AZIENDA SANITARIA U.L.S.S. 3
REGIONE VENETO
Via Dei Lotti, 40
36061 BASSANO DEL GRAPPA (VI)

DOCUMENTO PROGRAMMATICO

SULLA SICUREZZA

ALLEGATO Dpss - Strumenti Elettronici

Codice documento:

Rev.	Data	Descrizione	Redatto	Verificato	Approvato
0	28/07/05	Prima emissione			
1	27/03/06	Revisione			
2	30/03/07	Revisione			
3	28/03/08	Revisione			
4	20/03/09	Revisione			
5	22/03/10	Revisione			
6	21/03/11	Revisione			

Indice del documento

1 INTRODUZIONE 3
2 LA RETE....3
2.1 Rete locale (Lan) 3
2.2 Rete Geografica (Wan)....6
3 I SISTEMI 8
3.1 Server presso il SSI....8
3.2 I Client 14
3.3 Manutenzione Parco Macchine 14
4 LE COMUNICAZIONI 15
4.1 Accesso ad Internet....15
4.2 La posta elettronica 16
4.3 Accesso degli Utenti Esterni....17
5 GLI APPLICATIVI 17
5.1 Autenticazione al dominio....17
5.2 Autorizzazione per l'accesso a banche dati/applicazioni 17
5.3 Antivirus....19
5.4 Aggiornamenti software....19
5.4.1 Server....19
5.4.2 Client 19
6 I SERVIZI....20
6.1 Collegamento Rilevazione Presenze....20
7 CRITERI E MODALITÀ PER IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI....20
7.1 Procedure per il salvataggio regolare dei dati 20
7.2 Procedure per l'archiviazione dei supporti di memorizzazione 20
7.3 Procedure per la verifica della leggibilità dei supporti di memorizzazione 20
7.4 Criteri per l'eliminazione dei supporti di memorizzazione obsoleti....20
7.5 Misure per la custodia dei supporti di memorizzazione. 20
7.6 Prove di ripristino....21
7.7 Piano di continuità operativa e ripristino 21

1 INTRODUZIONE

Il Servizio per il Sistema Informatico (nel seguito denominato più semplicemente SSI) opera al servizio di tutte le Strutture complesse e semplici dell'AZIENDA SANITARIA ULSS N°3, garantendo la funzionalità e, quindi, la continuità operativa, della rete, delle telecomunicazioni e degli applicativi generali sui server centralizzati, restando gli applicativi specialistici e procedure non centralizzate sotto il diretto controllo gestionale dei singoli Centri di Responsabilità.

Il presente documento contiene una descrizione del sistema informativo e informatico dall'AZIENDA SANITARIA ULSS N°3 gestite dal SSI.

All'Amministratore di sistema è affidato il compito di redigere e di aggiornare ad ogni variazione il presente documento.

2 LA RETE

Si premette che le reti di telecomunicazione e i relativi apparati sono affidati in gestione all'Associazione temporanee di Imprese composta da Siemens SpA in qualità di capogruppo ed Alfa s.r.l. ed IBM S.p.A. in qualità di mandatarie.

La protezione della rete aziendale si basa sulle seguenti componenti:

- Sistema di firewalling;
- Segregazione delle reti (Virtual Local Area Network VLAN);
- Proxy;
- VPN (virtual private network);
- Sistema di antivirus;
- Controllo accessi.

2.1 RETE LOCALE (LAN)

Tutta l'infrastruttura passiva a sostegno delle reti fonia/dati è stata sviluppata, in ciascuna sede dell'Azienda, secondo quanto prescritto dalla normativa vigente che disciplina il cablaggio strutturato:

- distribuzione orizzontale: cavo cat. 6 (o 5E);
- dorsali verticali dati: cavo in fibra ottica (Gigabit Ethernet/Fast Ethernet);

- dorsali verticali fonia: cavo multi coppia 50/100 coppie.

A livello di apparati di rete tutta la parte di infrastruttura attiva L2/L3 a sostegno della rete dati è stata sviluppata in tecnologia Fast/Giga Ethernet:

Nodo funzionale di edificio:
dorsali di edificio dati: Gigabit Ethernet (o Fast Ethernet)
distribuzione orizzontale: Fast Ethernet con eventualmente link in Gigabit Ethernet configurazione fault tollerance;
duplicazione del nodo (solo nel Presidio Ospedaliero di Bassano)

Nodo funzionale di piano:
dorsali di piano dati: Gigabit ethernet (o Fast Ethernet)
distribuzione orizzontale: Fast Ethernet con eventualmente link in Gigabit Ethernet

Nodo funzionale di zona:
distribuzione orizzontale: Fast Ethernet con eventualmente link in Gigabit Ethernet

Gli apparati installati forniscono a tutte le prese dati in cablaggio strutturato porte di tipo 10/100/1000 autosensing con auto negoziazione presso il Presidio Ospedaliero San Bassiano e porte di tipo 10/100 autosensing con auto negoziazione presso gli altri Presidi Ospedalieri.

La topologia di rete è di tipo gerarchico stellare con possibilità di connettere cavi di dorsale tra livelli uguali di gerarchia, consentendo così la predisposizione di percorsi alternativi.

In particolare per ciascun presidio interessato al servizio si riportano le caratteristiche essenziali:

Presidio San Bassiano:

La rete dati è di tipo switched LAN basata su dispositivi CISCO Systems: al core/distribution sono impiegati due switch Catalyst 65xx, mentre per l'accesso ai piani sono usati switch Catalyst 3550 e 3570.

La rete è sviluppata tramite un centro stella Cisco Catalyst 6513, la struttura si contraddistingue per l'utilizzo di dorsali in fibra ottica multimodale 1000Base-SX per la connessione in trunk degli switch di distribuzione e/o accesso dislocati nei armadi dati del POB e per la presenza di una serie di montanti in fibra di back-up per garantire una continuità ai servizi aziendali primari tramite una parziale ridondanza del nucleo centrale ottenuta mediante trunk con un Cisco catalyst 6509 attivo in un secondo locale.

Presidio di Asiago:

La rete è sviluppata tramite un centro stella Cisco Catalyst 6509, la struttura si contraddistingue per una serie di dorsali in fibra ottica multimodale 1000 Base-sx per le connessioni in trunk degli switch.

Marostica:

La rete è gestita centralmente da uno switch Catalyst 4507R equipaggiato con Supervisor V 1000BaseX per permettere la gestione in Layer 3 e quindi il supporto dei protocolli di routing. Il catalyst core è collegato agli switch periferici con trasporto del trunk tramite protocollo CISCO ISL.

Monsignor Negrin:

La rete è stata aggiornata alla fine del 2010 ed è attualmente gestita da uno switch Cisco Catalyst 4507, opportunamente equipaggiato in modo da migrare dall'attuale modalità layer 2 al layer 3, potendo così espandere tutti i servizi proprietari Cisco, già in uso presso gli ospedali San Bassiano e di Asiago, e al Centro Socio Sanitario "Prospero Alpino" di Marostica.
Tale apparecchiatura permetterà l'ottimizzazione nella gestione delle VLAN perché semplificano la configurazione e rendono molto veloce la comunicazione; inoltre i protocolli proprietari Cisco permetteranno di realizzare percorsi di rete ridondati e gestiti tramite load-balancing per aumentare le garanzie di affidabilità e sicurezza. In questo modo si potranno espandere i servizi aziendali, quali server Web, Servizi terminal e server

multimediali, garantendo che tali servizi rispondano rapidamente anche in situazioni di intenso traffico di rete.

Si avrà così la possibilità di un notevole sviluppo futuro, in particolare, grazie all'implementazione e alla gestione delle VLAN, si potrà ad esempio gestire un sistema wireless basato su access point Cisco, estendere il progetto WIPT tramite WLC e Call-Manager e sfruttare le potenzialità della telefonia IP fissa e mobile, migliorare il funzionamento della centrale telefonica tramite il QoS, elaborare VLAN per i servizi legati agli apparati elettromedicali, gestire in modo appropriato le VLAN create al San Bassiano per l'accesso di ditte esterne, interfacciare il nuovo apparato con il sistema di gestione proprietario CiscoWorks elaborando opportuni monitoraggi del traffico dati. Sarà altresì possibile realizzare una struttura di collegamento verso la rete wireless WAN equivalente a quella presente presso l'ospedale San Bassiano e il Presidio Ospedaliero di Asiago.

Questa topologia di rete, dove i dispositivi radio sono collegati ad uno switch periferico con trasporto del trunk tramite protocollo Cisco ISL, ottimizza le prestazioni dei collegamenti Hyperlan e le funzionalità dei protocolli di routing e spanning-tree

In tutti i distretti dislocati, sul territorio, la realtà della rete dati si presenta eterogenea riconducibile ad un router per la gestione in Layer 3 della rete, un switch L2 per la distribuzione di eventuali montanti in rame/fibra e la presenza di switch per l'accesso alla connettività utente sugli armadi secondari.

2.2 RETE GEOGRAFICA (WAN)

E' presente un sistema wireless con collegamenti radio di tipo PTP (punto-punto) e PMP (punto-multi punto), in tecnica OFDM sulla banda di frequenza dei 5.47 – 5.725 GHz, che collega l'Ospedale San Bassiano alle seguenti sede dell'Azienda:

- Dipartimento di Prevenzione Via Cereria Bassano del Grappa;
- CEOD Via Rosmini di Bassano del Grappa;
- Centro Socio Sanitario "Mons. Negrin" Bassano del Grappa,
- Centro Socio Sanitario "Prospero Alpino" Marostica;
- Distretto Socio Sanitario n.1di Romano d'Ezzelino;
- Sede di Via Carducci

I primi due collegamenti si caratterizzano da un'architettura radio di tipo Punto-Multi Punto (PMP) mentre per le altre sedi l'architettura è di tipo Punto-Punto (PTP).

La soluzione tecnica per l'infrastruttura di rete dati di tipo wireless ad alta capacità per la connessione del Presidio Ospedaliero San Bassiano e del Presidio Ospedaliero di Asiago, consiste nei seguenti collegamenti radio:

1. Link radio a banda larga in tecnica PTP ethernet su PDH a 18 GHZ configurazione 1+0 con antenne paraboliche a disco solido dal diametro di 90 cm, Direct ODU Mount, tra il POB e la struttura "Casa Parco" località S. Giovanni ai colli Alti sul gruppo del Monte Grappa, posti a circa 13 Km di distanza;
2. Link radio a banda larga in tecnica PTP ethernet su PDH a 18 GHZ configurazione 1+0 con antenne paraboliche a disco solido dal diametro di 90 cm, Direct ODU Mount, tra la struttura "Casa Parco" località S. Giovanni ai colli Alti sul gruppo del Monte Grappa ed il secondo sito individuato sul Monte Ekar in prossimità dell'Osservatorio Astronomico, posti a circa 11 km di distanza;
3. Link radio a banda larga in tecnica PTP Ethernet su PDH a 38 GHz, configurazione 1+0 con antenne paraboliche a disco solido dal diametro di 60 cm, Direct ODU Mount, tra il Monte Ekar ed il Presidio Ospedaliero di Asiago, posti a circa 4 Km di distanza.

La banda erogabile netta a livello radio è di 36 Mbps, da suddividere tra le varie interfacce tributarie d'utente, a fronte di un'occupazione di banda RF di 28 MHz.

Il collegamento del distretto n.2 di via Monte Sisemol ad Asiago, è di tipo diretto attraverso ponte radio in tecnologia wireless PTP. Nel corso del 2010 con l'apertura della nuova struttura amministrativa sita presso l'istituto Cavanis è stato implementato un collegamento diretto attraverso ponte radio in tecnologia wireless PTP con capacità nominale di 15 Mbps. E' inoltre attivo un collegamento wireless tra il Presidio Ospedaliero San Bassiano e il Distretto Socio Sanitario n.2 di Enego.

Con le sedi di Marostica e Mons. Negrin è attivo un link con data rate nominale a 28 Mbps. Per la sede di Cassola per il servizio regionale ONGF e quella di Via Carducci è attivo un collegamento diretto attraverso tecnologia wireless PTP.

Ai collegamenti wireless sopraccitati si aggiungono i collegamenti di back-up con tecnologia ISDN con banda a 128 kbps esclusa la connessione di back-up tra i due Presidi Ospedalieri che si basa su un collegamento HDSL con 2 Mbps garantiti.

Le rimanenti sedi del territorio sono collegate tramite il centro stella HDSL.

Con la creazione del nodo HDSL ad elevate prestazioni presso il POB si è effettuato il collegamento con le sedi remote tramite l'installazione di un accesso ADSL; presso il POB è attivo il nodo DSL mediante router dedicato Cisco con accesso di tipo HDSL.

Le sedi attualmente raggiunte sono:

- Veterinari Asiago;
- Casa di riposo Villa Serena;
- Bassano Via Angarano;
- Hospice Casa Gerosa;
- Veterinari di Rosà;
- Distretto n. 1 di Rosà;
- Rossano Veneto;
- San Nazario;
- Casa di riposo di Valstagna;
- Conco;
- Tezze sul Brenta;
- Casa di Riposo di Cartigliano;
- Casa di Riposo Sturm.

3 I SISTEMI

3.1 SERVER PRESSO IL SSI

Presso il SSI sono allocati i seguenti server, ciascuno con le relative procedure/servizi:

- Coppia di Server, su cui sono state create delle istanze di database virtualizzate in cluster, per la gestione delle seguenti procedure:
  - Prenotazioni e Cassa;
  - Gestione Ricoveri;
  - Anagrafe Sanitaria;
  - Ecografie Ostetriche;
  - Cardiologia;
  - Repository per i referti del Laboratorio Analisi;
  - Gestione sistema informativo per l'informatizzazione del percorso chirurgico del paziente (sale operatorie);

- Pronto Soccorso;
- Endoscopia;
- Radiologia;
- Spisal;
- Gestione del backup dei database Oracle mediante tecnologia rman;
- Ambiente di test per le procedure Prenotazioni e Cassa, Gestione Ricoveri e Cardiologia;
- Ambiente in cui vengono realizzate le stampe e la reportistica aziendale della procedura Prenotazioni e Cassa e Gestione Ricoveri.

- Coppia di Server su cui sono state realizzate due istanze di database in cluster per la gestione delle seguenti procedure:
  - Laboratorio Analisi;
  - Microbiologia;
  - Cartella clinica informatizzata del Dipartimento di Medicina e Fisica Riabilitativa;
  - Cartella clinica informatizzata per la Pneumologia (broncoscopia);
  - Servizi Territoriali: Assistenza Domiciliare (Medici, Infermieri), RSA, Case di Riposo, Unità di Valutazione, Consultori, Centro Salute Mentale, Psichiatria Territoriale, Neuropsichiatria Infantile, Medicina Legale, Invalidi Civili.

- Coppia di Server su cui sono state realizzate due istanze di database in cluster per la gestione delle seguenti procedure:
  - Laboratorio Analisi per la consultazione dello storico;
  - Anatomia Patologica;
  - Genetica Medica;
  - Repository per la consultazione storica dei referti di Laboratorio Analisi antecedenti a Giugno 2010.

- Un server su cui sono state create tre istanze virtualizzate per la gestione delle procedure amministrative-contabili con relativo ambiente di test.

- Due server virtualizzati sui quali risultano installate gli application server delle seguenti procedure:

- Prenotazioni e Cassa con relativo ambiente di test (coppia di server in load balacing);
- Gestione Ricoveri con relativo ambiente di test (coppia di server in load balacing);
- Repository per i referti del Laboratorio Analisi con relativo ambiente di test (coppia di server in cluster);
- Prenotazioni e consultazione esiti esami per Laboratorio Analisi ed Anatomia Patologica da parte dei reparti ospedalieri interni;
- Tivoli storage management per la gestione delle copie di back-up;
- Syslog-Ng per la gestione dei log degli accessi ai sistemi degli “amministratori di sistema”, in ottemperanza al provvedimento del garante della privacy del 27 novembre 2008.

➢ Due server virtualizzati sui quali risultano installate gli application server in cluster delle seguenti procedure:

- Anatomia Patologica;
- Genetica Medica;
- integrazione applicativo Anatomia Patologica con apparecchiature elettromedicali mediante protocollo HL7;
- Broncoscopia;
- Gestione sistema informativo per l’informatizzazione del percorso chirurgico del paziente (sale operatorie);
- Gestione servizi integrati per l’invio in hl7 dei referti del Laboratorio Analisi al repository aziendale;
- Servizi Territoriali: Assistenza Domiciliare (Medici, Infermieri), RSA, Case di Riposo, Unità di Valutazione, Consultori, Centro Salute Mentale, Psichiatria Territoriale, Neuropsichiatria Infantile, Medicina Legale, Invalidi Civili;
- Servizio cuponline per l’integrazione con le procedure di prenotazioni e cassa di altre Aziende Sanitarie (servizio non in cluster);
- Servizio cuplite per la gestione delle prenotazioni ed annulli delle prestazioni sanitarie da remoto da parte del cittadino e per la visualizzazione della prima disponibilità in agenda (servizio non in cluster).

- Due server virtualizzati sui quali risultano installati i seguenti servizi:
  - Cartella informatizzata Centro Antidiabetico;
  - Gestione dei collegamenti in VPN dall'esterno verso la rete aziendale; il software funge anche da firewall limitando le risorse hardware rese disponibili al soggetto autorizzato ad accedere. L'autenticazione e l'abilitazione all'accesso avvengono attraverso un servizio integrato in tecnologia RADIUS. Il servizio viene utilizzato esclusivamente dalle Ditte che devono prestare assistenze sui Sistemi Informativi Aziendali, dopo aver compilato un regolare modulo di richiesta di accesso.

- Un server, posizionato in una rete logicamente separata da quella aziendale, dedicato alle integrazioni applicative tra il Laboratorio Analisi dell'Ulss n.3 di Bassano del Grappa e il Laboratorio Analisi dell'Ulss n. 6 di Vicenza mediante la rete intranet regionale in protocollo hl7.

- Un server su cui risulta installato un motore hl7 per l'integrazione della cartella clinica informatizzata della Cardiologia con la procedura Cup/Cassa per il passaggio dell'anagrafica dei contatti aziendali e delle work-list di competenza.

- Un server posizionato in DMZ, che funge da reverse-proxy, per la corretta gestione in sicurezza del servizio cuponline, per l'integrazione con le procedure di prenotazioni e cassa di altre Aziende Sanitarie.

- Un server posizionato in DMZ, che funge da reverse-proxy, per la corretta gestione in sicurezza del servizio cuplite per la gestione delle prenotazioni delle prestazioni sanitarie da remoto da parte del cittadino e per la visualizzazione della prima disponibilità in agenda.

- Un server su cui risulta configurata un'istanza SqlServer 2005 per le seguenti procedure:
  - Protocollo;
  - Delibere;
  - Ufficio Legale;

- Ufficio Formazione;
- Cartella informatizzata del Centro Antidiabetico;
- Procedura di customer satisfaction "Progetto Emoticons".

- Un server su cui risulta installata un'istanza di database per le seguenti procedure:
  - procedure per la gestione del Data Warehouse e del budget aziendale;
  - vecchia procedura per la gestione delle vaccinazioni, sostituita da metà 2009 da una procedura centralizzata regionale.

- Un server web su cui risulta installato un application server IIS per accedere alla procedure di protocollo informatico, delle delibere, dell'Ufficio Legale e del "Progetto Emoticons".

- Un server su cui risultano installati i Servizi Terminal utilizzati per accedere alle seguenti procedure:
  - ambiente di Data Warehouse aziendale e gestione budget aziendale;
  - Procedura Spisal (Servizio Prevenzione Infortuni sul lavoro).

- Un application server per la gestione del software del caricamento dei flussi provenienti dalle casse automatiche e dal servizio di tesoreria bancario per i pagamenti del ticket sanitario relativi alla procedura Cup/Cassa;

- Un application Server per la gestione dello storico del Repository di Laboratorio Analisi;

- Una coppia di server, l'uno l'immagine dell'altro, per la gestione dei collegamenti con la Regione Veneto e le altre Aziende Sanitarie del Veneto mediante la tecnologia delle "PORTE DI DOMINIO"; utilizzato per l'accesso esterno allo storico del Repository di Laboratorio Aziendale attraverso il Portale IESS regionale e per il Cup Provinciale;

- Un server per la gestione dei collegamenti con la Regione del Veneto mediante la tecnologia delle "PORTE DI DOMINIO", da utilizzare per l'integrazione in hl7 per

l'allineamento tra l'anagrafe regionale e quella aziendale dei contatti. Il server è posizionato in una rete logicamente separata da quella aziendale. Attualmente l'attivazione dell'anagrafe regionale è in fase di test.

- Un server per la gestione delle seguenti procedure:
  - Ufficio Relazioni con il Pubblico;
  - Mobilità sanitaria.

- Un apparato MPLS utilizzato per la connessione in modalità VPN-SSL dall'esterno, mediante il canale pubblico, alla rete dati dell'Azienda Sanitaria da parte dei seguenti soggetti:
  - Farmacie per la distribuzione dei referti del Laboratorio Analisi;
  - Case di riposo per consultazione dei referti del Laboratorio Analisi e richiesta farmaci al Servizio Farmaceutico Ospedaliero;
  - Mmg-pls per depositare i flussi operativi come previsto dalla DGRV n. 3578/2009 in attuazione dell'ACN 2009;
  - poliambulatori per l'emissione di fatture a nome di medici dipendenti dell'Azienda Sanitaria che, prestano presso di loro attività in libera professione allargata;
  - Aziende software per assistenza e manutenzione applicativi in uso presso l'Azienda Sanitaria.

- Una coppia di server, che fungono da Domain Controller primario e secondario indipendenti l'uno dall'altro e che contengono i database di Active Directory (utenti di dominio e relative abilitazioni) e la gestione dei servizi di DNS, DHCP e WINS.

- Quattro server, che fungono da Domain Controller per le sedi esterne (Presidio Ospedaliero di Asiago, C.S.S. di Marostica, Sede Distrettuale di Monsignor Negrin e Sede Distrettuale del Dipartimento di Prevenzione di via Cereria), ove risultano essere fisicamente dislocati in luoghi non accessibili se non da personale autorizzato;

- Un server Exchange per la gestione della posta aziendale;

- Un ISA server per la gestione dei collegamenti esterni (tipicamente Internet) che funge da proxy e da firewall;

- Un server per la gestione degli aggiornamenti automatici dei seguenti software aziendali:
  - sistemi operativi aziendali (Windows 2000 Professional e Xp Professional);
  - prodotto di Office Automation della Microsoft (Office Xp, 2003 e 2007);
  - Antivirus McAfee con cadenza giornaliera.

- Uno storage (NAS) con il quale è stato messo a disposizione degli utenti uno spazio per la condivisione di documenti all'interno dello stesso Reparto/Ufficio, il cui accesso è limitato sfruttando le credenziali del dominio aziendale. Nello storage vengono memorizzate le copie di backup del Servizio Informatico sia per quanto riguarda i sistemi operativi che le copie fisiche e logiche dei database.

3.2 I CLIENT

Il parco macchine è attualmente costituito da circa 1100 personal computers, per la maggior parte desktop e con un numero limitato di notebook, dotati di sistema operativo Windows 2000 Professional (circa 100) o Windows Xp Professional (circa 1000) regolarmente aggiornati con i Service Pack e le patch rilasciate mensilmente da Microsoft. La distribuzione attuale sulle varie sedi aziendali è approssimativamente la seguente:

- 700 client a Bassano;
- 100 ad Asiago;
- 100 in via Monsignor Negrin;
- 40 in Dipartimento di via Cereria;
- 50 nell'ospedale di Marostica;
- i rimanenti sono dislocati presso le sedi territoriali aziendali.

Tutti i client, prima di essere distribuiti, vengono configurati dal Servizio Informatico con l'installazione del Sistema Operativo proprietario, dell'Antivirus, del software di Office Automation e di tutti quei software licenziatari oppure Open Source necessari all'utente per espletare le sue attività quotidiane.

Ciascun Personal Computer è assegnato ad una persona fisica che viene individuata dal responsabile del Centro di responsabilità a cui il bene viene assegnato.

L'accesso alle risorse di rete avviene mediante l'assegnazione di un indirizzo in DHCP tranne in alcuni casi eccezionali per i quali è necessario assegnare alle apparecchiature un indirizzo statico e riservato.

3.3 MANUTENZIONE PARCO MACCHINE

La manutenzione hardware dei server viene effettuata dai rispettivi produttori/fornitori; mentre per quanto riguarda i client viene effettuata da un'Azienda esterna gestita dall'Ufficio Impianti e telecomunicazioni.

Al momento di espletare l'intervento il personale tecnico deve contattare gli operatori del SSI che, dopo aver valutato la necessità dell'operazione, provvedono a rendere disponibile l'accesso alla macchina mediante l'utente amministratore sbloccandone la relativa password, sarà compito successivamente della Ditta contattare il SSI per il ripristino della stessa.

Ad intervento concluso i manutentori esterni firmano un modulo di intervento validato dall'utente, che ne ha richiesto l'intervento, in cui vengono espletate le operazioni eseguite e successivamente valutato dal personale Aziendale preposto.

4 LE COMUNICAZIONI

4.1 ACCESSO AD INTERNET

Gli accessi ad Internet sono messi a disposizione dopo la compilazione di un apposito modulo cartaceo firmato dall'utente e dal Responsabile del “Centro di Responsabilità” a cui egli afferisce.

Propedeutica all'abilitazione è la creazione del corrispettivo utente di dominio, con l'assegnazione di uno username e di una password che, sono utilizzati per accedere ai personal computer posti nel dominio aziendale (autenticazione mediante firma elettronica debole) e ,conseguentemente dopo la corrispettiva abilitazione alle funzionalità del servizio di Internet. Tutti gli accessi a Internet sono nominali e non vengono resi disponibili

ad utente generici. Gli accessi vengono gestiti da un Server ISA che funge da Proxy e da Firewall.

Al momento non sono previste soluzioni di High Availability per Firewall e Proxy.

Le attività di manutenzione del Router utilizzato per i collegamenti è a carico della ditta fornitrice e viene seguito dalla ditta che gestisce il servizio in outsourcing.

Collegamenti Esterni

Esistono anche due collegamenti esterni realizzati mediante router Cisco di proprietà di terzi, che erogano i servizi ed a carico dei quali sono le relative attività di manutenzione:

- collegamento con la Regione del Veneto (intranet ed extranet regionale);
- collegamento con il Server della ditta Sigma per la gestione centralizzata delle procedure dell'Ufficio Personale.

Entrambi i collegamenti sono monitorati da un firewall in modo da limitare agli utenti i solo servizi necessari ed alle ditte fornitrici la visione dei soli router di loro proprietà.

4.2 LA POSTA ELETTRONICA

L'abilitazione al Servizio di Posta Elettronica aziendale è messo a disposizione degli utenti dopo la compilazione di un apposito modulo cartaceo firmato dallo stesso e dal Responsabile del “Centro di Responsabilità” a cui egli afferisce. Il servizio è gestito da un Server Exchange integrato con Active Directory pertanto anche in questo caso propedeutica all'abilitazione è la creazione di un utente di dominio. Tutti gli accessi al Servizio sono nominali e non vengono resi disponibili ad utente generici. A disposizione di ogni singolo utente vi è sul server uno spazio predeterminato; su richiesta, nel caso in cui si manifesti la necessità, la posta viene scaricata sul personal computer intestato all'utente stesso con l'avvertenza che, a quel punto le eventuali copie di backup non sono più a carico del SSI ma del singolo utente stesso.

Al momento non sono previste soluzioni di High Availability per il Server di Exchange, la protezione da virus ed eventuali agenti esterni viene assicurato da un antivirus regolarmente aggiornato.

4.3 ACCESSO DEGLI UTENTI ESTERNI

L'accesso degli utenti esterni può avvenire in due modi:

- ✓ per le ditte fornitrici di software e/o servizi aziendali che effettuano attività di manutenzione, avviene attraverso un server VPN (protocollo PPTP) che funge anche da firewall limitando agli utenti l'accesso ai soli servizi da loro erogati. L'autenticazione avviene mediante un server Radius integrato con l'Active Directory per cui, ogni utente esterno per accedere, deve compilare un modulo scritto di richiesta di creazione utente di dominio con il quale viene abilitato al Servizio. L'abilitazione avviene su richiesta ad un particolare indirizzo di posta elettronica messo a disposizione dal SSI specificando motivazione e scopo dell'intervento e a conclusione dello stesso ne viene richiesta la disabilitazione; in ogni caso è attiva una regola sul firewall per la quale alle ore 20,00, salvo eccezioni particolari, tutte le connessioni attive vengono disabilitate automaticamente e non risulta più possibile accedere al Servizio.
- ✓ per la connessione VPN-SSL dall'esterno, mediante il canale pubblico, alla rete dell'Azienda Sanitaria è attivo un apparato MPLS abilitato ai seguenti soggetti:
  - farmacie per la distribuzione dei referti del Laboratorio Analisi;
  - case di riposo per consultazione dei referti del Laboratorio Analisi e richiesta farmaci al Servizio Farmaceutico Ospedaliero;
  - mmg-pls per depositare i flussi operativi come previsto dalla DGRV n. 3578/2009 in attuazione dell'ACN 2009;
  - alcuni poliambulatori per l'emissione di fatture a nome di medici dipendenti dell'Azienda Sanitaria che prestano presso di loro attività in libera professione allargata.

GLI APPLICATIVI

4.4 AUTENTICAZIONE AL DOMINIO

L'abilitazione all'accesso ai pc posti nel dominio aziendale viene concessa agli utenti dopo la compilazione di un apposito modulo cartaceo firmato dallo stesso e dal Responsabile del "Centro di Responsabilità" a cui egli afferisce. Il SSI procede con la

creazione dell'utente di Active Directory e l'assegnazione della relativa password provvisoria che deve essere modificata dall'utente al primo accesso.

Nella realtà aziendale esistono anche degli utenti generici a cui non risulta però abilitato alcun servizio o applicativo in modo automatico ma vengono utilizzati solo per accedere alle risorse messe a disposizione dal personal computer successivamente sarà necessario un ulteriore utente per accedere agli applicativi aziendali.

L'utente ha accesso a tutti i client collegati alla rete aziendale e posti in dominio, generalmente solo su quello a lui intestato o utilizzato per la sua attività quotidiana vengono installati e/o configurati i programmi e/o Servizi richiesti (es. Posta Elettronica), negli altri egli ha diritto ad accedere ad un insieme ben identificato di applicazioni (es. Internet, Posta Elettronica mediante l'accesso web, applicativi web). Il profilo dell'utente risulta essere diverso a seconda del personal computer a cui egli accede.

Su ogni client è configurato un utente amministratore utilizzato per le attività di manutenzione ed installazione di nuovo software la cui password è conosciuta solo dal personale del SSI.

Tutte le password di autenticazione al dominio sono lunghe almeno 8 caratteri, hanno validità di 90 giorni scaduti i quali devono essere modificate senza poter riutilizzare le precedenti.

4.5 AUTORIZZAZIONE PER L'ACCESSO A BANCHE DATI/APPLICAZIONI

Tutte le procedure applicative gestite dal SSI prevedono un ulteriore User ID e Password per l'accesso diverso rispetto a quelli utilizzati per accedere al dominio.

L'abilitazione all'applicativo è messo a disposizione degli utenti dopo la compilazione di un apposito modulo cartaceo firmato dallo stesso e dal Responsabile del "Centro di Responsabilità" a cui egli afferisce.

Al momento della creazione dell'utente viene assegnato uno username ed una password lunga almeno 8 caratteri con una scadenza della stessa impostata a 90 giorni, successivamente sarà compito dell'utente procedere con il cambiamento della stessa al primo accesso ed alle successive scadenze. Ogni applicativo gestisce anche la profilazione ossia la possibilità di abilitare all'utente solo quelle funzionalità necessarie per l'espletamento delle sue attività lavorative.

Esistono delle procedure che consentono al SSI di resettare le password nel caso in cui queste siano andate smarrite ma questo avviene solo previa autorizzazione scritta dell'interessato.

4.6 ANTIVIRUS

La protezione di tutte le postazioni di lavoro collegate alla rete aziendale e dei server avviene attraverso un antivirus server che garantisce con cadenza giornaliera l'aggiornamento automatico del relativo database attraverso un collegamento al sito McAfee.

4.7 AGGIORNAMENTI SOFTWARE

4.7.1 Server

4.7.1.1 Software di base e Oracle

Quando viene rilasciata una patch sia per quanto riguarda i database (Oracle e SqlServer) che per quanto riguarda i sistemi operativi (Windows o AIX) questa viene verificata a cura dei sistemisti e solo successivamente applicata.

4.7.1.2 Software applicativo

Gli aggiornamenti per rimediare ad eventuali bug sia quelli evolutivi vengono applicati a cura dei manutentori esterni sotto la supervisione del SSI.

4.7.2 Client

Gli aggiornamenti sul sistema operativo vengono effettuati in automatico, dopo l'approvazione da parte dei sistemisti Windows, mediante VSUS, tale metodologia viene applicata anche per tutti i prodotti Microsoft (es. Office, Internet Explorer), questo permette di mantenere i pc sempre aggiornati e non esposti ad eventuali bug.

5 I SERVIZI

5.1 COLLEGAMENTO RILEVAZIONE PRESENZE

Il server dell'ATI Siemens, che gestisce la Rilevazione Presenze del personale dipendente, è collegato su linea dedicata a SIGMA, ditta che gestisce il relativo servizio, via router Cisco. I dati vengono trasmessi mediante protocollo FTP.

6 CRITERI E MODALITÀ PER IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI

6.1 PROCEDURE PER IL SALVATAGGIO REGOLARE DEI DATI

Il salvataggio dei dati è una procedura che ricopre una funzione cruciale. Attraverso questa procedura, è possibile, in caso di guasto hardware dei dischi, "ripristinare" il sistema nello stesso stato in cui si trovava nel momento dell'ultimo salvataggio.

Tutti documenti informatici contenenti dati personali vengono salvati.

La tipologia e la pianificazione dei salvataggi sono riportate in apposito documento (DPSS-Backup) conservato presso il Servizio per il Sistema Informatico.

6.2 PROCEDURE PER L'ARCHIVIAZIONE DEI SUPPORTI DI MEMORIZZAZIONE

I supporti di memorizzazione vengono etichettati con informazione per l'identificazione e conservati.

6.3 PROCEDURE PER LA VERIFICA DELLA LEGGIBILITÀ DEI SUPPORTI DI MEMORIZZAZIONE

La verifica dell'integrità dell'informazione memorizzata viene eseguita ogni volta in modo automatico dal software; vengono inoltre regolarmente controllati i file di log.

6.4 CRITERI PER L'ELIMINAZIONE DEI SUPPORTI DI MEMORIZZAZIONE OBSOLETI

I supporti rimovibili, se non utilizzati, sono distrutti o resi inutilizzabili.

Possono essere riutilizzati da altri incaricati se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

6.5 MISURE PER LA CUSTODIA DEI SUPPORTI DI MEMORIZZAZIONE.

I supporti dei backup settimanali vengono custoditi in armadio chiuso a chiave presso un locale del Servizio Ingegneria Clinica, situato in uffici esterni al SSI, sempre presso l'Ospedale di San Bassiano.

6.6 PROVE DI RIPRISTINO

Periodicamente vengono eseguite prove di ripristino dei dati dagli incaricati delle copie di sicurezza.

6.7 PIANO DI CONTINUITÀ OPERATIVA E RIPRISTINO

L'obiettivo del piano di continuità operativa è quello di garantire la continuità del servizio informatico e la disponibilità delle informazioni, evitando o limitando i danni al patrimonio informativo a fronte di una emergenza.

Il ripristino è un processo di ricostruzione dell'operatività dell'infrastruttura a seguito dell'evento dannoso.

Si ha bisogno di un piano di continuità operativa e ripristino in caso di danneggiamento delle risorse (dati o strumenti), come ad esempio:

- Failure delle apparecchiature (es. disk crash)
- Rottura dei power supply o apparecchiature di telecomunicazione
- Failure degli applicativi o corruzione dei database
- Errori umani, sabotaggio
- Malicious Software (Viruses, Worms, Trojan horses)
- Hacking o altri attacchi Internet attacks
- Social engineering
- Eventi naturali: Acqua, Fuoco, terremoti, intemperie

Il piano di continuità operativa e ripristino non deve essere inteso come misura alternativa a quelle di prevenzione, ma a completamento di queste ultime.

Le misure di sicurezza preventive, che rilevano e/o riducono l'impatto, adottate dall'AZIENDA SANITARIA ULSS N°3 sono:

- Auditing: tutte le misure di sicurezza adottate vengono verificate periodicamente;
- Aggiornamenti software di base e applicativo;
- Aggiornamenti antivirus;
- Manutenzione periodica di reti e sistemi;
- Gruppi UPS;

- High availability: dischi configurati in modo che il guasto di uno di questi non comporti alcuna perdita di dati (utilizzo di RAID DP e RAID 5 sui server principali e mirroring sugli altri); clusterizzazione dei server principali;
- Salvataggio regolare dei dati.