REGOLAMENTO DI SICUREZZA ICT

Sistemi di protezione e sicurezza dei dati

La sicurezza ICT (**tecnologie dell'informazione e della comunicazione)** è un processo che coinvolge la rete, gli host, i software e gli operatori e, in quanto processo, non è una condizione stabile ma va continuamente adeguata alle nuove esigenze.

Obiettivi del presente regolamento sono:

1. fornire un modello organizzativo e un insieme di regole per la tutela della rete, delle apparecchiature e dei software;
2. Fornire delle regole per la gestione del posto di lavoro e la sicurezza dei dati personali.

La struttura organizzativa responsabile della rete aziendale è il Servizio Informativo aziendale che in collaborazione con la ditta esterna che gestisce la rete si occupa della progettazione, della realizzazione e del continuo aggiornamento della rete esistente.

PARTE I° La Rete Aziendale

1.1 la rete informatica aziendale

La rete aziendale è costituita:

- dal collegamento alla rete Internet con un doppio collegamento a banda larga con accesso simmetrico da 100Mbps e 60Mbps con portante in fibra ottica, livello di servizio L5 a due vie. Sono presenti 2 router Cisco 3800 con i relativi firewall Fortigate 3600° per il collegamento da 100 e 2 Huawei con relativi firewall Cisco 525x per il collegamento da 60 (utilizzato per consentire l'accesso al sito aziendale e la connettività con il Cup-Regionale). Sull' accesso verso internet sono stati implementati i servizi di security obbligatori previsti da Cnipa ora Agid: Firewall Management, Network Intrusion Detection System Management, Event e Log Monitoring Management, Antivirus e Content Filtering Management, Vulnerability Assessment forniti da Wind secondo le modalità previste dalle specifiche tecniche del capitolo di gara aggiudicato da Consip;
- dalle sottoreti (LAN) afferenti alle varie U.O. che fanno rifermento a vari armadi di piano collegati via fibra al centro stella ;
- dai servizi di gestione della rete;
- dai servizi applicativi di base forniti sulla rete, quali Posta, News, Proxy, Web;
- dal servizio di accesso remoto via tunnel VPN solo per fornitori di servizi espressamente autorizzati;
- da tutti quegli strumenti di interoperabilità e apparati attivi di rete che permettono ai soggetti autorizzati di accedere alla rete e di comunicare tra loro.

1.2 Protocolli consentiti

Nella rete aziendale è garantito il supporto per la suite di protocolli TCP/IP, di norma vengono consentite tutte le porte utilizzate dai diversi applicativi ed in particolare le porte 80, 8080 e dei protocolli SMNP e UDP. E' possibile utilizzare anche altri protocolli, su richiesta autorizzata dal gestore della rete.

E' vietato avere risorse condivise su proprio PC, qualora dovessero emergere esigenze di servizio, è necessario concordare con il SIA la soluzione più sicura per la rete.

1.3 Soggetti che possono accedere alla rete

L'acceso alla rete è consentito al personale aziendale previa opportuna autenticazione.
Gli utenti non accedono al sistema con i privilegi di amministratore in quanto è vietata l'installazione di applicativi non autorizzati.
Ogni utente, dopo aver fornito le proprie credenziali può navigare in internet su tutti i siti istituzionali ad eccezione de siti inseriti nelle categorie di cui all' allegato n.1.

1.4 Accesso/estensioni della rete via VPN

Il servizio VPN è disponibile solo per alcuni fornitori di servizi dell'A.O. Moscati che hanno rappresentato al SIA la necessità di operare come se fossero connessi direttamente alla rete aziendale dalla loro sede remota (ad es. per utilizzo e monitoraggio dei propri applicativi, verifica di funzionamento ed aggiornamento di apparecchiature elettromedicali). L' accesso in VPN dell'utenza in questa modalità viene gestito centralmente dal gestore della rete; gli utenti connessi tramite opportuna autenticazione, vengono mappati su una classe di rete dedicata e possono raggiungere solo i sistemi indicati e solo per i servizi richiesti nella nota trasmessa al SIA.

1.5 Le reti wireless

La rete wireless attiva solo all'interno delle varie U.O. di degenza è stata progettata e realizzata al fine di consentire la consultazione e l'aggiornamento della cartella clinica a letto del paziente sia per attività mediche che infermieristiche con l'ausilio di portatili o tablet. Su tali dispositivi non è consentito l'accesso ad internet e ad altre applicazioni aziendali. Per quanto riguarda la sicurezza, l'implementazione della soluzione wireless è tale da garantire l'accesso soltanto agli utenti abilitati (autenticazione) e prevede la criptazione del traffico (riservatezza), per portare il livello di sicurezza di questo tipo di reti allo stesso livello garantito da quelle cablate.

1.6 Assegnazione degli indirizzi IP

Gli indirizzi IP per gli host all'interno della rete aziendale vengono assegnati dal SIA, in modo statico. Il piano di indirizzamento IP della rete è amministrato dal SIA. I servers DNS da configurare sui vari hosts sono curati e mantenuti dal gestore della connettività di rete. Solo per la sottorete del laboratorio d'Analisi l'assegnazione degli indirizzi I.P. viene concordata con il fornitore e gestore del software del laboratorio d' Analisi.

1.7 Identificazione dei soggetti in rete

Tutti gli utenti a cui vengono forniti accessi alla rete aziendale sono riconosciuti ed identificabili; Ogni utente che si collega ad un applicativo specifico deve fornire le proprie credenziali di accesso.

1.8 Inserimento in rete di un Host

L'inserimento di un host nella rete aziendale sarà a carico del SIA, tramite la società che assicura la manutenzione su vari P.C. dell' A.O. che:

- assegna un indirizzo IP al pc;
- Installa una protezione antivirus fornita dal SIA per i sistemi operativi che lo necessitino;
- Controlla se la macchina dispone di servizi di rete e in caso affermativo elimina tutti i servizi non autorizzati;
- Applica tempestivamente tutte le patches di sicurezza del sistema e degli applicativi di cui si intende fare uso e ne mantiene l'aggiornamento nel tempo.

Il responsabile dell' U.O. è ritenuto responsabile di tutte le PDL assegnate.

1.9 Limiti di utilizzo della rete da parte degli host

Un host che produce un grande flusso di dati in rete diviene fonte di problemi per la rete, in questi casi il SIA, dopo opportuna verifica potrà disabilitare tale host dalla rete, finché non viene rimossa la causa della anomalia.

1.10 Attività di logging

Il gestore della rete Wind opera un'attività di logging sui router della rete WAN allo scopo di produrre statistiche di utilizzo, occupazione di banda e tipologia di servizio/protocollo. Tale attività consente di ottimizzare i flussi di dati entro la rete aziendale. Solo su espressa richiesta del Sia è possibile ottenere i report statistici. Questi log sono conservati per periodi di un anno da parte del gestore in modo da consentire eventuali indagini interne o richieste dall'autorità giudiziaria, nei casi in cui si verifica un uso improprio delle risorse. Solo il SIA nella figura dell'amministratore della rete può monitorare al momento ed occasionalmente il traffico sulla rete al fine di valutare e prevedere disfunzioni attive.

1.11 Provvedimenti verso i trasgressori

In caso di accertata inosservanza delle norme di utilizzo della rete, il SIA prenderà le opportune misure, necessarie al ripristino del corretto funzionamento della rete, compresa la sospensione dell'accesso alla rete stessa da parte del trasgressore per motivi cautelari. In caso di reiterata inosservanza, per colpa grave o dolo, il trasgressore sarà segnalato al proprio responsabile per un eventuale provvedimento disciplinare secondo la normativa vigente. In caso di misure d'emergenza, tese a salvaguardare il funzionamento della rete nel suo insieme o in una delle sue parti (es: attacchi D-DOS, Worm ecc.), il gestore della rete , come misura transitoria, può attuare una sospensione parziale o totale all'accesso alla rete di un singolo o di un'intera LAN, oppure di uno o più servizi di rete o effettuare una riduzione anche drastica nella banda assegnata a una certa struttura o su un particolare link WAN.

PARTE II° Gestione del Posto di Lavoro

2 Gestione del posto di lavoro e sicurezza dei dati personali

Scopo di questo articolo è quello di contribuire alla massima diffusione della cultura della sicurezza e ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza del sistema nella sua complessità. Si richiede pertanto agli utenti del sistema di:

Acquisire piena consapevolezza e comprensione delle norme, regole e procedure operative emanate dall'amministrazione in merito all'accesso e utilizzo degli strumenti informatici messi a disposizione nonché all'uso corretto di internet e posta elettronica sul luogo di lavoro e al rispetto dei principi generali in materia di privacy e trattamento dei dati personali.

2.1 Utenti della rete Aziendale

Gli utenti della rete aziendale possono essere utenti interni: personale dirigente e di comparto a tempo indeterminato e a tempo determinato e collaboratori occasionali e utenti esterni: ditte fornitrici di software che effettuano attività di manutenzione sulle applicazioni di propria competenza. A tutti gli utenti viene fornito un account di accesso per lo svolgimento delle proprie attività.

2.2 Accesso alle aree di trattamento di dati personale

L'accesso alle aree dove vengono trattati i dati personali è consentito esclusivamente al personale dipendente e al personale collaboratore al quale è stato attribuito specifico incarico. L'accesso per il personale esterno è consentito sotto il controllo e la responsabilità dei dipendenti e collaboratori incaricati.

2.3 Gestione e utilizzo del posto di lavoro

L'amministrazione considera il sistema informativo e i servizi informatici messi a disposizione uno strumento fondamentale dell'attività lavorativa, che consente la possibilità di accedere ad un vasto patrimonio di risorse informative.
Gli utenti del sistema informativo sono tenuti ad utilizzare i sistemi e servizi informatici messi a disposizione in modo responsabile e con diligenza professionale.
L'azienda mette a disposizione delle U.O. sanitarie le apparecchiature informatiche necessarie allo svolgimento delle attività di reparto. Ogni postazione di lavoro sarà utilizzata da più operatori in base ai turno che si troveranno a svolgere.. Non è consentito a nessun utente modificare le caratteristiche Hardware e Software impostate dall'azienda ed è vietato installare software non esplicitamente autorizzati e certificati dal servizio informativo. Non è consentita la riproduzione e duplicazione di programmi informatici ai sensi della normativa sulla tutela del Diritto d'Autore.
Il Servizio Informativo può procedere alla rimozione di file o applicazioni che ritiene pericolosi per la sicurezza del PC e della rete e può procedere con la formattazione del
pc e reinstallazione del sistema operativo.
In caso di allontanamento dal posto di lavoro è necessario procedere al log out dal sistema o dall'applicativo utilizzato. Tale disposizione è una garanzia sia per l'utilizzatore che per il sistema complessivo.

2.4 Gestione dell'autenticazione informatica

Gli operatori aziendali utilizzano varie procedure informatiche. Su ciascuna procedura è necessario richiedere a cura del responsabile del servizio le credenziali di accesso per gli operatori abilitati all'utilizzo. Ogni procedura utilizza specifiche regole per la composizione delle credenziali di autenticazione, tali regole vengono comunicate dal Servizio Informativo.
Le credenziali di accesso sono strettamente personali ed è buona regola non comunicare le proprie credenziali ad altri. La responsabilità delle attività effettuate su procedure è del proprietario delle credenziali.

2.5 **Accesso ed utilizzo internet**

Il servizio informativo ha comunicato ad ogni operatore dell'azienda le credenziali di accesso ad internet. All'interno del sito Web Aziendale è stata predisposta un area riservata ai dipendenti per la visualizzazione sia dei cedolini paga, cud, rapportini di presenza sia di tutte le eventuali comunicazioni che la direzione vuole trasmettere ai dipendenti. Per accedere a tale servizio gli utenti utilizzano le stesse password di accesso ad internet. La password per internet deve essere costituita da almeno 8 caratteri maiuscoli e minuscoli e da numeri o caratteri speciali.

Le risorse di rete e di memoria dei Computer sono limitate. Tutti gli utenti hanno pertanto la responsabilità di un uso oculato delle risorse di rete evitando di sprecare deliberatamente dette risorse o di monopolizzare l'uso a discapito di altri utenti ed in particolare devono astenersi da:

- Inviare messaggi di posta ad un gran numero di destinatari o partecipare a catene di S. Antonio;
- spendere un'eccessiva parte del proprio tempo navigando su Internet;
- caricare e scaricare file di grandi dimensioni
- generare un carico eccessivo sulle strutture elaborative per scopi personali.

L'accesso ai servizi di connettività internet può essere totalmente o parzialmente limitato dal SIA anche senza preavviso per garantire la sicurezza del sistema o della rete. E' fatto divieto a tutti gli utenti di utilizzare il collegamento internet per:

- trasmettere o scaricare ed installare materiale protetto da copyright
- scaricare o trasmettere materiale osceno, diffamatorio, intimidatorio sotto qualunque forma (immagini, testi, filmati, ecc.)
- scopi commerciali o di profitto personale e per attività illegali.

Gli utenti della rete aziendale devono comunque sapere che il personale che gestisce le reti di telecomunicazione può avere saltuariamente la necessità di analizzare i dati risultanti dai file di log delle connessioni internet. Tale personale è tenuto comunque al rispetto dei vincoli di riservatezza qualora si verificassero

E' proibito accedere ad internet dalle postazioni di lavoro dell'azienda utilizzando modem o altri mezzi di accesso diretto.
E' proibito fornire le proprie credenziali di accesso alle varie procedure aziendali.

2.6 Utilizzo della posta elettronica e posta elettronica certificata

L'amministrazione incoraggia l'uso della posta elettronica e della posta elettronica certificata per scambiare informazioni, migliorare le comunicazioni e per rendere più efficaci ed efficienti i processi di lavoro.

Ogni utente ha ricevuto le credenziali di accesso alla propria casella di posta con uno spazio dedicato alla gestione dei messaggi in entrata ed in uscita.

L’azienda attraverso il Servizio Informativo Aziendale sta progressivamente inserendo l’utilizzo della posta elettronica certificata a seguito di richiesta formale del singolo utente o del Dirigente dell’ufficio per la posta istituzionale del Servizio.

Il Servizio di posta elettronica erogato tramite fornitore esterno è di proprietà dell’azienda, pertanto ogni casella assegnata ai singoli operatori o uffici con il dominio: aosgmoscati.av.it ed il dominio cert.aosgmoscati.av.it per la certificata sono di proprietà dell’azienda.

L’amministrazione non può essere ritenuta responsabile:

1. dell’eventuale interruzione del servizio
2. dell’eventuale smarrimento di messaggi
3. di accesso non autorizzato o di alterazioni di trasmissioni o dati dell’utente

L’amministrazione non accede ai messaggi di posta elettronica dei singoli utenti senza l’autorizzazione dell’utente. L’accesso alla casella di posta senza autorizzazione è possibile solo nei seguenti casi:

1. richiesta scritta dell’autorità giudiziaria
2. situazioni critiche e di emergenza

E’ fatto divieto a tutti gli utenti di utilizzare il servizio di posta elettronica per inviare messaggi dannosi di tipo offensivo con contenuti oltraggiosi (sessuali, razziali, religiosi, politici, ecc.)che possano arrecare danno alla reputazione dell’amministrazione.
E’ vietato inoltre l’uso della posta elettronica aziendale per scopi commerciali e per attività illegali, è proibito fornire le proprie credenziali di accesso e/o rispondere a messaggi e-mail che facciano richiesta di questo tipo di informazioni.
E’ consentito l’utilizzo dell’account di posta elettronica fornito con il dominio: aosgmoscati.av.it e della casella certificata con il dominio: cert.aosgmoscati.av.it a fini privati e personali purchè tale utilizzo non sia causa diretta o indiretta di eventuali disservizi al sistema informatico aziendale.
Il servizio di posta elettronica e posta elettronica certificata viene affidato a fornitori altamente qualificati, va comunque ribadito che la sicurezza e riservatezza della posta elettronica non possono essere garantite in ogni circostanza in particolare per i messaggi scaricati sul PC. In questi casi è necessario che l’utente utilizzi tutte le buone regole di gestione della postazione di lavoro.
La casella di posta elettronica deve essere mantenuta in ordine cancellando documenti inutili e soprattutto allegati troppo grandi.

PARTE III - Sicurezza Sistemi Informativi e Server

3.1 Regole generali per i sistemisti

I server presenti in azienda ospitano le banche dati sottoelencate:

titolo	descrizione	formato	descrizione dell'applicativo	produttore dell'applicativo
SIGRU	sistema informativo gestione risorse umane	DBMS Oracle/firebird	Gestione dell' aspetto economico, giuridico e della pianta organica del personale aziendale	PUBLISYS
RILPRES	gestione rilevazione presenze	DBMS Oracle	Rilevazione presenze	PUBLISYS
CONTAB	base dati contabile	DBMS Oracle	Gestione della Contabilità e bilancio di azienda Sanitaria	GPI S.P.A.
MAGAZ	base dati dei magazzino	DBMS Oracle	Gestione dei magazzini, richieste ed ordini di azienda sanitaria	GPI S.P.A.
CESPITI	base dati dei cespiti	DBMS Oracle	Gestione dei cespiti aziendali	GPI S.P.A.
SOCCORSO PRONTO	base dati area sanitaria per la gestione dei dati relativi cartella clinica, cup-ticket	DBMS/MySql	Gestione integratadella cartella clinica, cup-ticket	MY Admin
SOCCORSO PRONTO ALPI	base dati per gestioni alpi allargata	DBMS/MySql	Gestione alpi allargata, prenotazione, refertazione, pagamento	MY Admin
ELIOT	base dati per la gestione del' attività del servizio immuno-trasfusionale	DBMS Oracle	Gestione integrata attività servizio immuno trasfusionale	ENGINEERING INGEGNERIA INFORMATICA
WINLABLAB	base dati per gestione laboratorio analisi	SQL Server M.S.	Gestione integrata laboratorio analisi	TESI S.P.A.
WINLABVIRO	base dati per gestione laboratorio virologia	SQL Server M.S.	gestione laboratorio di virologia	TESI S.P.A.
WINLABMICRO	base dati per gestione microbiologia	SQL Server M.S.	gestione laboratorio di microbiologia	TESI S.P.A.
WINLABWEB	base dati risultati esami	SQL Server M.S.	Servizio di richieste esami e consultazione referti dai vari reparti	TESI S.P.A.
ARMONIA	base dati per gestione anatomia patologica	DBMS Oracle	Gestione integrata attività servizio anatomia patologica	DEDALUS S.P.A.
PROT-FLOW	base dati protocollo informatico	POSTGRESS	Gestione protocollo informatico	MASTERS' TEAM

Nel rispetto del provvedimento del garante per la protezione dei dati personali del 27 novembre 2008 e s.m.i., l'azienda, ha individuato gli operatori (aziendali e delle aziende fornitrici di software) che esercitano la funzione di amministratore di sistema:

- dipendenti aziendali appartenenti al S.I.A. che assegnano le credenziali ai vari incaricati del trattamento per accedere ad internet, al portale aziendale, alla posta elettronica aziendale, alla posta certificata aziendale, alla procedura di gestione contabile e di magazzino;
- dipendenti aziendali appartenenti al S.E.F. che assegnano le credenziali ai vari incaricati identificati dai responsabili per accedere alla procedura di gestione contabile e di magazzino;
- dipendenti aziendali appartenenti al SIMT che assegnano le credenziali ai vari incaricati identificati dal responsabile per accedere alla procedura "Eliot";
- dipendenti delle ditte Wind, Aruba, Dedalus, Eng-Sanità, Publisys, Tesilab, My-Admin, GPI, Netway che gestiscono i server di propria competenza ed assegnano le credenziali ai vari utenti aziendali per le loro applicazioni;
- dipendenti della ditta H.S. che assicurano la manutenzione sui client della rete aziendale.

Tutti gli amministratori di sistema devono garantire l'efficiente fruibilità dei servizi offerti dai vari sistemi minimizzando il rischio di usi impropri come accessi non autorizzati ai sistemi e ai dati.

3.2 Sicurezza Fisica

I locali dove sono allocati i server sono:

- Sala server c/o SIA 1° piano stanza n°1 sede amministrativa
- Sala CED 1°piano sede sanitaria
- Sala server c/o Laboratorio Analisi p/terra sede sanitaria
- Sala server c/o Simt p/terra sede sanitaria
- Sala server c/o QVRS p/terra sede sanitaria

I locali che ospitano i server hanno caratteristiche indipendenti dalla piattaforma hardware e software utilizzata ed in particolare sono:

- Dedicati solo ai server e accessibili solo al personale autorizzato
- Dotati di un sistema di rilevazione di incendio
- Equipaggiati con dispositivi di stabilizzazione e continuità di tensione
- Climatizzati

Eventuali interventi di qualsiasi natura in tali locali devono sempre avvenire alla presenza di personale autorizzato.

3.3 Accessi

Tutti gli applicativi utilizzati rispettano le norme previste nell'allegato B del 196/2003 per quanto riguarda l'accesso tramite login e password con relativo profilo di utenti o gruppi di utenti che possono accedere alle risorse (database, applicazioni, transazioni, cartelle, file) con specifico profilo di autorizzazione (solo lettura, lettura ed aggiornamento, controllo completo).

I sistemi operativi presenti in azienda (windows7, windows8, windows2010 server, windows-2002-server, linux (red-hat, suse, Ubuntu,etc) e le relative applicazioni installate sono in grado di rispettare le seguenti regole:

- Identificazione utente in modo univoco;
- Assegnazione password in conformità alla normativa vigente con relativa conservazione in forma crittografata sconosciuta anche all'amministratore di sistema; la password avrà una durata di 6 mesi per l'accesso a banche dati con trattamenti riguardanti dati personali e 3 mesi per l'accesso a banche dati riguardanti dati sensibili; la password è composta da almeno 8 caratteri o, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito (allegato b del 196/2003 punto 5).
- Revoca utente su richiesta responsabile o non utilizzo dell'utente per un periodo superiore a 180 giorni
- Ripristino password in caso di perdita/dimenticanza della parola chiave da parte dell'utente, avviene solo su espressa richiesta dell'utente con intervento dell'amministratore di sistema che assegna una nuova password. L'utente al primo accesso con la nuova password è tenuto a modificarla
- L'inserimento e modifica dell'abilitazione utenti viene effettuata dall' amministratore di sistema solo dopo comunicazione del responsabile della U.O.
- Il responsabile del trattamento deve essere a conoscenza ed autorizzare tutti i previlegi che vengono assegnati al personale di assistenza
- Tutti i collaboratori esterni all' azienda (assistenza, consulenti, collaboratori, etc) devono avere un account con una scadenza regolata sul presunto periodo di attività presso l'azienda

3.4 Protezione da virus informatici

L' Azienda Wind che assicura la connessione ad Internet ha installato presso la nostra sede un apparato "Fortimanager" che gestisce centralmente l'antivirus aziendale "forticlient" installato sui singoli pc della rete aziendale; su ogni singolo P.C. oltre all'antivirus sono presenti ed attivati (se l'applicativo utilizzato lo consente) il firewall, webfilter, antispam. L'aggiornamento avviene in modo centrale sull'apparato che lo distribuisce ai vari pc in rete.

3.5 Custodia e Conservazione dei Supporti Utilizzati.

Si conferma quanto disposto nel documento programmatico di sicurezza delibera n. 194/2012:

- i supporti rimovibili (cd-rom, floppy-disk, dvd-rom, USB storage media) contenenti dati sensibili e giudiziari non devono essere lasciati incustoditi, ma devono essere custoditi e conservati dai singoli incaricati in modo da evitare che possano essere utilizzati da terzi non autorizzati.
- i fascicoli e documenti delle pratiche non devono essere lasciati in posizione visibile sulla propria scrivania e su altri ripiani di lavoro ma devono essere conservati negli schedari e prelevati solamente per il tempo necessario allo studio della pratica, per poi esservi riposti al termine del trattamento della stessa.

3.6 Back-Up dei Dati (Backup Cifrato)

Le procedure di backup sono automatizzate mediante compressione e cifratura dei dati inviati ai sistemi di storage dei singoli sistemi.

E' attiva (per alcune banche dati) una procedura unificata di salvataggio dei dati che quotidianamente effettua le copie di sicurezza su supporti magnetici o su server d'appoggio.

3.7 Manutenzione di Sistemi Operativi ed Applicazioni Software

Servizio di manutenzione software - generalità

Il servizio di manutenzione del sistema di elaborazione e comunicazione si articola su:

- manutenzione del software di base
- manutenzione del software d'ambiente
- manutenzione del software applicativo.

Manutenzione del software di base

Il servizio comprende:

- Aggiornamento dei programmi con installazione di moduli software correttivi (service pack, hot fix, ecc.);
- reinstallazione e personalizzazione del software a fronte di problemi tecnici accertati
- aggiornamento del sistema contro il rischio di vulnerabilità e di difetti dei programmi
- Gestione dell' antivirus aziendale

Manutenzione del software d'ambiente

Il servizio viene effettuato per eliminare i difetti che potrebbero riscontrarsi nell'utilizzo del software d'ambiente, costituito dal prodotto per la gestione delle basi di dati relazionale e per l'installazione di eventuali release successive. Tale attività, di norma è garantita, in massima parte, dalle aziende che hanno in gestione o in manutenzione l'applicativo.

Manutenzione del software applicativo

L'assistenza e la manutenzione del software applicativo viene effettuata dall'Impresa partner con proprio personale di elevata competenza tecnica e professionale, che provvede alla formazione del personale dell'Amministrazione.

1. Il servizio di manutenzione **ordinaria** dei Programmi Applicativi comprende:

a) La manutenzione ***correttiva*** che consiste nella rimozione di eventuali errori o malfunzionamenti da effettuarsi anche con intervento on site

b) La manutenzione ***adeguativa*** che riguarda adeguamenti derivanti da nuove disposizioni legislative, sempre che non comportino sostanziali modifiche alla logica dei programmi e/o alla struttura dei dati. Gli interventi che comportano sostanziali modifiche rientreranno nel servizio di manutenzione straordinaria.

2. Il servizio di manutenzione **straordinaria** dei Programmi Applicativi comprende:

a) La manutenzione ***migliorativa*** relativa al mantenimento dell'efficienza delle procedure e dei programmi al variare delle condizioni e dei carichi di lavoro.

b) La manutenzione ***innovativa*** per la creazione di nuovi elaborati, personalizzati o generalizzati utili al soddisfacimento di nuove esigenze dell'A.O.

4 . CRITERI E MODALITÀ DI RIPRISTINO DELLA DISPONIBILITÀ DEI DATI

Il piano di ripristino della disponibilità dei dati è finalizzato alla definizione delle idonee misure da adottare per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

Attualmente l'A.O. non ha ancora un piano organico di continuità di servizio disaster recovery; tuttavia i servers dell'Ente sono singolarmente dotati di unità di back-up (nastri, DVD-R, Nas ecc.), ed il back up è effettuato giornalmente; queste procedure, sicuramente utili, non sono tuttavia sufficienti a configurare il ripristino da disaster recovery di tutti i dati dell'A.O. Le operazioni possibili di recovery sono legate al ripristino dell'ultima copia di salvataggio.

Per quanto attiene alle copie di salvataggio, è necessario definire regole comuni per l'ubicazione e l'etichettatura delle copie. La definizione di politiche uniformi di salvataggio, conservazione dei supporti di backup e politiche di ripristino, deve essere studiata, realizzata e posta in essere nel più breve tempo possibile. A conclusione di questa attività potrà essere avviato un progetto di definizione di un piano di disaster recovery.

in particolare, vanno definiti:

- modalità di backup (automatico, manuale, frequenza, supporto, ecc.);
- l'ubicazione delle copie;
- eventuali convenzioni nella applicazione di etichette o contrassegni;
- la frequenza di rotazione dei supporti;
- i metodi per il trasporto dei salvataggi dal luogo di archiviazione verso l'esterno e le procedure di ritorno dei salvataggi in caso di situazione di disaster.

Nell'ipotesi di distruzione o danneggiamento dei dati o degli strumenti elettronici:

- deve essere avvertito l'incaricato che ha in custodia il supporto di back up nonché i CD ROM contenenti i vari software installati sugli strumenti elettronici;
- ci si deve rivolgere immediatamente al tecnico manutentore sollecitandone al più presto l'assistenza;
- ciascun incaricato deve provvedere ad inventariare nella maniera più precisa possibile il lavoro svolto dal momento dell'ultimo back up al momento della rottura irreversibile;
- si devono reinstallare i programmi danneggiati o distrutti, sempre che non sia necessario sostituire l'intero hardware, provvedere a reinstallare tutti i dati contenuti nel supporto di back up;
- si deve provvedere all'aggiornamento dei sistemi operativi una volta reinstallati;

Per prevenire eventi di perdita dei dati e di danneggiamento degli strumenti elettronici è prevista, almeno una volta all'anno, una manutenzione preventiva su tutti i PC aziendali, effettuata da tecnici incaricati.

Protezione dei dati personali e dei sistemi

Ciascuna Unità Operativa che tratta dati personali deve operare nel rispetto delle disposizioni contenute nel decreto legislativo n. 196/2003 "Codice in materia di protezione dei dati personali " e s.m.i. e del regolamento adottato dall'azienda con delibera n. 194 del 23/03/2012

Aggiornamento e Revisione

Il presente regolamento è soggetto a revisione annuale ed in tutti i casi in cui è necessario inserire integrazioni.