità di approvare la procedura di controllo accessi è del Dirigente preposto al Settore Servizi Generali Aziendali.
La procedura è operativa per tutto il personale dell'Unità Organizzativa "Sicurezza Sedi e Gestione Sale Multimediali" ed è estesa al personale operante presso il CED, alla Sorveglianza ed alle Reception delle sedi (composte sia da personale dipendente e sia di personale qualificato esterno).

1.2.3 IMPIANTI

Sistemi Antintrusione, Controllo Accessi e Antincendio

- Antintrusione – Centrali Saet Delphi – SW di supervisione Saet Gemss
- Controllo Accessi – Centrali Tebe - SW di supervisione Saet Gemss
- Antincendio – Sede Centrale e Magazzino – Centrale Notifier AM6300
- Antincendio Altre Sedi: implementati su Saet Delphi
- Supporto rete dati: Vlan Sicurezza riservata e protetta
- Supporto Server: CSI2WKMON e SRVGEMSS01 in Server Farm

Il sistema unica di Supervisione Gemss ha fornito un notevole aumento nelle prestazioni di gestione della sicurezza delle Sedi. Integrando, in un unico SW, antintrusione, antincendio e controllo accessi, permette di integrare le diverse funzionalità su un'unica console.
La struttura si appoggia alla tecnologia Client-Server (SRVGEMSS01) su rete tcp/ip, con diversificazione delle policy d'accesso a seconda del personale operante.
Attivo H24, dotato di diverse procedure di controllo sull'efficienza dei sistemi, permette altresì di gestire eventi anomali e di malfunzionamento da remoto.

Impianti di sicurezza della sede centrale

Presso la Sede Centrale è stato creato un nuovo locale Server dedicato alla Sicurezza Fisica. La sala macchine sicurezza corrisponde al locale T03, ubicato dietro il nuovo corpo Reception- Sorveglianza. L'accesso al locale è monitorato mediante sistema di controllo accessi e le policy riservate al personale autorizzato.

a) Centrale allarmi SAET

E' realizzata con l' impiego di due unità intelligenti master e slave in entrambe con possibilità di scambiare la gestione del sistema dall' una all'altra in modo da garantire la continuità di funzionamento in caso di guasto (sistema in ridondanza di backup).
L'interfaccia verso l'operatore è assicurata da client Gemss installati su PC Mitas, tramite tecnologia client- server.
Il funzionamento del tipo interattivo consente di visualizzare opportune maschere video per una facile guida alla gestione del sistema.
Sul monitor a colori in caso di allarme compaiono le piantine delle aree controllate, con la specifica dell'evento di intrusione. Oltre a ciò vengono gestiti anche gli allarmi relativi al:

allarme antincendio/antiallagamento per CED e Magazzino, Sale Condizionamento
allarme bagni handicappati P.T.

Nel corso dell'anno 2008 saranno approntate misure di sicurezza aggiuntive in vista della ristrutturazione dell'area Ced, mediante installazione di barriere ad infrarossi e mediante potenziamento dell'attuale struttura perimetrale del Data Center, con la creazione di un anello di sicurezza controllato da bussole di regolazione del flusso.

b) Impianto TVCC
Il Sistema TVCC di Video controllo è composto da telecamere suddivise in Area Esterna ed Area Interna. L'Area Esterna è totalmente coperta mediante l'ausilio di telecamere fisse e n. 2 telecamere brandeggianti. Tutti i cancelli carrai sono dotati di telecamera fissa che consentono l'identificazione dei mezzi in ingresso.
L'Area Interna è totalmente coperta da telecamere fisse per quanto concerne le aree di passaggio dei piani principali (corridoi, androni ascensori). Tutte le porte d'accesso dall'esterno sono dotati di telecamera fissa, con coordinamento del citofono relativo.

c) Impianto anti- intrusione
Il Sistema anti- intrusione, composto da barriere a microonde, radar volumetrici e sensori porta, è coordinato funzionalmente con il Sistema TVCC, pertanto anch'esso è suddiviso in Area Esterna ed Area Interna. L'Area Esterna è dotata di barriere a microonde che proteggono totalmente le aree di passaggio e che nel rilevare il movimento di persone o cose coordinano la telecamera di zona sui monitor della Sorveglianza.
L'Area Interna è dotata di radar volumetrici e sensori porta con visualizzazione singola su planimetria presso il Personal Computer di controllo della Sorveglianza, con coordinamento per zone al Sistema TVCC rispetto alla telecamera di zona. Pertanto l'allarme di un radar o di un sensore viene rilevato su planimetria e contestualmente appare in Sorveglianza sui monitor di controllo l'immagine della telecamera più prossima al sensore o radar in allarme.

d) Controllo Accessi
Il nuovo Sistema di Controllo Accessi è dotato di un Personal Computer presso la Sorveglianza che contestualmente al passaggio di una persona o autovettura presso un accesso controllato ne visualizza i dati, la foto e coordina la telecamera relativa su monitor di controllo.
Le aree interne particolarmente a rischio sono protette da radar volumetrici e sensori porta atti a rilevare intrusioni, tutti collegati a impianto TVCC e relativo sistema registrazione eventi.

e) Sistema Antincendio
Il Sistema Antincendio copre l'intero edificio, conferendo maggior protezione presso le aree dichiarate sensibili, mediante anche l'ausilio di sensori d'allagamento, controlli della temperatura e cavi termosensibili. Le aree di particolare rilevanza sono:

Area Tecnologica C.so Unione Sovietica 218
CED (Sala Macchine) piano interrato di C.so Unione Sovietica 216

Presso le sedi del CSI sono dislocate secondo norma apparecchiature antincendio quali estintori e prese d'acqua per spegnimenti.

f) Sistema Human Detection
Il Sistema Human Detection si integra con l'attuale sistema TVCC mediante un particolare Server di elaborazione delle immagini. Posto a difesa perimetrale della Sede Centrale, consente di identificare la presenza umana e di veicoli, discrimandole dalle restanti forme e figure. Il SW di supervisione è reso disponibile alla Sorveglianza, mediante PC Client.

f) Impianti elettrici Sala Macchine e Area Tecnologica
L'alimentazione elettrica di tutte le unità di Sala Macchine è garantita da 6 quadri di distribuzione in campo, ed in taluni casi con doppia alimentazione proveniente da quadri diversi, collegati ad un sistema di continuità assoluta composto da 2 inverter rotanti Piller UBS 420 in ridondanza parallela, ciascuno in grado di supportare l'intero carico in sede di manutenzione o per emergenze sulla singola macchina. Ciascun inverter è dotato di una catena di batterie al piombo di 204 elementi, in grado di assicurare un'autonomia di 20 minuti a pieno carico (l'attuale carico del CED consente un'autonomia di batteria di circa 40 minuti).
L'alimentazione a monte del sistema è dotata di un sistema di commutazione automatica rete-gruppo elettrogeno che provvede in caso di assenza rete a gestire tutti i processi in modo automatico relativi all'avviamento del gruppo elettrogeno, della commutazione rete-gruppo e relativo rientro al ritorno della rete.
L'autonomia del gruppo elettrogeno con serbatoi gasolio pieni è di circa 12 ore e il riempimento dei medesimi è effettuabile a gruppo elettrogeno funzionante.
La sicurezza e il monitoraggio tecnologico degli impianti elettrici è gestita tramite software apposito di supervisione, il cui client è reso a disposizione del Sorvegliante, ed attivo H24.

g) Climatizzazione locali CED
Il condizionamento all'interno dei locali del CED è effettuato mediante impiego di 2 sistemi termici:
raffreddamento locale mediante 10 Hiros/denco ad aspirazione superiore e a ventilazione forzata nel cavedio sottopavimento, allacciati al sistema idrico della centrale frigorifera. Le tubazioni di detto impianto sono integralmente aeree e pertanto visibili ed ispezionabili a vista nonché sezionabili in vari punti e per ciascuna macchina;
ricambio aria primaria mediante UTA sita nei locali adiacenti magazzino con presa aria esterna e trattamento temperatura a 20° C ed umidità 45% in normale funzionamento (con possibilità di modifica dei parametri).
La centrale frigorifera è composta da n. 3 frigoriferi TRANE di recente installazione (1998-99) e di n. 1 frigorifero SEVESO acquisito nel 1996 dal Comune di Torino: le risorse di tale complesso vengono gestite, in considerazione del fatto che nella stagione estiva erogano servizio anche per gli uffici, in modo da dare priorità massima ai locali del CED.

1.2.4 SORVEGLIANZA

Il servizio di Vigilanza (Sorveglianza) è soggetto alla normativa di cui agli artt. 133-141 del R.D. n. 773/31 (T.U.L.P.S.).
La Sorveglianza H24 della Sede, tramite impiego di guardie giurate, ha il compito di prevenire accessi fisici non autorizzati, danni o interferenze ai luoghi di lavoro.
Il servizio si avvale dell'ausilio di sistemi tecnologici atti a controllare il perimetro esterno, l'accesso fisico delle persone e dei materiali, i percorsi interni e gli accessi alle aree protette.
Le procedure di accesso alla Sede sono descritte in dettaglio all' articolo 4 del "Manuale del Servizio di Sorveglianza".
La responsabilità sull'esecuzione del servizio appartiene al Responsabile dei Servizi Generali Aziendali, su direttiva della propria Direzione.

Il servizio consiste nell'assicurare la tutela della sicurezza dei beni e del personale del CSI Piemonte oltre che nell'analisi e nella determinazione delle soluzioni tecniche e/o organizzative più idonee per svolgere i compiti assegnati con efficacia ed efficienza.

Il servizio di Sorveglianza viene svolto con idoneo personale di presidio presso le sedi del CSI-Piemonte, secondo modalità e orari indicati all'art. 2 del Capitolato Speciale d'Appalto – "Requisiti Tecnici".
In particolare in tale documento è riportato quanto concerne i servizi di:
Vigilanza, per attività di piantonamento armato,
Reception, svolto da operatori specializzati, consistente in attività di accoglienza, registrazione, informazione ed accompagnamento ospiti - ove richiesto - all'interno degli uffici

Compito principale del personale di Sorveglianza e Reception è quello di controllare, anche con l'uso degli impianti e delle apparecchiature elettroniche di sicurezza (TVCC, sensori, rilevatori accessi,barriere volumetriche, ecc.), l'ingresso del personale dipendente, collaboratori, pubblico, al fine di evitare l'accesso agli immobili di persone non autorizzate.

Il servizio è espletato assicurando il costante controllo della struttura da sorvegliare.
Il personale di servizio, di norma, staziona nella sala controllo o presso la reception di sede, a verificare che durante il turno di lavoro tutto si svolga nel migliore dei modi, e secondo le istruzioni operative concordate. A tale scopo è necessario che all'inizio del turno si informi se per il turno di competenza, vi siano delle consegne particolari. Presa visione di ciò viene comunicato alla centrale Operativa di competenza l'inizio del servizio. Su apposito registro inoltre si provvede a registrare l'espletamento del proprio turno e tutti gli eventi che si verificano durante l'espletamento del servizio. Per eventi straordinari è prevista la compilazione anche del "Rapporto di servizio". Durante il servizio si provvede a rispondere alle chiamate della centrale Operativa e vigilare attentamente la struttura ed a procedere ad apposito controllo ed eventuale segnalazione alla Centrale operativa ogni qualvolta venga notato qualcosa di sospetto.
Il servizio di piantonamento armato garantisce:

- controllo degli accessi attraverso l'utilizzo della tecnologia passiva. In particolare le guardie armate devono controllare, anche con l'uso di eventuali apparecchiature elettroniche, l'ingresso del pubblico (e, per i passi carrai, degli automezzi) evitando l'introduzione di armi od oggetti contundenti (per le sedi di presidio), procedendo se del caso all'identificazione, avvalendosi dell'ausilio della Forza Pubblica nel rispetto delle disposizioni del T.U.L.P.S.;
- controllo dei movimenti di merci e persone, con presenza alle opere di carico/scarico merci ovvero "a distanza" con utilizzo della tecnologia messa a disposizione dal CSI Piemonte (TVCC, sistemi antintrusione, controllo accessi, human detection);
- ispezione ai locali delle sedi, con ronde interne giorno/notte. Le ronde hanno lo scopo di prevenire situazioni anomale e di garantire la sicurezza dei locali, sia per antintrusione che per prevenzione incendi (vie d'esodo ostruite, porte allarmate in stato di chiuso, porte e/o finestre comunicanti direttamente con piano strada esterno regolarmente chiuse, manomissione impianti di sicurezza, ecc...);
- intervento, entro i 15 minuti dall'"all'erta",di proprie radiopattuglie a seguito di allarmi intrusione per le sedi del CSI Piemonte in Torino, con relativa ispezione dei locali di dette sedi;
- messa in allerta, coordinamento, collaborazione e interazione con radiopattuglie degli Istituti di Vigilanza in loco per le sedi del CSI Piemonte site in Cuneo, Novara, Vercelli (e/o altre sedi si dovessero successivamente aggiungere), di cui il CSI Piemonte fornirà i riferimenti utili, in caso di segnalazioni di allarme di intrusione e/o incendio provenienti dalle stesse;
- eventuale segnalazione alle Autorità di P.S., a seguito di eventi dolosi;
- eventuale segnalazione e attivazione dei VV.FF., a seguito di pericolo di incendi e/o altre calamità;
- eventuale chiamata al 118, per interventi di pronto soccorso di persone presenti nelle sedi del CSI Piemonte;
- ispezione, all'inizio, durante e alla fine della giornata, di tutti i locali delle sedi oggetto del servizio di presidio e/o a seguito di allarmi, attivazione radiopattuglie, sulle sedi decentrate in Torino anche non direttamente presidiate;

Gli addetti (di norma personale esterno) alla Reception devono:

- registrare su supporto informatico, fornito da CSI Piemonte, in ingresso ed uscita i visitatori, fornitori e clienti non provvisti di badge, verificandone i dati da documento di riconoscimento: al termine di ogni giornata lavorativa deve essere attuato il back-up e l'archiviazione in sicurezza dei dati sui supporti informatici e secondo le modalità indicate dal CSI;
- informare i visitatori, fornitori e clienti, ai sensi del D.Lgs.626/94, della necessità di visionare le planimetrie di sicurezza all'interno dell'edificio (indicazione vie d'esodo più vicine), richiedendone contestualmente controfirma per presa visione;
- avvisare tempestivamente il personale interessato dell'arrivo dei visitatori, fornitori o clienti, al fine di rendere minimi i tempi di attesa e farsi autorizzare l'accesso degli esterni;
- indicare agli stessi il percorso migliore per accedere all'ufficio interessato;
- avvisare la Segreteria di competenza, nel caso di ospiti, visitatori, fornitori, clienti per gli uffici Direzionali e/o aree "riservate", e curare il loro accompagnamento, salvo diversa disposizione;

- collaborare con il servizio di Sorveglianza, per segnalare e/o prevenire situazioni di rischio, per chiamate di emergenza;
- rendersi attivi con il Servizio di Prevenzione e Protezione interno, specialmente per le procedure di evacuazione degli immobili a seguito di pericolo di incendio e/o altre calamità;
- inoltrare all'ufficio Protocollo la posta in arrivo e/o eventuali notifiche giudiziarie (ad uffici chiusi avvisare il Responsabile di riferimento del CSI Piemonte);
- consentire telefonate di cortesia ad esterni autorizzati;
- avvisare il Ricevimento Merci dell'arrivo di eventuali corrieri per consegna materiale.

1.2.5 ACCESSO ALLE SEDI

L'accesso e la permanenza nelle Sedi aziendali del CSI Piemonte è consentito, secondo le regole più oltre indicate, alle seguenti tipologie di persone:

- dipendenti, interinali, stagisti, collaboratori a progetto;
- collaboratori esterni e consulenti;
- ospiti, visitatori;
- fornitori, trasportatori, corrieri;
- maestranze dei cantieri.

Per ognuna delle suddette tipologie il servizio di Vigilanza/Reception opera i necessari controlli di accesso, come di seguito specificato.

Dipendenti, interinali, stagisti, collaboratori a progetto
Sono dotati di badge aziendale a seguito di comunicazione di inizio rapporto lavorativo da parte dell'Ufficio Personale. Sono autorizzati all'accesso e alla permanenza nei propri uffici senza limiti di orario nei giorni feriali e fino alle ore 15,00 del sabato nelle sedi di Torino C.so Unione Sovietica 216 e C.so Tazzoli 215/12, ove esiste piantonamento con vigilanza h/24: occorre invece specifico permesso nei giorni festivi e dopo le ore 15,00 del sabato, da richiedersi tramite posta elettronica alla Sorveglianza/Reception da parte del rispettivo Responsabile, con indicata la motivazione. Per le altre Sedi l'accesso e la permanenza possono avvenire nei seguenti orari: giorni feriali con orario 8,15/21,00 e il sabato con orario 8,15/15,00.
Ogni dipendente/interinale/stagista dotato di badge è responsabile della custodia del medesimo e deve dare pronta comunicazione in caso di furto o smarrimento alla Reception.
La Sorveglianza può richiedere all'ingresso e/o all'uscita dalla Sede di ispezionare il contenuto di borse, sacche, cartelle, .

Collaboratori esterni e consulenti
Sono dotati di badge aziendale e autorizzati all'accesso esclusivamente per il periodo contrattuale, stabilito dalla Direzione richiedente e comunicato dall'Ufficio Commesse Esterne prima dell'inizio del rapporto di lavoro. Per questi lavoratori valgono le stesse regole di accesso e permanenza negli uffici indicati per i dipendenti. Collaboratori esterni sprovvisti di badge possono entrare solo come "visitatori" e la Vigilanza/Reception comunicherà al Responsabile del Servizio Prevenzione e Protezione la loro presenza:

sarà sua cura verificare con Commesse Esterne il periodo di presenza, provvedendo se necessario al tesseramento.
Ogni collaboratore dotato di badge è responsabile della custodia del medesimo e deve dare pronta comunicazione in caso di furto o smarrimento alla Reception.
La sorveglianza può richiedere all'ingresso e/o all'uscita dalla Sede di ispezionare il contenuto di borse, sacche, cartelle, ...

Ospiti, visitatori
Il servizio di Vigilanza cura l'accettazione di ospiti/visitatori presso gli ingressi principali di ogni Sede, registrando su apposito software dedicato i seguenti dati:
- data visita con precisazione di ora entrata/uscita
- dati anagrafici della persona
- ente e/o azienda di appartenenza
- ufficio o persona dipendente con cui intende conferire

Alla persona, prima di accedere agli uffici, deve essere fatto firmare apposito modulo, per presa conoscenza delle misure antincendio di palazzo (planimetrie vie di fuga e punti di raccolta). Il personale di Vigilanza/Reception deve fornire le necessarie indicazioni in merito all'ubicazione delle vie di fuga e al comportamento da tenere in caso di allarme ed evacuazione.
Prima di consentire l'accesso alla persona, la Vigilanza/Reception ne deve sempre annunciare l'arrivo al personale dell'ufficio richiesto e solo dopo avvenuto consenso lasciarla entrare ed indirizzarla alla destinazione richiesta.
Se la persona intende conferire con personale dirigente del CSI Piemonte, l'operatore di Reception deve chiamare la segreteria del dirigente medesimo e, su richiesta di questa e/o a discrezione della Reception, accompagnare la persona a destinazione. Alla persona, se non accompagnata, va indicato il percorso migliore per accedere all'ufficio richiesto.
La sorveglianza può richiedere all'ingresso e/o all'uscita dalla Sede di ispezionare il contenuto di borse, sacche, cartelle: la presenza di personal computer e/o altre apparecchiature elettroniche di proprietà del visitatore deve sempre essere rilevata e registrata in ingresso su apposito modulo (fornito dal servizio reception) e poi verificata come riscontro in uscita.
L'ospite/visitatore, se dotato di badge fornitogli per l'accesso, è responsabile della custodia del medesimo e deve dare pronta comunicazione in caso di furto o smarrimento alla Reception.

Fornitori, trasportatori, corrieri
In caso di fornitura di servizi o di beni per i quali espressamente non è prevista la consegna a Magazzino, il fornitore può accedere per la consegna all'interno delle Sedi solo previa registrazione presso la Reception, che controlla prima dell'inizio dello scarico e/o del carico merci, l'effettiva legittimità della fornitura (ordine, ragione sociale del mittente, ecc...).
Lo scarico o il prelievo di merci da parte di fornitori deve sempre avvenire in presenza del personale preposto al controllo (personale interno del CSI Piemonte): in assenza, i fornitori possono procedere al carico/scarico solo in presenza personale di Vigilanza, che provvederà ad indicare anche il luogo di scarico più idoneo.
In questo caso è necessario che la Reception, all'arrivo del materiale, controlli la corrispondenza del numero dei colli e la loro integrità con quanto segnalato sul documento di trasporto e successivamente firmi tale documento apportando la dicitura

"accettazione con riserva" (uso apposito timbro inchiostrato in dotazione) congedando il trasportatore. Copia del documento di trasporto deve tempestivamente essere inviata al Servizio Movimentazione Merci di c.so Tazzoli 215/15. Il Servizio Movimentazione Merci informerà la Reception se è necessario che il materiale segua la procedura cespiti e provvederà in merito.
Il materiale in uscita deve essere accompagnato da apposito documento di trasporto, che la Reception deve verificare per la necessaria autorizzazione alla fuoriuscita merci. In assenza del documento di trasporto, dovrà mettersi in contatto con il Servizio Movimentazione Merci del Magazzino di c.so Tazzoli 215/15. Copia del documento di trasporto in uscita dovrà riportare "visto autorizzazione Uscita Merci" da parte dell'addetto di Reception.
Il fornitore, se dotato di badge fornitogli per l'accesso, è responsabile della custodia del medesimo e deve dare pronta comunicazione in caso di furto o smarrimento alla Reception.

Maestranze dei cantieri
Le maestranze di ditte esterne impegnate nei lavori nelle aree dei cantieri, verranno munite di apposito badge di riconoscimento, senza il quale non potranno accedere al cantiere. Detto badge dovrà essere ritirato, prima dell'inizio dei lavori, presso la Reception all'inizio della giornata lavorativa, previa consegna di documento di riconoscimento personale, che verrà restituito al lavoratore previa riconsegna del badge CSI all'uscita dalla Sede. La Reception, su apposito "registro di Cantiere" elettronico, installato sul personal computer in dotazione al servizio, annoterà le seguenti informazioni (quelle contrassegnate con * sono anche riportate sul badge):

- cognome nome (*)
- ditta di appartenenza (*)
- denominazione cantiere
- zona di cantiere autorizzata (*)
- orario di entrata ed uscita

Se nell'anagrafica precaricata sul programma "accesso cantieri" non si rileva il nominativo del lavoratore, la Reception non gli consente l'accesso e avvisa il Responsabile del Servizio Prevenzione e Protezione, per farsi autorizzare in merito all'accesso richiesto.
I lavoratori addetti ai cantieri sono soggetti a controllo da parte della Vigilanza interna che verificherà che la zona in cui si trovano sia conforme a quella autorizzata, indicata sul badge CSI loro fornito che dovranno portare in modo "visibile" (dotazione di apposito porta-badge con cordoncino e pinza): lavoratori trovati impropriamente fuori della/e zona/e autorizzata/e saranno allontanati e del fatto sarà dato avviso al Responsabile del Servizio Prevenzione e Protezione. Le zone sono identificate con le stesse sigle utilizzate per denominare le aree "Antincendio".
Ogni addetto dotato di badge è responsabile della custodia del medesimo e deve dare pronta comunicazione in caso di furto o smarrimento alla Reception. Non potrà accedere al cantiere senza essere sottoposto a nuovo tesseramento, che avverrà solo previa "autocertificazione" del motivo per cui ne è sprovvisto.
L'Appaltatore dovrà tempestivamente comunicare ogni variazione che si dovesse verificare tra il suo personale impiegato nell'appalto.
Lavoratori occasionali al cantiere (non continuativi e/o fornitori estemporanei dell'Appaltatore) saranno registrati come visitatori in accesso al cantiere e saranno forniti di badge Visitatore a seguito del rilascio di un documento di identità.

Il Responsabile del Servizio Prevenzione e Protezione si riserva la facoltà di pretendere l'allontanamento del personale dell'Appaltatore che contravvenga ai propri doveri di sicurezza o che non rispetti norme e regolamenti in tema di sicurezza.
La sorveglianza può richiedere all'ingresso e/o all'uscita dalla Sede di ispezionare il contenuto di borse, sacche, cartelle, ...

1.2.6 AREE A ACCESSO CONTROLLATO

Per i locali più critici (aree protette e/o riservate ospitanti server ed apparecchiature di TLC) vale quanto segue:

- vi è controllo diretto o tramite videocamera;
- le porte di ingresso sono controllate tramite lettore badge di prossimità e TVCC collegata direttamente dalla Sorveglianza;
- l'accesso è consentito solo alle persone preventivamente accreditate e autorizzate;
- i tecnici di ditte esterne accreditate, muniti di apposito badge di riconoscimento individuale, possono accedere a tali locali solo dopo avviso e conseguente autorizzazione del personale CED;
- i visitatori possono accedere alle aree protette, in presenza degli operatori CED e, in assenza di questi, devono essere accompagnati ma solo previa autorizzazione del responsabile CED

Il badge di accesso ai locali protetti, qualora non sia di persona dipendente, non può essere portato all'esterno della sede CSI Piemonte e viene ritirato solo previa consegna del documento di riconoscimento individuale del tecnico o visitatore, di cui la sorveglianza ne verifica corrispondenza con i dati del badge medesimo.

CED- Data Center

Il Data Center (locale ove risiedono le principali apparecchiature di calcolo) è collocata presso il Centro di Calcolo nella sede di Corso Unione Sovietica 216.
Essendo indubbiamente il locale più a rischio dell'intera azienda per esso valgono criteri molto rigorosi che ne regolano gli accessi.
L'accesso ai locali del Data Center è consentito esclusivamente al personale dipendente autorizzato e preventivamente stabilito dalla Direzione competente.
In tutti gli altri casi l'accesso dovrà avvenire esclusivamente mediante accompagnamento di sicurezza da parte del personale dipendente autorizzato, previo avviso al personale operativo del CED.
Durante gli orari di presidio operativo l'accesso alla Sala Server è limitato agli operatori della Sala Macchine, al personale sistemistico e al personale (interno od esterno) autorizzato. Attività estemporanee svolte da personale interno presso la Sala Server avverranno dopo eventuale verifica del responsabile di sala macchina e sotto il controllo dell'Operativo.
L'ingresso nell'area CED (o Sala Macchine) ed in particolare alla Sala Server è in generale regolamentato come segue:

il personale dipendente, preventivamente autorizzato all'accesso all'area CED e/o sala Server ha il proprio badge aziendale magnetico abilitato per l'accesso in dette aree e comunque per l'apertura della sola entrata principale (centrale) della sala server. L'autorizzazione per il consenso ai badge viene preventivamente concordata dal Responsabile Servizi Generali e la Direzione del CED;
il visitatore esterno (tecnico di assistenza hardware - software e/o operaio addetto alla manutenzione delle sedi) è preventivamente registrati in reception e successivamente annunciato telefonicamente agli operatori CED;
avuto assenso dagli operatori, il visitatore viene dotato di pass numerato (appositamente per accesso area CED e diverso quindi da quelli per accesso ad altri uffici delle sedi). Detto pass dovrà essere presentato agli operatori CED per autorizzazione e rilascio badge elettronico di accesso alla Sala Server;
gli operatori CED devono completare tramite procedura condivisa da reception, i dati dell'orario di ingresso e di uscita alla Sala Server. Al visitatore viene ritirato il pass della reception e consegnato il badge di accesso alla Sala Server. Al termine della visita, il visitatore deve restituire il badge agli operatori CED che contestualmente restituiscono il pass utile per il ritiro dei documenti personali presso la reception. Gli operatori registrano l'ora di fine visita certificandolo con la propria sigla sul software in linea. Nel caso l'esterno uscisse dalla sala Server e si dimenticasse di restituire il badge agli operatori CED, verrebbe bloccato dai sorveglianti, in quanto mancherebbe l'ora e la sigla di uscita dalla sala server.

In aggiunta a questa procedura resta di responsabilità della Sorveglianza, controllare gli accessi in CSI e controllare la siglatura da parte degli operatori, che attesti la effettiva restituzione del badge.

Nei casi di visite guidate al CED i visitatori vengono accompagnati personalmente dalla guardia particolare giurata.

Con questa procedura si evitano gli accessi multipli ed indesiderati, inoltre alla fine di ogni turno sarà compito degli operatori CED verificare che tutti gli accessi abbiano la giusta corrispondenza con le uscite. In caso contrario risulta semplice intuire che qualcuno sta ancora stazionando in sala Server e quindi si renderà necessario controllare attentamente e avvisare prontamente la Sorveglianza.

La porta di ingresso alla sala Server lato ascensore in fondo alla sala server è disabilitata a tutti tranne personale CED, personale Servizi Generali, personale di Sorveglianza ed alla persona addetta alle pulizie del locale.

Durante lo svolgimento delle attività presso la Sala Server vale quanto segue:
- deve essere presente sempre un responsabile (anche pro-tempore) dell'area in caso di accesso da parte di personale non addetto;
- il locale deve essere mantenuto chiuso anche quando presidiato dal personale operativo;
- l'accesso deve essere consentito solo alle persone autorizzate dal Dirigente Responsabile del CED;
- l'accesso deve essere possibile solo dall'interno dell'area sotto la responsabilità di CSI Piemonte ed eventuali uscite di sicurezza devono essere allarmate;
- l'accesso all'area di norma deve avvenire tramite il lettore di badge;

Durante i periodi di assenza del presidio operativo l'accesso alla Sala Server è possibile solo al personale:

- della Sorveglianza,
- della UO Sicurezza Sedi e Gestione Sale Multimediali
- dei Reperibili della Sicurezza
- Sistemistico in reperibilità e alle eventuali persone da questo coinvolte in interventi straordinari di ripristino,
- appartenente a ditte esterne nominativamente autorizzato e con elenco depositato presso la Sorveglianza dopo essere stato controllato dal Responsabile dei Servizi Generali.

Anche nel caso di assenza del presidio operativo la Sorveglianza, e a maggior ragione, prima di consentire l'accesso ai locali del Centro di Calcolo e quindi alla Sala Server, procede con l'identificazione certa delle persone garantendo anche l'attuazione delle principali attenzioni (porte chiuse, videosorveglianza etc.).

1.2.7 STRUMENTAZIONE AUSILIARIA DI SORVEGLIANZA

Le telecamere sono presenti quale ausilio al personale della Sorveglianza per il controllo dei locali e delle aree più critiche nonché presso delle sedi decentrate essendo queste sprovviste di personale di Sorveglianza.
In osservanza a quanto prescritto dalla legge sulla privacy, nelle aree interne delle sedi, presidiate da telecamere, sono stati affissi cartelli indicatori che informano della presenza delle medesime.
Gli scopi di utilizzo delle telecamere interne sono esclusivamente la salvaguardia delle persone e dei beni del CSI Piemonte.
Le registrazioni filmate sono relative esclusivamente alle aree di passaggio comune (corridoi, scale, ingressi) e alle aree riservate e considerate a rischio. In dette aree si è avuta l'avvertenza di non riprendere le situazioni di lavoro, ma solo esclusivamente il transito delle persone (per altro registrato anche dal rilevatore a controllo badge delle aree protette).

Se necessario, per conservarne storia è possibile scaricare su supporto magnetico eventi ritenuti utili per la sicurezza interna ed eventuali verifiche su indicazione della Direzione Amministrazione e Servizi Generali.

Le procedure di video-registrazione, prevedono di conservare i dati prodotti per un periodo conforme alla normativa. Le procedure di registrazione visitatori prevedono viceversa una tenuta dei dati di un anno.
Trascorsi detti periodi i dati sono distrutti.

Le registrazioni video vengono archiviate in locale di sicurezza e possono essere visibili solo dagli Incaricati al Trattamento e/o dalle Autorità di Polizia Giudiziaria.

Il personale di Sorveglianza è tenuto alla riservatezza e quindi a non comunicare a terzi i fatti di cui vengono a conoscenza.

Le stampe di materiale contenenti dati personali e i supporti magnetici già utilizzati per archivi contenenti dati personali, vengono raccolti in appositi contenitori posizionati in aree ad accesso controllato e distrutti con garanzia del rispetto della legge sulla privacy.

1.2.8 APPARECCHIATURE INFORMATICHE CRITICHE

Sono considerate apparecchiature informatiche critiche ai fini della sicurezza le seguenti apparecchiature:

- tutti i Computer (escluse quelli ad uso esclusivamente personale che non dispongano della possibilità di collegarsi in rete): PC, work-station e server.
- apparecchiature per il collegamento dei canali, system o master console, unità dischi ottici e magnetici e nastri;
- Bridge, Gateway, Repeater, Router, Wiring hub;
- Performance e trace tool, Sniffer, protocol analyzer;
- porte di collegamento principali (backbone);
- apparecchiature per la crittografia e per l'emissione di badge, certificati etc.

Le apparecchiature delle LAN (Wiring hub, MAU, ecc.) non facenti parte del backbone e non situate nelle aree ad accesso controllate, devono essere riposte almeno all'interno di armadi chiusi a chiave.

1.2.9 SUPPORTI DI MEMORIZZAZIONE

Sono considerati supporti di memorizzazione i nastri magnetici, i dischi magnetici o ottici amovibili, i CD-ROM che contengono informazioni personali.
I supporti contenenti dati sensibili devono (DLgs 196/03) essere custoditi in un'area ad accesso controllato o in un ufficio che sia chiuso quando non presidiato o in un armadio/cassetto chiuso a chiave.
I supporti usati per i backup devono essere custoditi presso il CED in cassaforte ed in copia presso la sede di C.so Tazzoli 215.
E' compito delle funzioni Sistemistiche ed Operative l'individuazione delle copie di back-up di tutti i sistemi server da trasmettere in copia presso la sede di C.so Tazzoli 215 per l'assoluta garanzia di integrità e conservazione dei dati gestiti.
In fase progettazione dei servizi occorre garantire agli archivi contenuti una disponibilità nel tempo conforme a quanto convenuto con i Clienti e con riferimento alle prescrizioni di legge.

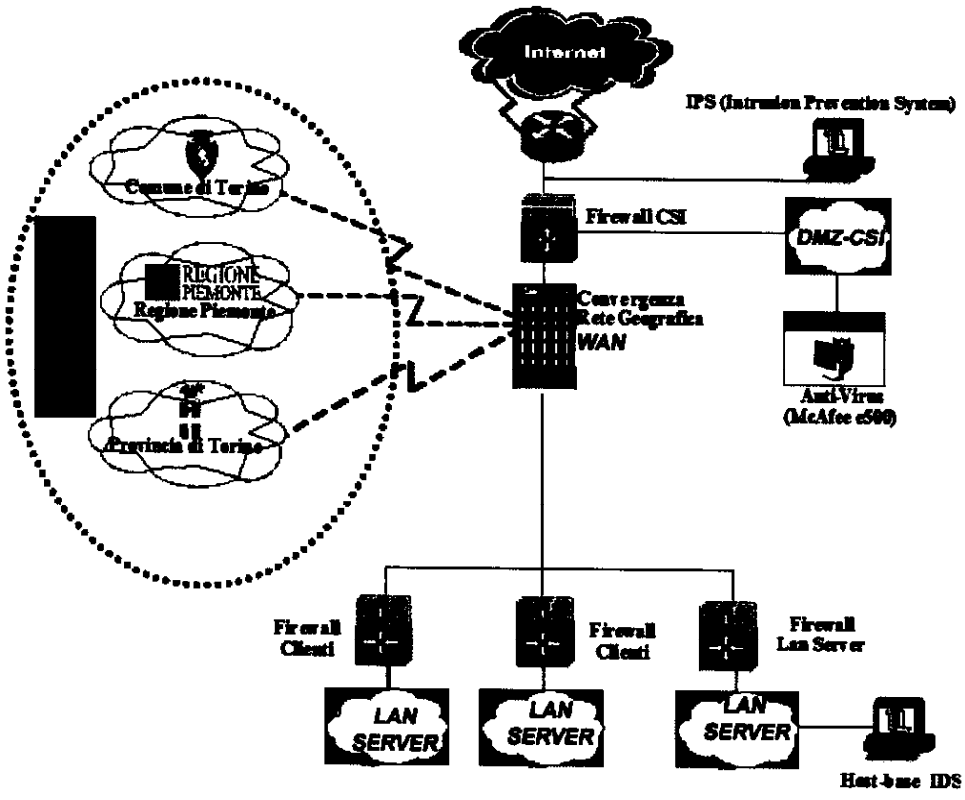
Sono definite informazioni residue quei dati personali ancora leggibili dopo la cessazione di un trattamento. (es. nastri, dischi magnetici, dischi ottici, ecc.).
Per riutilizzare un supporto di memorizzazioni contenenti dati personali, occorre rendere impossibile il recupero dei dati precedentemente memorizzati, anche mediante processi di sovrascrittura o formattazione a basso livello.
Gli Hard-Disk devono essere formattati prima della riassegnazione del pc ad altro Utente.

Dischi ottici e CD devono essere distrutti alla fine del trattamento.

1.3 CRITERI PER LA SICUREZZA DELLE TRASMISSIONI

1.3.1 PROTEZIONI SUI COLLEGAMENTI IN RETE

L'implementazione della Sicurezza delle Trasmissioni è basata sull'infrastruttura esposta di seguito:



1.3.2 CRITERI PER LA SICUREZZA DELLE TRASMISSIONI

La rete rappresenta una infrastruttura tecnologica comune ed utilizzata da più Utenti e da più comunicazioni contemporaneamente: a partire da tale considerazione sono state individuate le seguenti principali norme da seguirsi per la Sicurezza per le Trasmissioni.

- I client interni alla LAN devono avere, di norma, un indirizzo privato: specifiche esigenze di servizio devono essere valutate da Sicurezza e Reti.
- Tutti i server che devono essere raggiunti solo da HOST appartenenti alla rete INTRANET devono avere indirizzi privati
- Tutti i server che devono essere raggiunti da HOST appartenenti alla rete INTERNET devono avere indirizzi pubblici e posti su DMZ. In alternativa, se collocati su reti interne, devono essere protetti con specifici firewall o con opportune misure di sicurezza.
- La rete INTRANET e INTERNET devono essere fisicamente separate in modo tale da evitare che utenti esterni sfruttino un indirizzo pubblico di un server interno per collegarsi sulla rete INTRANET del CSI.
- Un servizio verso INTERNET che si vuole rendere disponibile a partire dalla rete INTRANET, deve usare o un PROXY SERVER o NAT (Network Address Translation).
- Le reti dei Clienti RUPAR devono essere protette da dispositivi Firewall le cui policy devono essere definite concordemente con i responsabili definiti dai Clienti.
- Le policy di accesso tengono conto dei dispositivi il cui colloquio deve, se possibile, essere abilitato anche in funzione del periodo orario.
- Le vulnerabilità dei Firewall costituiscono parte costante delle verifiche svolte annualmente in funzione dell'analisi dei rischi.

1.3.3 AUTORIZZAZIONE ALL'ACCESSO IN RETE

L'autorizzazione all'accesso da parte di client posti sulla rete RUPAR o su INTERNET verso server dati gestiti presso CSI è regolata da una specifica procedura informatica ("Autorizzazione all'accesso IP") disponibile sul sito dell'Intranet aziendale.
Questa procedura riguarda in particolare l'attivazione delle possibilità di colloquio tra un IP client ed i server che ospitano le basi dati.
Si determina quindi un intervento di modifica effettuato sui sistemi firewall e sulle interfacce tcp-wrap presenti sui sistemi server.
La richiesta è validata dalla Sicurezza, cui compete il controllo di congruenza di quanto riportato, e va sottoscritta dal Responsabile di Progetto o di Assistenza Clienti che ne avrà ricevuto richiesta da parte del Cliente.
L'archiviazione e la gestione del tempo di queste richieste è di competenza della Sicurezza.

1.3.4 CARATTERISTICHE GENERALI DELLA SICUREZZA DELLA RETE RUPAR

Sono definite le seguenti misure di Sicurezza Logica a protezione di servizi e dati presenti sulla rete RUPAR:

- Adozione di soluzioni di servizio basate su un'architetture a 3 livelli con sistemi il cui livello di sicurizzazione venga controllato in modo costante.
- Ogni postazione che accede alla rete o eroga servizi sulla stessa non deve essere visibile dall'esterno della RUPAR.
- I servizi che accedono a risorse Internet utilizzano server proxy o gateway configurati secondo opportuni requisiti di sicurezza al fine di garantire, secondo quanto previsto dalle regole aziendali, funzionalità di controllo e limitazione sui servizi accessibili.
- Il servizio di posta elettronica è comprensivo delle funzionalità Antispamming, Antirelay, gestione delle Black List e dei filtri Antivirus sia in ricezione che in trasmissione.
- Inoltre al fine di attuare una separazione tra la rete locale del Cliente e le diverse interconnessioni della RUPAR, è opportuna presso il Cliente una soluzione di firewall a protezione del punto di interconnessione tra la rete del Cliente e la RUPAR in grado così di garantire un elevato grado di sicurezza, assicurando in ogni caso l'interoperabilità e l'interscambio applicativo, consentendo nel caso in cui occorra di consentire la visibilità INTERNET di server interni alla rete del Cliente (RUPAR).

1.3.5 GESTIONE DEI LOG

Le apparecchiature di controllo agli accessi (firewall e proxy) ed i dispositivi IPS (anti intrusione) producono file di log.

Il personale CSI (ed in particolare quello addetto alla gestione delle Reti) può visionare tali supporti solamente se indispensabile:

- per finalità statistiche e consuntive sull'uso delle macchine a fronte di necessità interne o richieste dei Clienti;
- per l'individuazione delle cause di problemi di funzionamento dei sistemi gestiti.

E' esclusa la possibilità di svolgere il trattamento di questi dati da parte di qualsiasi altra funzione aziendale del CSI.

Le attività appena elencate non consentono di risalire ai siti visitati dal personale (nel rispetto quindi della privacy dell'utente e di quanto stabilito dall'art. 4 dello Statuto dei Lavoratori).

L'iter sopra descritto sarà anche quello che il CSI porrà in essere su specifica richiesta del Cliente, qualora il Cliente stesso manifesti l'esigenza di prevenzione di possibili reati riferibili alle attività poste in rete dal proprio personale. In ogni caso, il ritorno che il CSI darà al Cliente sarà costituito da informazioni consuntive o statistiche, riservando

esclusivamente all'Autorità di Polizia Giudiziaria approfondimenti sulle attività svolte da specifiche persone[2] .

I log (del CSI e dei suoi Clienti) verranno conservati per un periodo coerente con le vigenti disposizioni di legge. La finalità della conservazione di questi dati, che possono contenere informazioni sensibili riconducibili a specifici utenti, è specificamente e unicamente finalizzata a supporto di eventuali verifiche disposte dalla magistratura.

1.3.6 UTILIZZO DEL SISTEMA DI POSTA AZIENDALE

Tutti i dipendenti CSI dispongono dell'accesso al Sistema di Posta aziendale.
Il Personale gestore del servizio di posta è autorizzato ad effettuare gli interventi individuati come opportuni per garantire il corretto funzionamento del servizio medesimo.
Questa autorizzazione è comprensiva in caso di necessità dell'accesso alle caselle di posta del personale dipendente, mentre in caso di intervento sulle caselle di posta dei Dirigenti dovrà essere richiesta l'autorizzazione da parte della Direzione Infrastrutture.

1.3.7 USO DEI MODEM

Le connessioni, con modem o linee dirette, tra i sistemi e la rete CSI Piemonte con reti e sistemi esterni possono presentare un serio rischio per CSI Piemonte. Come conseguenza di collegamenti non corretti dal punto di vista della sicurezza è possibile che si esponga l'intero sistema informativo CSI Piemonte ed i dati in esso contenuti, ciò può avvenire senza che il dipendente se ne renda conto.
Per tale motivo ogni collegamento dall'interno verso l'esterno e viceversa deve essere verificato dalla Gestione Reti ed essere reso noto a Sicurezza.
L'uso dei modem deve avvenire in alternativa e non contemporaneamente a quello della scheda di rete.
Di norma i modem collegati alle postazioni devono restare spenti se non utilizzati.

1.3.8 IP PUBBLICI

Premesso che:
- l'attribuzione di un indirizzo ufficiale non costituisce né privilegio né consente prestazioni migliori rispetto ad un indirizzo di classe privata (anzi le prestazioni relative alla navigazione in rete sono mediamente penalizzate del 60%).
- l'utilizzo dell'indirizzo ufficiale consente abusi non possibili con un indirizzo di classe privata: pertanto è da tenere sotto controllo

si definiscono le seguenti regole di attribuzione, gestione ed utilizzo degli IP ufficiali all'interno dei servizi gestiti da CSI Piemonte:

1) l'utilizzo dell'indirizzo ufficiale è riservato a quanto segue:
- svolgimento di specifiche attività di controllo della rete
- svolgimento di attività non possibili da indirizzo privato (non proxabili quindi)

[2] Evitando quindi l'attribuzione di profili sensibili o atti specifici a persone completamente identificate.

- sperimentazione di servizi
- necessità a termine (fiere e saloni)

2) l'assegnazione di un indirizzo IP ufficiale deve essere richiesta dal responsabile dell'assegnatario precisando quali funzionalità debbano essere consentite in rete

3) l'utilizzo dell'IP è limitato alle funzionalità autorizzate anche mediante specifiche policy definite sui sistemi Firewall
4) l'assegnatario dell'indirizzo pubblico risponde direttamente delle attività svolte sulla rete INTERNET
5) è proibita la modifica autonoma dell'IP ricevuto in assegnazione
6) l'assegnatario dell'indirizzo IP risponde direttamente e personalmente in sede penale e civile di qualsiasi azione svolta in contrasto con le vigenti leggi mediante l'IP avuto in uso e comunque di qualsiasi accesso in rete specie se acquisito proditoriamente (spoofing). Questa norma riguarda in special modo le eventuali violazioni alle leggi dello stato e a quelle internazionali (relative alla pirateria informatica, al copyright , alla privacy ed alla pedofilia) ed a qualsiasi azione contraria al corretto comportamento in rete.
7) l'utilizzo dell'indirizzo IP, dei vari collegamenti/servizi (es: posta elettronica) e più in generale della stessa postazione di lavoro, è riservata alle sole attività attinenti gli incarichi ricevuti all'interno dell'Azienda.

1.3.9 BACK-UP DEI DATI

Al fine di garantire nel tempo l'integrità e la disponibilità dei dati, vengono effettuati periodicamente i salvataggi degli stessi.
Per realizzare il processo di salvataggio dei dati e per monitorarne la corretta esecuzione è utilizzata un'applicazione software a questo dedicata (sw Legato).
Vengono quindi effettuate quotidianamente copie di salvataggio incrementali dei dati residenti sui sistemi server in gestione presso il CSI Piemonte; a queste si affiancano procedure settimanali e mensili di salvataggio degli interi archivi.
Nel caso in cui occorra ripristinare un singolo file o documento, il sistema recupera l'ultima versione salvata oppure consente di effettuare una scelta tra le versioni conservate.
La seguente tabella illustra la pianificazione dei backup.

Backup Totale	Ha una frequenza mensile, è effettuato durante il fine settimana.	E' conservato per 1 anno	Fa una copia completa del file system del server su supporti magnetici
Backup Settimanale	Ha una frequenza di tre cicli, è effettuato durante i fine settimana.	Viene conservato per 3 mesi	Il backup raccoglie tutte le variazioni prodotte, durante la settimana, rispetto al backup totale od al precedente backup settimanale. E' detto anche differenziale
Backup giornaliero	Ha una frequenza giornaliera, di norma serale, dal lunedì al venerdì	E' conservato per 3 settimane	Il backup raccoglie tutte le variazioni prodotte, durante una giornata, rispetto al backup totale od al precedente differenziale, nel giorno di lunedì, od al precedente giornaliero nei giorni diversi da lunedì. E' detto anche incrementale
Backup annuale	Ha una frequenza annuale	Viene conservato in conformità alle norme di legge e contrattuali	Il backup ha il fine di produrre una copia dei dati relativamente all'anno di riferimento

Più in generale, si individuano le seguenti linee guida:

- CSI Piemonte è responsabile delle procedure di salvataggio su nastro (o altro opportuno supporto) delle basi dati contenenti dati personali residenti sui sistemi server, con opportuna frequenza;
- Gli incaricati che trattano dati personali su archivi residenti in locale sulle proprie postazioni di lavoro sono responsabili del salvataggio periodico di tali archivi sulle risorse di rete o su supporti rimovibili (floppy, cd-rom, ecc.); tali supporti rimovibili andranno custoditi in sicurezza.

I salvataggi sono registrati su cassette.
Le cassette dei salvataggi sono trasportate in appositi locali di sicurezza, in sede diversa da quella che ospita la sala macchine CSI- Piemonte.
Le procedure usate per il salvataggio ed il ripristino dei dati sono ampiamente collaudate prima del rilascio in esercizio e sono svolte in modo conforme, oltre alle misure disposte dalla Legge, anche secondo i criteri della NORMA VISION 2000.

I tempi previsti di ripristino per gli archivi sono:

- se si tratta di dati non appartenenti ai salvataggi totali, e quindi immediatamente disponibili, il ripristino avviene nel tempo più breve possibile e comunque entro le 6 ore dalla richiesta; la celerità dipende dalle dimensioni dei dati da ripristinare e dall'ora della giornata in cui si effettua la richiesta;
- se per il ripristino occorre utilizzare cassette in sicurezza, al tempo suddetto occorre aggiungere il tempo del trasporto del nastro dalla sala di sicurezza al CSI Piemonte stimabili normalmente in 1 o 2 ore.

Prove di ripristino: prima di introdurre nuove procedure e/o nuove architetture di backup, si effettuano prove di salvataggio e ripristino, a garanzia dell'integrità e della disponibilità dei dati.

Per i servizi ospiti in housing o in hosting, il CSI-Piemonte non entra nel merito della consistenza dei dati ripristinati e della congruenza tra le basi dati dislocate sui diversi server, ma garantisce unicamente il buon esito delle operazioni eseguite in base alle specifiche fornite dal Cliente nella richiesta di ripristino.

Il CSI-Piemonte non entra inoltre nel merito (liceità, veridicità, attendibilità, violazione della normativa vigente in materia di diritto d'autore e di tutela dei marchi) dei dati, dei programmi software ed in generale delle informazioni che dovessero emergere nell'ambito dell'attività di salvataggio sopra descritta.
E' cura aggiuntiva in fase di progettazione dei servizi, identificare esigenze di archiviazione diverse da quanto esposto sopra. Per quanto di competenza, tali esigenze dovranno essere comunicate e concordate con i gruppi incaricati di tali trattamenti.

La continuità dell'operatività dei più importanti servizi pubblici erogati è garantita con l'utilizzo di apparecchiature di tipo fault-tolerance: inoltre tutti i dispositivi hardware sono coperti da contratti di manutenzione che prevedono opportuni tempi di intervento per le riparazioni.
Oltre ad essere in avanzata fase di allestimento il piano di Disaster recovery, resta comunque di garanzia a difesa dell'integrità dei dati gestiti, come già ricordato, l'esecuzione di puntuali copie di back-up di tutti i server e delle rispettive basi dati ospiti che vengono periodicamente trasferite presso la sede di C.so Tazzoli 215/13 in cui sono stati predisposti appositi locali per il mantenimento dei supporti utilizzati per i servizi di back-up. In questo modo un evento disastroso anche rilevante che interessasse la sede principale non comporterebbe la perdita dei dati relativi ai servizi della Pubblica Amministrazione ospiti di CSI Piemonte.

ALLEGATO 1: ELENCO DELLE PROCEDURE INFORMATICHE

É riportato di seguito l'elenco delle procedure informatiche erogate in favore dell' ASL 14:

- ADT14 - Accettazione, Dimissioni e Trasferimenti ASL14
- CUPW14 - Sistema Gestione Prestazioni Web ASL14
- FAID14 - First AID
- PAST14 - Pasteur per ASL14
- SCE14 - Scerev per ASL14
- SGP14 - Sistema Gestione Prestazioni ASL14

ALLEGATO A4
COMPOSTO DA 5 PAGG.

ALTEA

6 dicembre 2011

Documento Operativo

ASLVCO – Backup Policy

Preparato da: Altea S.p.A.
(Firma)

Altea S.p.A.
Strada Cavalli 42, 28831 Feriolo di Baveno (VB)
T +39 0323 280811 F +39 0323 2808110
www.alteanet.it - altea@alteanet.it

SOMMARIO

1 RELEASE DEL DOCUMENTO

- Release 1 aggiornata il 06/12/2011

2 INTRODUZIONE

Il presente documento illustra agli amministratori della rete ASLVCO e a tutte le persone interessate nel progetto, la gestione del backup, le modalità di restore, RTO e RPO.

3 SERVIZIO DI BACKUP

Il servizio di backup è configurato su Data protector 6.20 installato sul server SRVBCK su libreria nastro LTO Ultrium con 7 nastri LTO5. A seconda del processo vengono salvati sia i dati interni alle virtual machines che database SQL, Exchange e immagini delle singole macchine virtuali. Di seguito il dettaglio di tutti i job:

Nome processo	Descrizione	Server	Tipo	Schedulazione	RPO	RTO
vCenter	VM Snapshot	• cedweb • cedwsus • intranet • isaserver • mailproxy • nedi • nm • regport • srvLifeRay • srvMcAfee • srvSpartito • VCENTERASL • ZimbraMailServer • cedprog • cedrdp • Proxy	VM	9 p.m. incr lu-sa 9 p.m. full do	24 ore	24 ore

Il campo RPO (Recovery Point Objective) è uno dei parametri usati nell'ambito delle politiche di disaster recovery per descrivere la tolleranza ai guasti di un sistema informatico. Esso rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza (ad esempio attraverso backup) e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di guasto improvviso.

Il campo RTO è il tempo necessario per il pieno recupero dell'operatività di un sistema o di un processo organizzativo in un sistema di analisi. Il tempo impiegato per il recupero varia a seconda della mole di dati toccati.

4 RESTORE

La corretta procedura per il rispristino è quella di mandare un'email al servizio ETM support@alteanet.it specificando il server, i dati da restorare (se sql o files) e il timing del restore da considerare.

Il primo operatore disponibile si occuperà della presa in carico del ticket e la procedura di ripristino.

5 DISASTER RECOVERY

Il servizio di disaster recovery con replica remota verso il cluster di Verbania (MGMT_Verbania) è operativo con una scadenza oraria (1h) per i seguenti volumi:

Name	Data Protection Level	Compression	Consumed Space
Remote_Cedbkp	Network RAID-0 (None)	Full	758,24 GB
Remote_Cedweb	Network RAID-0 (None)	Full	35,17 GB
Remote_Cupweb	Network RAID-0 (None)	Full	1,51 GB
Remote_intranet	Network RAID-0 (None)	Full	10,85 GB
Remote_MailProxy	Network RAID-0 (None)	Full	9,49 GB
Remote_proxy	Network RAID-0 (None)	Full	21,91 GB
Remote_Vcenterasl	Network RAID-0 (None)	Full	30,92 GB
Remote_Zimbra	Network RAID-0 (None)	Full	50,31 GB
test	Network RAID-0 (None)	Full	4,87 GB

ALLEGATO A5
COMPOSTO DA 15 PAGG.

ALTEA

6 dicembre 2011

Documento Operativo

ASLVCO – Virtualizzazione e Disaster Recovery

Preparato da Altea S.p.A.
(Firma)

Altea S.p.A.
Strada Cavalli 42, 28831 Feriolo di Baveno (VB)
T +39 0323 280811 F +39 0323 2808110
www.alteanet.it - altea@alteanet.it

SOMMARIO

1 PERIMETRO

Il presente documento contiene le specifiche tecniche relative al progetto di installazione infrastruttura hardware e software in supporto all'implementazione come da offerta Off11_0321_Rev01.

L'implementazione riguarda:

- Installazione componenti server, storage e backup
- Configurazione server
- Installazione e configurazione Sistemi operativi Server
- Installazione configurazione VMware VSphere
- Virtualizzazione sistemi di produzione attuali
- Installazione e configurazione Data Protector

Il dimensionamento dell'infrastruttura è fatto per poter supportare la virtualizzazione dei sistemi attualmente in produzione.

2 ARCHITETTURA

L'architettura prevede una farm VMWare vSphere con due nodi nella sede di Omegna che condividono due storage condivisi P4500 connessi in iSCSI ed un nodo ESXi nella sede di Verbania con uno storage P4500 connesso in iSCSI con le repliche remote dei volumi da utilizzare in caso di disaster recovery.

Le macchine virtuali sono gestite da vCenter con le funzionalità di HA (High Availability), in modo da consentire la ripartenza automatica delle VM in caso di guasto hardware.

La manutenzione hardware dei server può essere gestita con le funzionalità di vMotion per lo spostamento a caldo delle VM da un nodo all'altro senza interruzione di servizio.

2.1 Architettura server

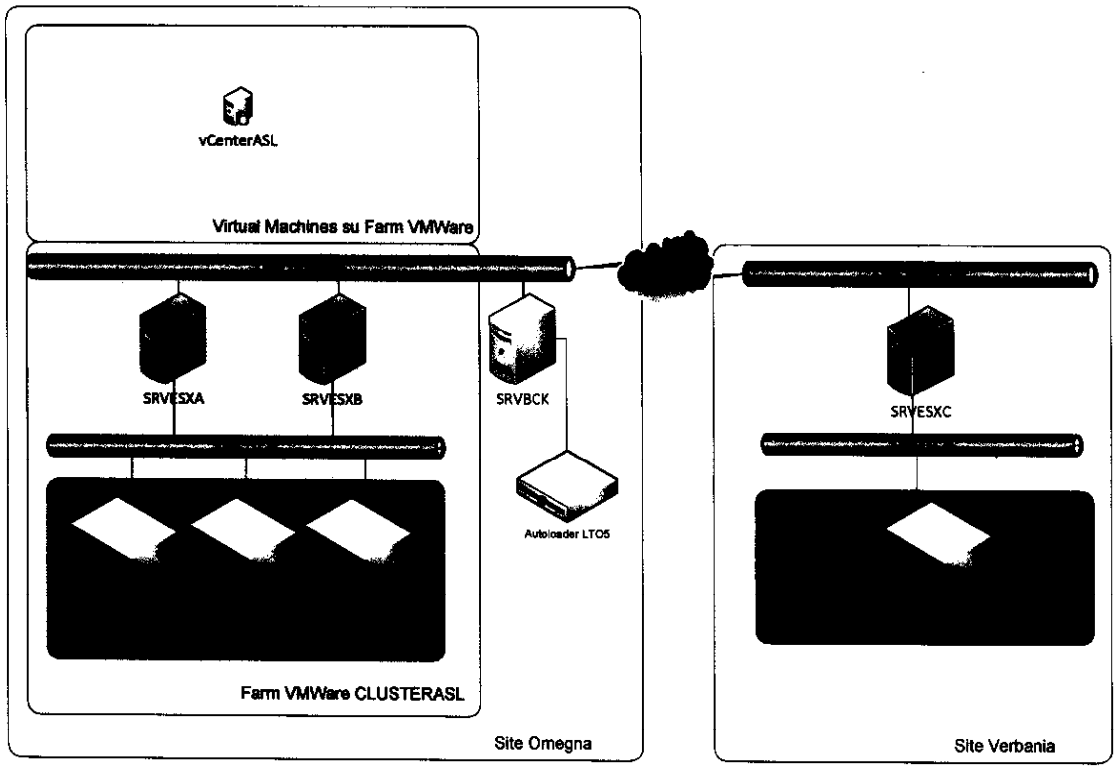
L'infrastruttura esistente prevedeva sia macchine fisiche che virtuali distribuite su soluzioni server e storage diversificate.

Le macchine fisiche sono virtualizzate AS-IS sulla farm VMware mentre quelle già virtuali sono migrate tramite le utility di VMware.

Il backup è gestito da un server dedicato con DataProtector e un autoloader LTO5.

Il disaster recovery viene gestito tramite snapshot remoti verso la sede di Verbania utilizzando le funzionalità del P4500 Lefthand.

Il disegno complessivo dell'architettura è riportato di seguito.



2.2 Architettura network

Il progetto non ha avuto impatti sulla struttura di rete esistente, attualmente i server sono connessi ad un unico switch.

Per garantire la ridondanza e bilanciare i carichi si consiglia di installare uno switch aggiuntivo con connessioni in etherchannel verso il core.

3 COMPONENTI

I componenti installati sono quelli indicati nei DDT di consegna allegati.

L'informazione aggiornata sulla configurazione è riportata sul CMDB di Altea, accessibile all'indirizzo http://nm.alteanet.it/glpi

Le attività di installazione sono documentate nelle Change e nei Ticket di OTRS (http://support.alteanet.it) allegate in PDF al presente documento.

3.1 Network

Di seguito l'export di GLPI con l'elenco degli apparati e il loro indirizzamento

VIPSTORE	-> ASLVCO	172.16.24.100		SAN	P4500 Virtual IP		2011-12-05 15:53

3.2 Server

Di seguito lo screenshot di GLPI con l'elenco dei server installati e le loro caratteristiche

NAS1	172.16.1.81	HP	CZ112182AU	Rack Mount Chassis	ProLiant DL320 G6	Microsoft Windows Storage Server 2008 R2 Standard	administrator			System System Reserved	61 332 99	62.00% 72.00%		2011-10-04 17:36
SRVBCK	172.16.12.24		CZJ1358888			CentOS release 5.7 (Final)		domain admin	Data Protector					2011-12-05 15:23
SRVESXA	172.16.12.21 172.16.24.21 172.16.24.121 172.16.12.11	HP	CZ3136T4B4		DL380 G7	VMware ESXi		root						2011-12-06 15:23
SRVESXB	172.16.12.22 172.16.24.22 172.16.24.122 172.16.12.12	HP	CZ3136T4B0		DL380 G7	VMware ESXi		root						2011-12-06 15:21
SRVESXC	172.16.12.23 172.16.24.23 172.16.24.123 172.16.12.13	HP	CZ3136T4B2		DL380 G7	VMware ESXi		root						2011-12-06 15:22
SRVSTORE1	172.16.24.14	HP	CZJ1288JT1		P4500 Lefthand			admin						2011-12-05 15:32
SRVSTORE2	172.16.24.15	HP	CZJ1278033		P4500 Lefthand			admin						2011-12-05 15:30
SRVSTORE3	172.16.24.16 172.16.12.16	HP	CZJ127063F		P4500 Lefthand			admin						2011-12-05 15:30
SRVSTORE4	172.16.24.17 172.16.12.17	HP	CZJ1286J9T		P4500 Lefthand			admin						2011-12-06 15:31
VCENTERASL	172.16.12.25			Virtual Machine		Microsoft Windows Server 2008 R2 Standard		domain admin	CMC vCenter					2011-12-05 15:32

3.3 Storage

Di seguito lo screenshot dell'interfaccia di gestione del P4500 con la configurazione delle LUN e l'occupazione attuale:

Name	Data Protection Level	Provisioning	Consumed Space
srvLifeRay	Network RAID-10 (2-Way Mirror)	Full, 114,88 GB Reclaimable	140,00 GB
srvMcAfee	Network RAID-10 (2-Way Mirror)	Full, 115,76 GB Reclaimable	140,00 GB
srvSpartito	Network RAID-10 (2-Way Mirror)	Full, 129,13 GB Reclaimable	140,00 GB
Template	Network RAID-10 (2-Way Mirror)	Thin, 399 GB Saved	10,98 GB
VCENTERASL	Network RAID-10 (2-Way Mirror)	Full, 147,4 GB Reclaimable	205,35 GB
vol_cedbkp	Network RAID-10 (2-Way Mirror)	Thin, 1,47 TB Saved	1,44 TB
vol_cedprog	Network RAID-10 (2-Way Mirror)	Thin, 14,96 GB Saved	385,03 GB
vol_cedweb	Network RAID-10 (2-Way Mirror)	Thin, 499 GB Saved	69,05 GB
vol_cedwsus	Network RAID-10 (2-Way Mirror)	Thin, 227,26 GB Saved	192,73 GB
vol_CupWeb	Network RAID-10 (2-Way Mirror)	Thin, 129 GB Saved	4,06 GB
vol_intranet	Network RAID-10 (2-Way Mirror)	Thin, 79 GB Saved	21,19 GB
vol_jeeserver	Network RAID-10 (2-Way Mirror)	Thin, 62,67 GB Saved	237,33 GB
vol_MailProxy	Network RAID-10 (2-Way Mirror)	Full, 79 GB Reclaimable	97,69 GB
vol_nm_nedi	Network RAID-10 (2-Way Mirror)	Thin, 139,06 GB Saved	60,93 GB
vol_proxy	Network RAID-10 (2-Way Mirror)	Thin, 59 GB Saved	6,66 GB
vol_regport	Network RAID-10 (2-Way Mirror)	Thin, 859 GB Saved	1,00 GB
vol_Temp	Network RAID-10 (2-Way Mirror)	Full, 681,65 GB Reclaimable	2,00 TB
vol_WinXpOracle	Network RAID-10 (2-Way Mirror)	Thin, 129 GB Saved	1,00 GB
vol_Zimbra	Network RAID-10 (2-Way Mirror)	Thin, 2 TB Saved	4,06 GB

Di seguito lo screenshot della configurazione degli storage della farm vSphere:

Identification	Status	Device	Capacity	Free	Type	Last Update	Alarm Actions	Storage I/O Control
ISO	Normal	nas1.asl14:/ISO	1,38 TB	620,51 GB	NFS	06/12/2011 13:11:11	Enabled	Not supported
SRVESXA	Normal	naa.600508b100...	274,25 GB	267,16 GB	vmfs3	06/12/2011 13:11:11	Enabled	Disabled
SRVESXB	Normal	naa.600508b100...	274,25 GB	269,75 GB	vmfs3	06/12/2011 13:11:15	Enabled	Disabled
SRVESXC	Normal	naa.600508b100...	274,25 GB	273,70 GB	vmfs3	06/12/2011 13:13:14	Enabled	Disabled
srvLifeRay	Normal	naa.6000eb3a26...	69,75 GB	52,91 GB	vmfs3	06/12/2011 13:13:14	Enabled	Disabled
srvMcAfee	Normal	naa.6000eb3a26...	69,75 GB	51,45 GB	vmfs3	06/12/2011 13:13:14	Enabled	Disabled
srvSpartito	Normal	naa.6000eb3a26...	69,75 GB	64,25 GB	vmfs3	06/12/2011 13:13:14	Enabled	Disabled
Template	Normal	naa.6000eb3a26...	199,75 GB	195,57 GB	vmfs3	06/12/2011 13:13:14	Enabled	Disabled
VCENTERASL	Normal	naa.6000eb3a26...	74,75 GB	26,30 GB	vmfs3	06/12/2011 13:13:14	Enabled	Disabled
vol_cedbkp	Normal	naa.6000eb3a26...	754,75 GB	707,77 GB	vmfs3	06/12/2011 13:13:14	Enabled	Disabled
vol_cedprog	Alert	naa.6000eb3a26...	199,75 GB	67,00 GB	vmfs3	06/12/2011 13:13:14	Enabled	Disabled
vol_cedweb	Normal	naa.6000eb3a26...	249,75 GB	214,95 GB	vmfs3	06/12/2011 13:13:14	Enabled	Disabled
vol_cedwsus	Alert	naa.6000eb3a26...	209,75 GB	5,71 GB	vmfs3	06/12/2011 13:13:14	Enabled	Disabled
vol_cupweb	Normal	naa.6000eb3a26...	64,75 GB	64,38 GB	vmfs3	06/12/2011 13:13:14	Enabled	Disabled
vol_intranet	Normal	naa.6000eb3a26...	19,75 GB	8,54 GB	vmfs3	06/12/2011 13:13:14	Enabled	Disabled
vol_jsaserver	Warning	naa.6000eb3a26...	149,75 GB	28,38 GB	vmfs3	06/12/2011 13:13:14	Enabled	Disabled
vol_mailproxy	Normal	naa.6000eb3a26...	39,75 GB	27,62 GB	vmfs3	06/12/2011 13:13:14	Enabled	Disabled
vol_nm_nedi	Normal	naa.6000eb3a26...	99,75 GB	61,14 GB	vmfs3	06/12/2011 13:13:14	Enabled	Disabled
vol_proxy	Normal	naa.6000eb3a26...	29,75 GB	7,32 GB	vmfs3	06/12/2011 13:13:14	Enabled	Disabled
vol_regport	Normal	naa.6000eb3a26...	319,75 GB	12,08 GB	vmfs3	06/12/2011 13:13:14	Enabled	Disabled
vol_Temp	Normal	naa.6000eb3a26...	1.023,75 G	262,02 GB	vmfs3	06/12/2011 13:13:14	Enabled	Disabled
vol_winXPoracle	Normal	naa.6000eb3a26...	64,75 GB	64,20 GB	vmfs3	06/12/2011 13:13:14	Enabled	Disabled
vol_zimbra	Normal	naa.6000eb3a26...	1.023,75 G	966,23 GB	vmfs3	06/12/2011 13:13:14	Enabled	Disabled

3.4 Servizi

Di seguito l'export di GLPI dei servizi censiti, con relative dipendenze su Server

CMC	Computer - VCENTERASL			2011-12-05 15:57
Data Protector	Computer - SRVBCK			2011-12-05 15:57
GLPI		GLPI 0.80, FusionInventory 2.3.4 su domini ASL14 e FUJI	2011-06-06	2011-06-06 11:30
OTRS		OTRS 3.0.8	2011-06-06	2011-06-06 11:56
vCenter	Computer - VCENTERASL			2011-12-05 15:57

3.5 Account

Di seguito l'export di GLPI degli account censiti, con relativi ambiti. Ove possibile sono differenziati gli accessi di Altea e del Cliente con utenze separate. Le credenziali del Cliente sono state fornite brevi manu e non sono riportate in questo documento per motivi di sicurezza.

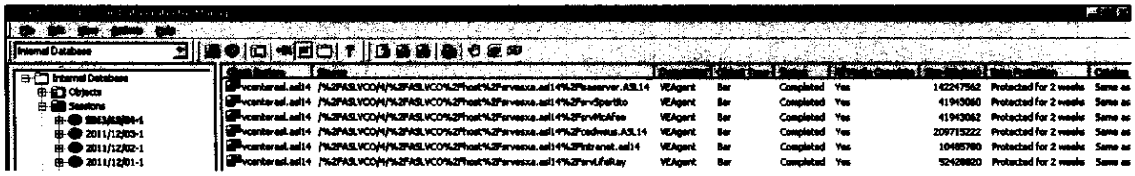
admin	- > ASLVCO	admin	Computer - SRVSTORE1 Computer - SRVSTORE2 Computer - SRVSTORE3 Computer - SRVSTORE4	Nessuna scadenza	2011-12-05 16:19	Altea-ETM
domain admin	- > ASLVCO	adminaltea	Computer - SRVBCK Computer - VCENTERASL	Nessuna scadenza	2011-12-05 16:00	Altea-ETM
root	- > ASLVCO	root	Computer - SRVESXA Computer - SRVESXB Computer - SRVESXC	Nessuna scadenza	2011-12-05 15:57	Altea-ETM

4 BACKUP E RECOVERY

Il dettaglio delle modalità di backup è indicato nel documento "ASL VCO - Backup policy", di seguito i risultati dei test di backup e restore effettuati sulla configurazione.

4.1 Verifica backup

I backup sono configurati e funzionanti, come da log che segue:



4.2 Verifica restore

Il funzionamento del restore è stato verificato, come da log che segue:

```
[Normal] From: RSM@srvbck.asl14 ""  Time: 05/12/2011 15:09:12
        Restore session 2011/12/05-3 started.

[2011-12-05 15:11:01.783 23344 info 'DiskLibPlugin'] Current working directory:
C:\Windows\system32
[2011-12-05 15:11:01.783 23344 verbose 'ThreadPool'] TaskMax=10, IoMin=1, IoMax=21
[Normal] From: OB2BAR_VEAgent@vcenterasl.asl14 "/ASLVCO"  Time: 05/12/2011 15:11:09
        Creating folder C:\ProgramData\OmniBack\tmp\03a61fd7-c3d6-4462-9772-89e44b4e3cb0\
...

[Normal] From: OB2BAR_VEAgent@vcenterasl.asl14 "/ASLVCO"  Time: 05/12/2011 15:11:12
        Virtual Machine 'Proxy': Power off ...

[Normal] From: OB2BAR_VEAgent@vcenterasl.asl14 "/ASLVCO"  Time: 05/12/2011 15:11:14
        Virtual Machine 'Proxy': deleting disk scsi0:0...

[Normal] From: OB2BAR_VEAgent@vcenterasl.asl14 "/ASLVCO"  Time: 05/12/2011 15:11:17
        Virtual Machine 'Proxy': Restoring session 2011/12/05-2 ...

[Normal] From: RMA@srvbck.asl14 "HP:Ultrium 5-SCSI_1_srvbck"  Time: 05/12/2011 15:10:02
        STARTING Media Agent "HP:Ultrium 5-SCSI_1_srvbck"

[Normal] From: RMA@srvbck.asl14 "HP:Ultrium 5-SCSI_1_srvbck"  Time: 05/12/2011 15:10:02
        By: UMA@srvbck.asl14@/dev/sg2
        Loading medium from slot 2 to device /dev/nst0

[Normal] From: OB2BAR_VEAgent@vcenterasl.asl14 "/ASLVCO"  Time: 05/12/2011 15:13:27
        Starting OB2BAR Restore:
vcenterasl.asl14:/%2FASLVCO/4/%2FASLVCO%2Fhost%2Fsrvesxb.asl14%2FProxy "VEAgent"

[Normal] From: OB2BAR_VEAgent@vcenterasl.asl14 "/ASLVCO"  Time: 05/12/2011 15:13:34
        Virtual Machine 'Proxy': Creating snapshot ...

[2011-12-05 15:13:38.449 22288 trivia 'ThreadPool'] PrepareToWait: Starting new thread
[2011-12-05 15:13:38.536 21328 trivia 'ThreadPool'] PrepareToWait: Starting new thread
[Normal] From: OB2BAR_VEAgent@vcenterasl.asl14 "/ASLVCO"  Time: 05/12/2011 15:13:50
        Virtual Machine 'Proxy': Restoring disk scsi0:0 using transport method NBD ...

Deleted directory C:\Windows\TEMP\vmware-SYSTEM\422ab619-ebdd-d8dd-d6cf-69a2740b4673-vm-
289\nbd
[Normal] From: OB2BAR_VEAgent@vcenterasl.asl14 "/ASLVCO"  Time: 05/12/2011 15:28:12
        Completed OB2BAR Restore:
vcenterasl.asl14:/%2FASLVCO/4/%2FASLVCO%2Fhost%2Fsrvesxb.asl14%2FProxy "VEAgent"

[Normal] From: OB2BAR_VEAgent@vcenterasl.asl14 "/ASLVCO"  Time: 05/12/2011 15:28:13
        Virtual Machine 'Proxy': Register vm ...
```

```
[Normal] From: RSM@srvbck.asl14 ""  Time: 05/12/2011 15:26:30
       OB2BAR application on "vcenterasl.asl14" disconnected.

[Normal] From: RMA@srvbck.asl14 "HP:Ultrium 5-SCSI_1_srvbck"  Time: 05/12/2011 15:27:46
       By: UMA@srvbck.asl14@/dev/sg2
       Unloading medium to slot 2 from device /dev/nst0

[Normal] From: RMA@srvbck.asl14 "HP:Ultrium 5-SCSI_1_srvbck"  Time: 05/12/2011 15:28:10
       COMPLETED Media Agent "HP:Ultrium 5-SCSI_1_srvbck"


================================================================================
                      Session completed successfully!
================================================================================
```

4.3 Verifica disaster recovery

Il funzionamento della funzionalità di disaster recovery è stata verificata ed è riportata integralmente nella sezione procedure.

5 PROCEDURE

5.1 Accensione

1. Switch
2. SAN P4500 (SRVSTORE1, SRVSTORE2)
3. Autoloader LTO
4. Server SRVBCK
5. Server farm VMWare (SRVESXA, SRVESXB)
6. Virtual Machine – l'accensione automatica è gestita da vSphere per le seguenti VM:
    a. VCENTERASL

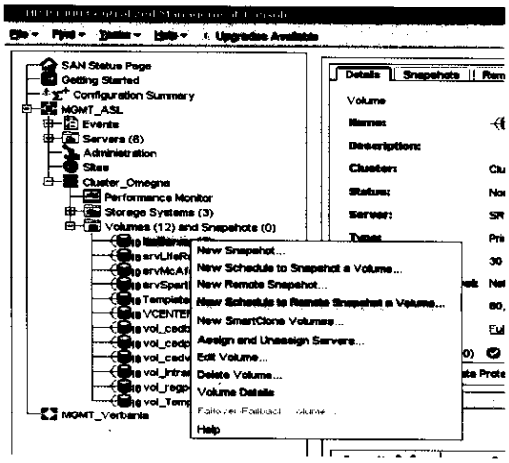
5.2 Spegnimento

1. Virtual Machine (Per ultima la macchina VCENTERASL)
2. Server farm VMWare (SRVESXA, SRVESXB)
3. SAN P4500 (SRVSTORE1, SRVSTORE2) – Utilizzare una macchina esterna con la console CMC
4. Server SRVBCK
5. Autoloader LTO
6. Switch

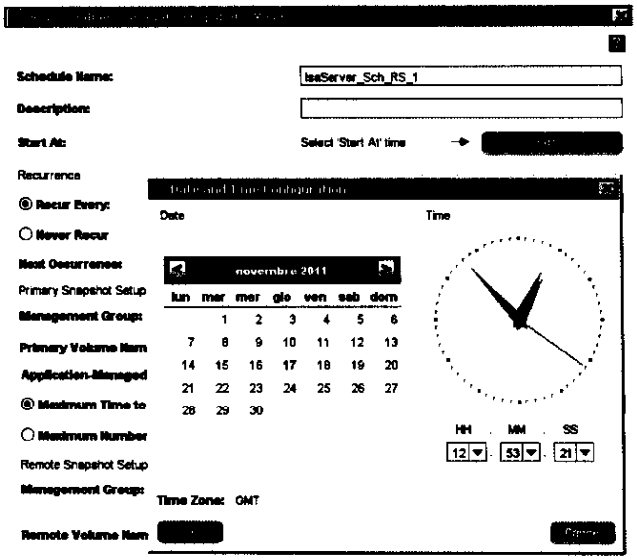
5.3 Creazione snapshot remoti

Per attivare la funzionalità di creazione snapshot remoto verso l'infrastruttura storage di Verbania è necessario eseguire le seguenti operazioni:

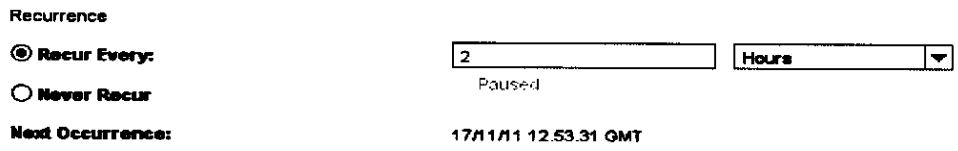
1) Selezionare il volume locale desiderato e creare un nuovo snapshot remoto



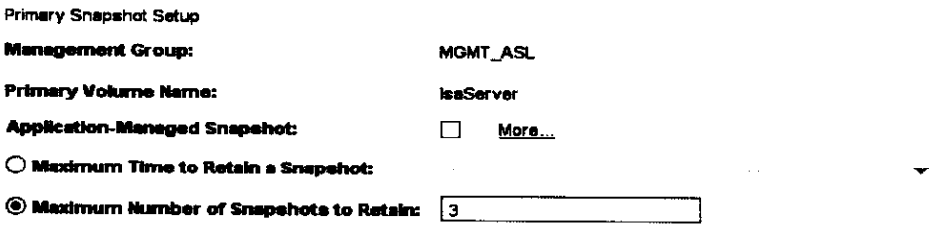
2) Selezionare la data e ora di partenza della schedulazione



3) Selezionare la ricorrenza della schedulazione. Per una soluzione di disaster recovery la ricorrenza deve essere inferiore alle 2 ore.

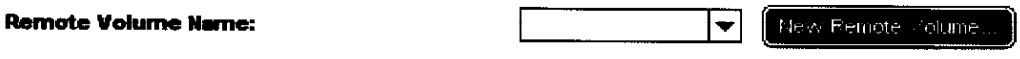


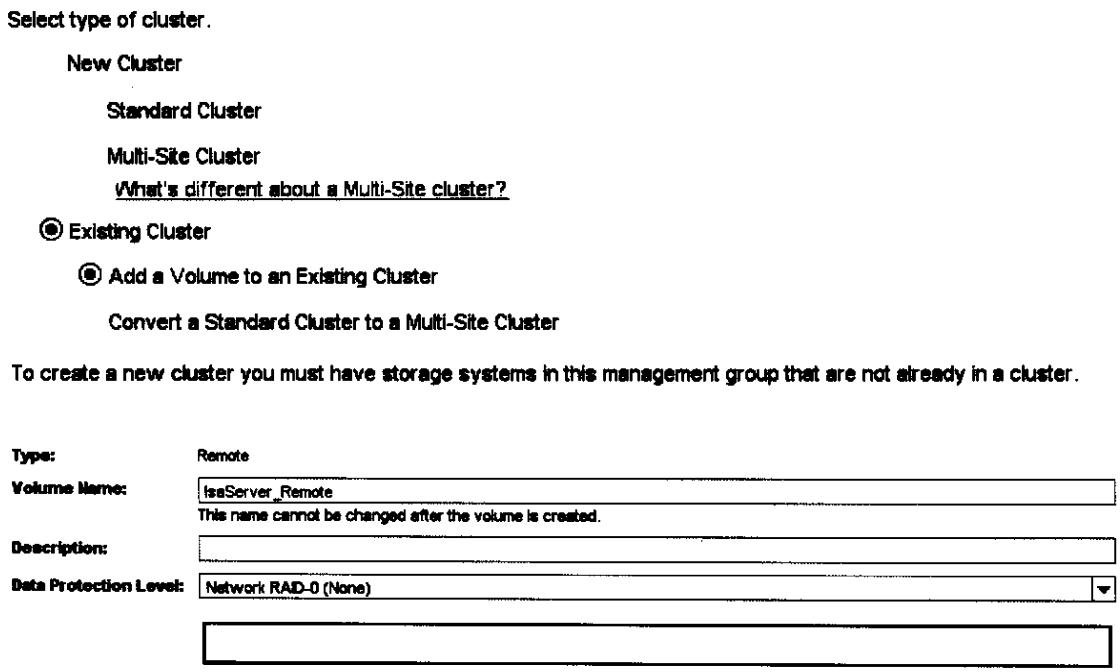
4) Selezionare il massimo numero di snapshot da mantenere. Consigliato per la soluzione di disaster recovery è 3.



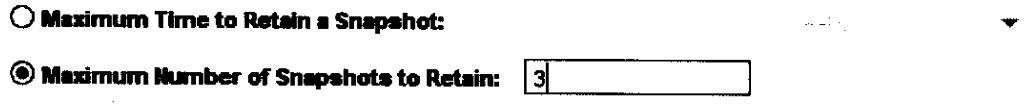
5) Selezionare il management group verso il quale effettuare lo snapshot

6) Creare un nuovo volume remoto





7) Impostare il numero massimo di snapshot remoti da mantere

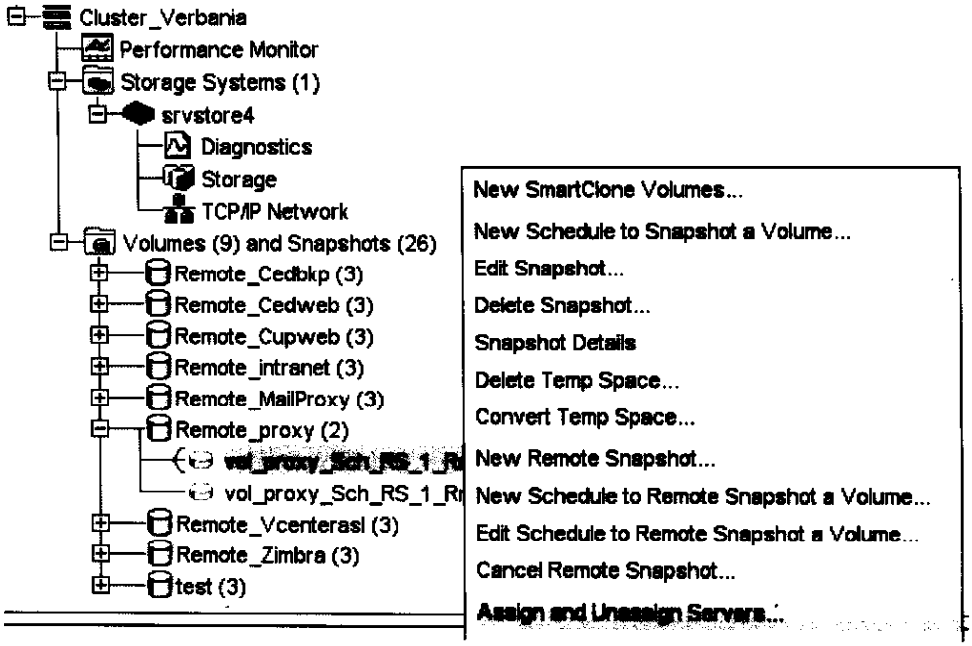


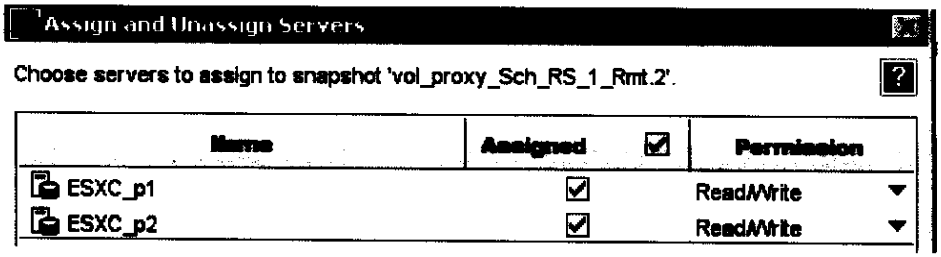
5.4 Disaster Recovery

In caso di ripristino da disaster recovery sono necessari i seguenti componenti:

- Accesso allo storage remoto P4500 della sede di Verbania
- Accesso ad una nodo ESXi con visibilità tramite iSCSI allo storage

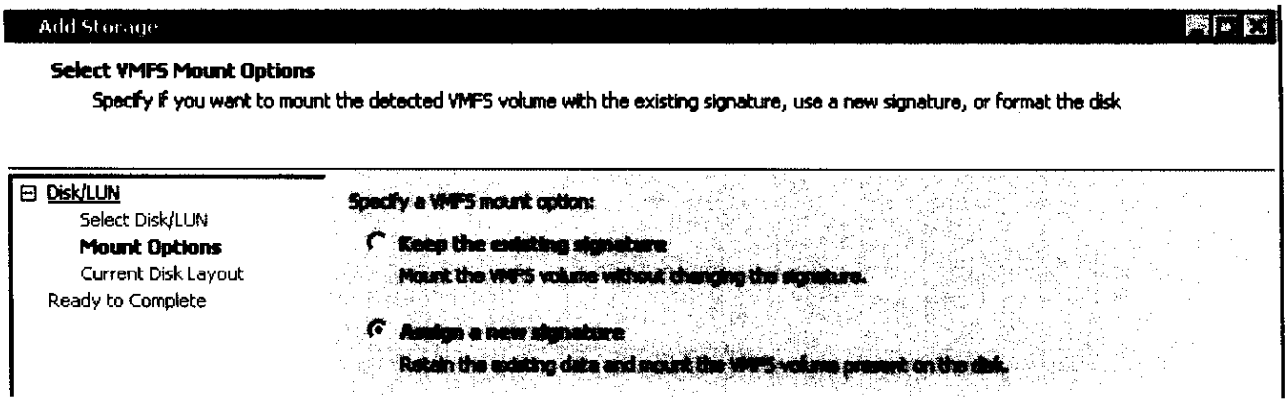
1) Selezionare l'ultimo snapshot del volume da ripristinare ed assegnarlo al server



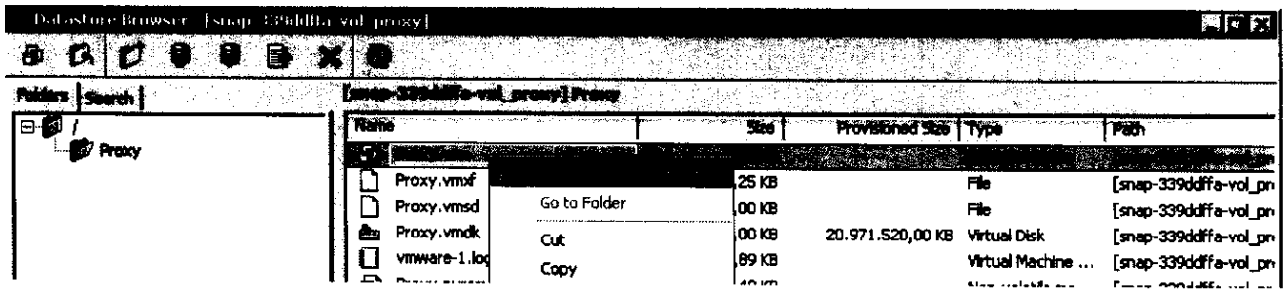


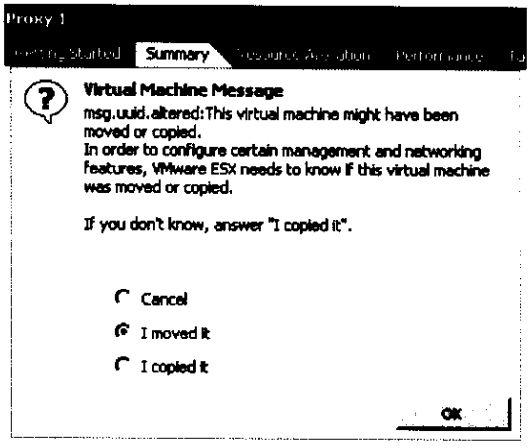
2) Effettuare un **Rescan all** dal nodo ESXi e aggiungere un dispositivo di storage tramite **Add Storage**. Selezionare il volume desiderato, a differenza dei volumi standard possiede già una Label VMFS:

Name	Path ID	LUN	Capacity	VMFS Label
LEFTHAND iSCSI Disk (naa.6000eb3...	iqn.2003-10.com.lefthandnetworks:mgmt-asl:944:vol-nm-nedl	0	100,00 GB	
LEFTHAND iSCSI Disk (naa.6000eb3...	iqn.2003-10.com.lefthandnetworks:mgmt-asl:946:vol-mailproxy	0	40,00 GB	
LEFTHAND iSCSI Disk (naa.6000eb3...	iqn.2003-10.com.lefthandnetworks:mgmt-asl:948:vol-zimbra	0	1,00 TB	
LEFTHAND iSCSI Disk (naa.6000eb3...	iqn.2003-10.com.lefthandnetworks:mgmt-asl:952:vol-cupweb	0	65,00 GB	
LEFTHAND iSCSI Disk (naa.6000eb3...	iqn.2003-10.com.lefthandnetworks:mgmt-asl:954:vol-winxporacle	0	65,00 GB	
LEFTHAND iSCSI Disk (naa.6000eb3...	iqn.2003-10.com.lefthandnetworks:mgmt-verbania:6826:vol-proxy-sch-rs-1-rmt.3	0	30,00 GB	vol_proxy (...

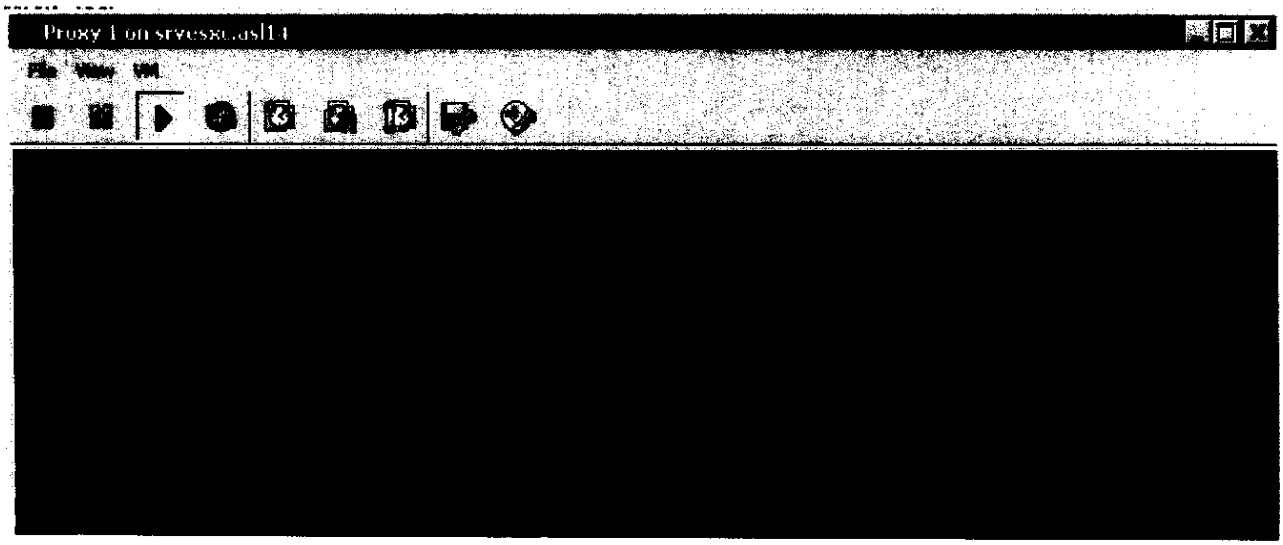


3) Aggiungere la macchina all'inventory tramite il browse del nuovo datastore e selezionare l'opzione **I moved it** dopo l'avvio della stessa.





4) A seconda della macchina, potrebbe essere necessario ripristinare la connettività di rete



6 VERBALE DI ACCETTAZIONE

L'infrastruttura descritta in questo documento è rilasciata al Cliente, che la prende in gestione in data 06/12/2011 concludendo e accettando integralmente la fornitura e le attività dell'offerta: Off11_0321_Rev01.

Ogni attività successiva sarà oggetto di contratto separato.

ALLEGATO A-6
COMPOSTO DA 3 PAGG.

ASL

FMEA

Omegna, 13 marzo 2012

ID	Item	Funzione/ Processo	Modo di guasto	Effetto del guasto (locale e sul sistema)	Note	Gravità	Causa potenziale del guasto	Probabilità	Azione preventiva: difese, protezioni.	Azione per rendere il guasto rilevabile	Rilevabilità	RPN	Azione raccomandata	Tipo di azione	Responsabile e scadenza	Azione intrapresa / mitigazione	Gravità	Probabilità	Rilevabilità	RPN
1	Armadio di distribuzione	Collegamento rete CCE	Mancanza di corrente elettrica	La CCE è indisponibile nella zona dell'armadio di distribuzione		4	Guasto elettrico	7	Collegamento degli armadi alla rete elettrica privilegiata. E'stato attivato per ogni armadio di piano un collegamento di rete dati ad anello con gli apparati di distribuzione centrale di sede. Gli operatori dovranno gestire le attività sanitarie utilizzando documenti cartacei (CC, STU, richieste etc) come da direttive aziendali		1	28	Collegare l'armadio alla rete elettrica privilegiata		Servizio di manutenzione, elettricisti di sede	Verifica del tipo di alimentazione elettrica per eventuale spostamento dell'attacco sotto alimentazione privilegiata	4	7	1	28
2	Switch di piano	Collegamento rete CCE	Guasto switch di piano	La CCE è indisponibile ai PC collegati direttamente allo switch	La rete può risultare indisponibile sia per un guasto alllie apparecchiature, sia per mancanza di corrente elettrica nell'armadio di distribuzione	4	Guasto elettrico, mancanza di corrente	4	Controllo periodico apparecchiature. Idem come sopra	Controllo degli switch remoti con allarmi	2	32	Verifica presenza di corrente elettrica. Disponibilità di switch di riserva. Installazione di un allarme che segnali la presenza di un guasto		Servizio Tecnicomanutenzione, in caso di mancanza di corrente. Immediata. CED. Immediata (Se l'apparato di riserva è a disposizione, il tempo necessario per configurare il nuovo apparato, recarsi nella sede dove si è verificato il guasto e sostituirlo)	Attivazione procedura privilegiata di acquisto urgente	4	4	2	32
3	Switch di distribuzione centrale in Ospedale	Collegamento rete CCE	Guasto switch di distribuzione centrale in Ospedale	La CCE è indisponibile in tutto l'Ospedale	La rete può risultare indisponibile sia per un guasto allo switch, sia per mancanza di corrente elettrica nell'armadio di distribuzione	5	Guasto elettrico	4	Lo switch è ridondato. Controllo periodico degli apparati. Idem come sopra	Contro degli switch remoto con allarmi	2	40	Verifica di presenza di corrente elettrica. Disponibilità di switch di riserva. Installazione di un allarme in caso di guasto		Servizio Tecnicomanutenzione, in caso di mancanza di corrente. Immediata. CED. Immediata (Se l'apparato di riserva è a disposizione, il tempo necessario per configurare il nuovo apparato, recarsi nella sede dove si è verificato il guasto e sostituirlo)	Attivazione procedura privilegiata di acquisto urgente	5	4	2	40

4	Switch di distribuzione centrale al CED	Collegamento rete CCE	Guasto switch di distribuzione centrale al CED	La CCE è indisponibile	La rete può risultare indisponibile sia per un guasto allo switch, sia per mancanza di corrente elettrica nell'armadio di distribuzione	6	Guasto elettrico	4	Lo switch è ridondato. Controllo periodico degli apparati. Idem come sopra	Controllo degli switch da remoto con allarmi	2	48	Verifica di presenza di corrente elettrica. Disponibilità di switch di riserva. Installazione di un allarme in caso di guasto		Servizio Tecnicomanutenzione, in caso di mancanza di corrente. Immediata. CED. Immediata (Se l'apparato di riserva è a disposizione, il tempo necessario per configurare il nuovo apparato e sostituirlo)	Attivazione procedura privilegiata di acquisto urgente	6	4	2	48
5	Collegamento di rete tra le sedi	Collegamento rete CCE	Interruzione delle linee	La CCE è indisponibile solo nel momento di passaggio dal collegamento principale a quello di backup.	Si tratta di un guasto "esterno"	6	Interruzione fisica di una linea o guasto in una centrale di distribuzione esterna (TELECOM)	4	I collegamenti in fibra ottica sono backuppati mediante collegamenti MPLS che, in caso di guasto, entrano in funzione automaticamente in pochi secondi	L'entrata in funzione del collegamento MPLS provoca evidenti rallentamenti nell'utilizzo della CCE	2	48	In caso di rallenamenti su tutte le PDL avvertire immediatamente il CED		TELECOM. Il ripristino della situazione ottimale dipende dal tipo di guasto (si è rotta un'apparecchiatura, è stata tranciata una fibra ottica ...)	E' attivo un collegamento di emergenza, a velocità inferiore, che entra in funzione automaticamente in caso di guasto	6	4	2	48
6	PC locale	Utilizzo della CCE	Il PC non funziona	La CCE è indisponibile sul singolo PC	Il PC può non funzionare per un problema hardware o software	1	Guasto elettrico, malfunzionamento del PC dovuto a un VIRUS o utilizzo del PC con modalità diverse da quelle previste dalla normative interne	7	Nel reparto ci sono più postazioni di lavoro collegate alla CCE, utilizzare un'altra postazione.	Il guasto è rilevabile direttamente dal personale	1	7	Utilizzare il PC secondo le modalità previste nel documento programmatico di sicurezza		CED (in caso di ripristino del software), Ditta preposta alla manutenzione (in caso di guasto riparabile), Ufficio acquisti (in caso di guasto non riparabile)	L'accesso alla CCE avviene tramite l'autenticazione dell'utente a cui sono attribuite le funzionalità specifiche. In caso di guasto di un PC possono essere utilizzati gli altri PDL del Reparto o quelli di altri reparti vicini.	1	7	1	7
7	PC locale	Utilizzo della CCE	Il PC funziona, ma non si collega alla rete dati	La CCE è indisponibile sul singolo PC		1	Guasto sugli apparati di distribuzione dell'area, sulla scheda di rete del PC, cavo di rete scollegato	7	Nel reparto ci sono più postazioni di lavoro collegate alla CCE. Utilizzare un'altra postazione.	Il guasto è rilevabile direttamente dal personale	1	7	Verificare che il cavo di rete sia correttamente collegato		CED, Ditta preposta alla manutenzione (in caso di guasto riparabile), Ufficio acquisti (in caso di guasto non riparabile)	L'accesso alla CCE avviene tramite l'autenticazione dell'utente a cui sono attribuite le funzionalità specifiche. In caso di guasto di un PC possono essere utilizzati gli altri PDL del Reparto o quelli di altri reparti vicini.	1	7	1	7
8	Stampante locale	Stampa dei documenti della CCE	La stampante non funziona	La stampa dei documenti della CCE è indisponibile sul singolo PDL		1	Guasto, cavo di collegamento staccato o mancanza di materiali di consumo (toner ecc.)	7	Nel reparto ci sono più postazioni di lavoro collegate alla CCE. Utilizzare un'altra postazione.	Il guasto è rilevabile direttamente dal personale	1	7	Verificare il cavo di collegamento, dotarsi di idonea scorta di materiale di consumo		Ditta preposta alla manutenzione (in caso di guasto riparabile), Ufficio acquisti (in caso di guasto non riparabile), Magazzini	Ogni struttura deve tenere sotto controllo il proprio materiale di consumo, in modo da averne sempre a disposizione. Nel caso, attivazione procedura privilegiata di acquisto urgente.	1	7	1	7

9	SERVER	Gestione della CCE e archiviazione dati	Il Server non funziona	La CCE è indisponibile		6	Guasto hardware o problema software	6	Il Server della CCE è ridondato. Gestire l'attività con cartaceo fino a ripristino	Verifica sistematica di corretto funzionamento	2	72	Verifica costante del corretto funzionamento, aggiornamento sistematico del software di base e di ambiente, aggiornamento quotidiano delle protezioni antivirus.		TBS (Assistenza H24). Intervento immediato per la riattivazione del corretto funzionamento mediante azioni mirate a ripristinare l'hardware e/o il software.	Tutte le componenti hardware sono duplicate ed il sistema è configurato in modo da supportare eventuali guasti di ogni sua parte. Sono in corso la procedure per l'installazione di una nuova struttura aziendale di disaster recovery.	6	6	2	72
10	SERVER	Gestione della CCE e archiviazione dati	Il Server non funziona	La CCE è indisponibile		6	Mancanza di corrente elettrica; aumento della temperatura dei locali CED	6	Il CED è sotto UPS; sono installati rilevatori di aumento di temperatura. Gestire l'attività con cartaceo fino a ripristino	Verifica sistematica di corretto funzionamento	2	72	Verifica di presenza di corrente elettrica. Installazione di allarmi che segnalino anomalie dei parametri di funzionamento dei locali CED (corrente elettrica, temperatura, ecc.)		Servizio Tecnico, manutenzione	E' in corso una valutazione degli impianti elettrici per eventuali adeguamenti (es. aumento delle caratteristiche del gruppo di continuità)	6	6	2	72
11	SERVER	Gestione della CCE e archiviazione dati	La procedure CCE non funziona	La CCE è indisponibile		6	Problema al software di base o di ambiente; problema sulla base dati	6	Il database è sistematicamente monitorato. I dati sono quotidianamente backuppati. Gestire l'attività con cartaceo fino a ripristino	Allarmi automatici	1	36	Sono predisposti allarmi per la verifica del corretto funzionamento della base dati e del monitoraggio dello stato di occupazione degli archivi.		TBS (Assistenza H24). Intervento immediato per la riattivazione del corretto funzionamento mediante azioni mirate a ripristinare il software di base, di ambiente e applicativo	Sono in corso le procedure per l'installazione di una nuova struttura aziendale di disaster recovery.	6	6	1	36
12	CCE	Gestione della CCE: Prescrizione-Somministrazione della Terapia	La procedure Terapia - CCE non è accessibile o non funziona	La Terapia è indisponibile		6	Problema al software di base o di ambiente; problema sulla base dati; problema di connettività	6	Mediante un apposito pulsante predisposto sulla dashboard di terapia del IP,attraverso il quale, l'addetto provvederà periodicamente al salvataggio in locale della stampa della terapia. Vedere direttive dedicate	Il guasto è rilevabile direttamente dal personale sanitario	1	36	Periodicamnete il personale IP dovrà attivare la procedura mediante apposito pulsante, per garantire la presenza di una copia aggiornata della terapia ad uso IP.		TBS (Assistenza H24). Intervento immediato per la riattivazione del corretto funzionamento mediante azioni mirate a ripristinare il software di base, di ambiente e applicativo. CED per la parte infrastruttura.	Sono in corso le procedure per l'analisi / realizzazione della procedura di salvataggio da parte del fornitore TBS	6	6	1	36