ALLEGATO C - 3

DELIBERAZIONE N. - 174

DEL 31 MARZO 2011

COMPOSTO DA N. 26 PAGINE

Regione Piemonte
Azienda Sanitaria Locale VCO
Sede Legale – Via Mazzini 117
28887 – Omegna
C.E.D. / Sistema Informativo

Prot. n.: 15548/09 AG/ag
Allegati: 1

Omegna, 23/02/09

Al Direttore Generale
CSI PIEMONTE

Al Direttore Divisione Sanità
CSI PIEMONTE

p.c. Alla Direzione Generale ASL 14 VCO

Raccomandata A. R.

OGGETTO: *Aggiornamento Documento Programmatico della Sicurezza*

Alla luce di quanto previsto dall'art. 34 del D.Lgs. 196/2003 (indicato anche come CODICE SULLA PRIVACY), entrato in vigore dall' 1/01/2004, si è tenuti ad aggiornare il DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI entro il termine del **31 marzo di ogni anno**, fissato dall'art. 6 del D.L. 9.11.2004 n. 266, convertito in Legge 27.12.2004 n. 306.

Pertanto con la presente si chiede l'aggiornamento del documento dal titolo: "Misure adottate presso la server Farm CSI a garanzia di quanto previsto al punto 19.4 (Allegato B D.Lgs.196/2003)" la cui versione anno 2008 si allega in copia, con preghiera, se ritenuto necessario, di aggiornarlo per l'anno in corso al fine del conseguente aggiornamento del documento programmatico sulla sicurezza dei dati di codesta Azienda.

Non ricevendo nulla **entro il 18 marzo p.v.** si riterrà il documento relativo all'anno 2008 corretto anche per l'anno in corso.

Ringraziando per la collaborazione, si porgono cordiali saluti.

IL DIRETTORE
S.C. C.E.D. / Sistema Informativo
(Dott.ssa Anna GAGLIARDI)

Tel.: 0323-868202/203 Fax: 0323-868220 e-mail: ced@aslvco.it

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.

1.1 OBIETTIVI GENERALI

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.**

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

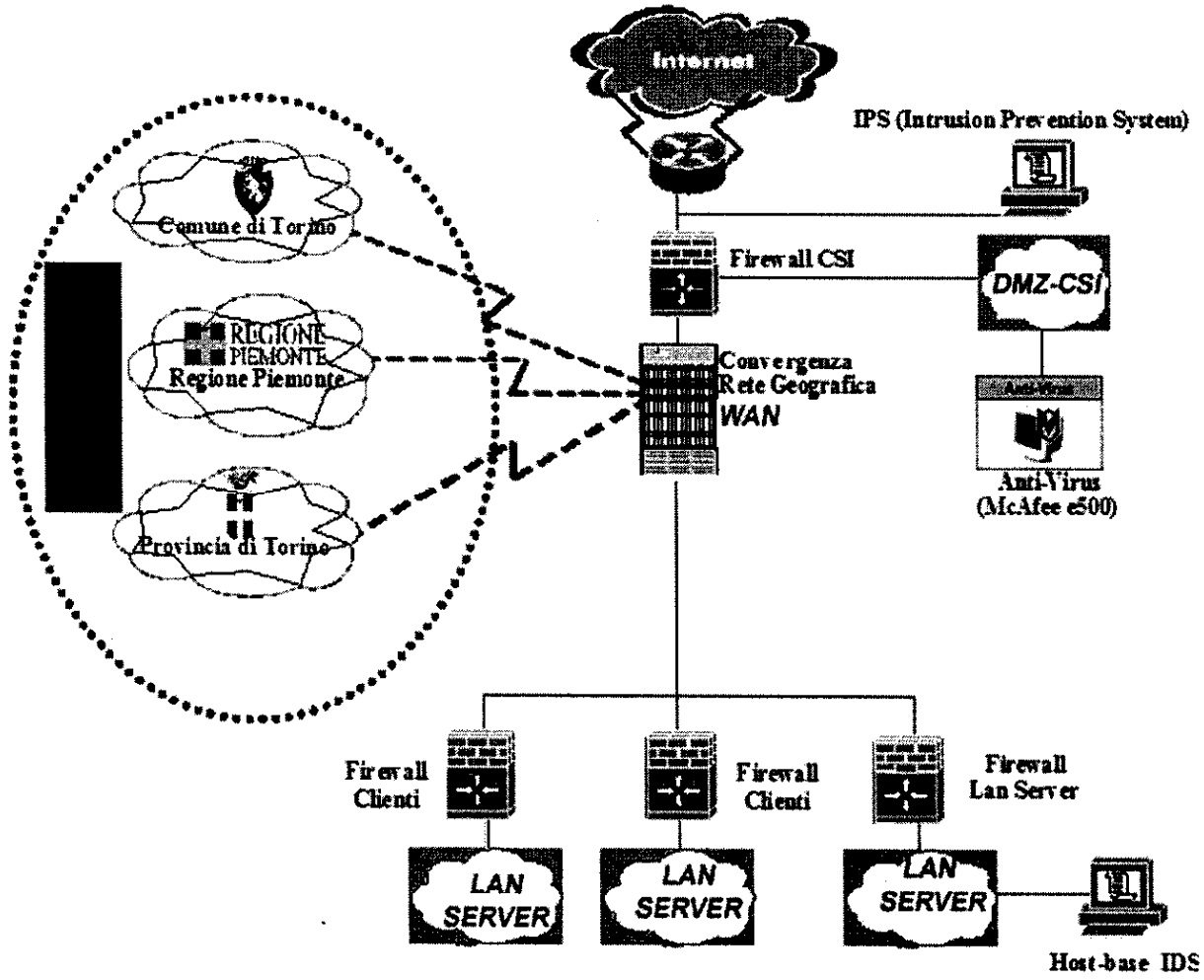
Sono considerati supporti di memorizzazione i nastri magnetici, i dischi magnetici o ottici amovibili, i CD-ROM che contengono informazioni personali.
I supporti contenenti dati sensibili devono (DLgs 196/03) essere custoditi in un'area ad accesso controllato o in un ufficio che sia chiuso quando non 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:

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

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)
- 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.

Tipo di Backup	Frequenza	Retention	Note
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