DOCUMENTO PROGRAMMATICO SULLA SICUREZZA NEL TRATTAMENTO DEI DATI A FINI PRIVACY ANNO 2012

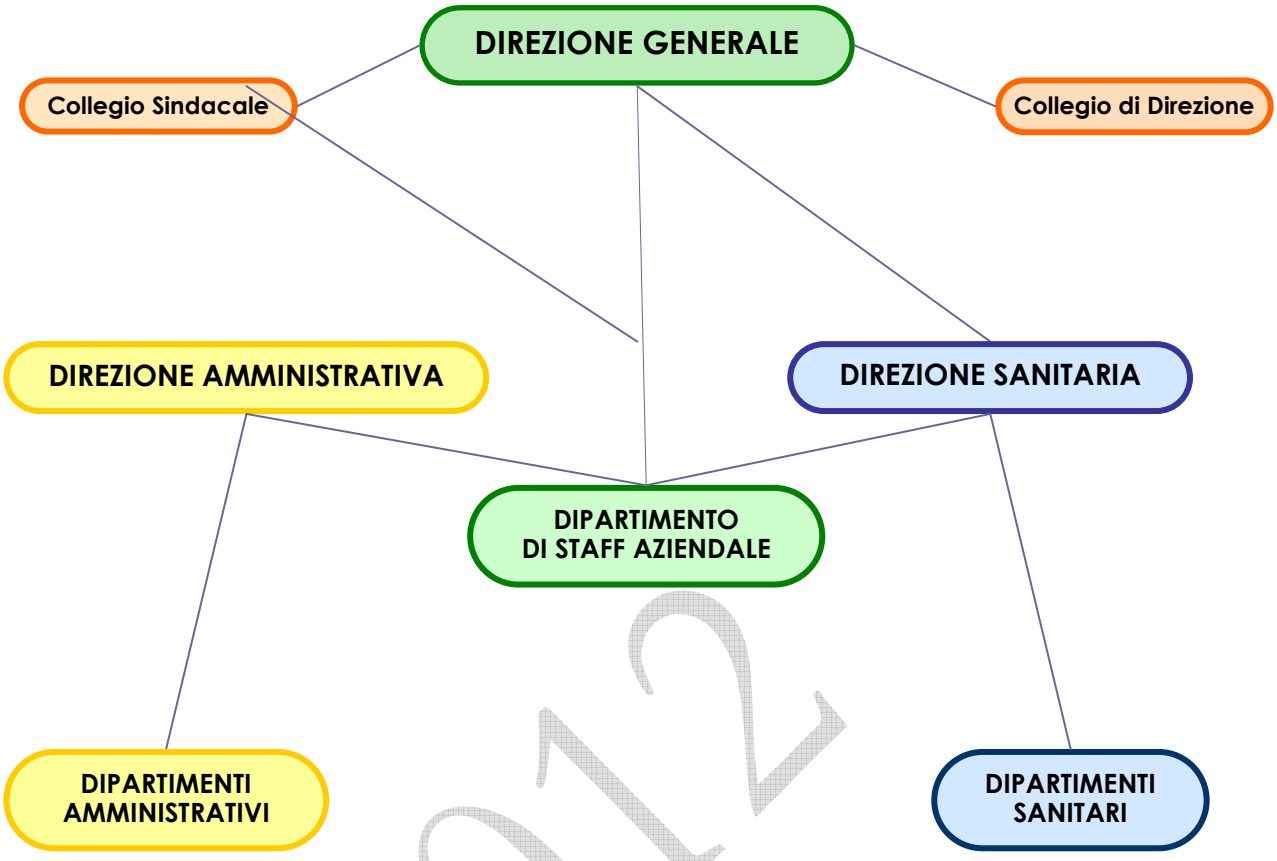
2012

SOMMARIO

2012

1. L'Azienda

L'Azienda Sanitaria Locale 2 Savonese si estende sull'intero territorio Provinciale abbracciando 69 Comuni con una popolazione di circa 285.000 abitanti . Il fabbisogno sanitario viene soddisfatto con le prestazioni offerte dalle quattro strutture ospedaliere (Ospedale San Paolo di Savona, San Giuseppe di Cairo Montenotte , Santa Corona di Pietra Ligure e Santa Maria di Misericordia di Albenga) dai servizi territoriali e dalla rete di emergenza provinciale. Il recente accorpamento con l'azienda ospedaliera " Ospedale Santa Corona di Pietra Ligure ha comportato una revisione organizzativa con la conseguente articolazione dei servizi in dipartimenti amministrativi e sanitari, Strutture Complesse, Strutture Semplici Dipatimentali e Strutture Semplici.



1.1 Organizzazione del Documento Programmatico sulla Sicurezza dei Dati

Il presente documento è redatto sulla base delle "Disposizioni inerenti l'adozione delle misure minime di sicurezza nel trattamento dei dati personali previste dagli articoli 33-36 e dall' allegato B del D.Lg. 196/2003".
Le disposizioni in parola stabiliscono la predisposizione e l'aggiornamento, con cadenza almeno annuale (entro il 31 marzo di ogni anno), di un Documento Programmatico sulla Sicurezza dei dati, per definire, sulla base dell'analisi dei rischi, della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati stessi, i seguenti elementi:

- l'elenco dei trattamenti di dati personali sensibili e giudiziari
- l'analisi dei rischi che incombono sui dati;
- le misure adottate per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- la previsione di interventi formativi degli incaricati del trattamento;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura ;
- i trattamenti soggetti a cifratura o a separazione per isolare dati dell'interessato ,sensibili o giudiziari, rispetto a quelli personali.

Il presente documento dà conto di tutte le misure adottate in relazione alla tipologia delle varie banche dati.

1.2 Metodologia per la redazione

Utilizzando la modulistica di cui alla "Guida operativa per redigere il D.P.S. " emanata l'undici giugno del 2004 dal Garante per la Protezione dei Dati Personali si è provveduto a censire i vari trattamenti dati in essere presso l' Azienda , le relative banche dati, le misure di sicurezza adottate o proposte, i criteri e le procedure per il salvataggio dei dati stessi nonché i tempi di ripristino.
La modulistica consente di ottenere, per ciascuna banca dati rilevata, informazioni circa:

Il responsabile del trattamento dati
il trattamento per il quale viene impiegata la banca dati;
la tipologia dei dati trattati;
i soggetti giuridici ai quali i dati si riferiscono;
le operazioni di trattamento eseguite sulla banca dati;
la natura dei dati;
le modalità di trattamento dei dati con varie tipologie di strumenti e mezzi;
l'eventuale intervento di titolari o contitolari o di terzi responsabili nel trattamento dati e nella gestione della relativa anca dati.
La rilevazione dei dati è stata effettuata muovendo dall'organizzazione aziendale prevista con deliberazioni 626 del 1.7.2008,831 del 4.9.2008 e 962 del 14.10.2010 coniugata con il Regolamento in materia di privacy adottato dall'azienda con provvedimento 931 del 15 ottobre 2009. Ai sensi di tale ultimo documento, costituiscono centri di responsabilità nel trattamento dei dati le singole S.S.D. e le Strutture Complesse facenti parte dei vari Dipartimenti in cui è funzionalmente articolata l'azienda.

1.3 Misure di tutela per la sicurezza delle banche dati cartacee

Le misure di sicurezza adottate dall'Azienda per la gestione delle banche dati cartacee sono di seguito elencate:

- custodia in uffici ed aree operative ;
- custodia in locali riservati e chiusi a chiave;
- custodia in contenitori dedicati chiusi a chiave;
- custodia in archivi di deposito chiusi a chiave ad accesso limitato ai soli responsabili ed incaricati
- custodia di documentazione storica o da conservarsi per esigenze di legge in locali di sicurezza ad accesso limitato ai soli responsabili ed incaricati.

1.4 Misure di tutela per la sicurezza delle banche dati informatiche

Attesa la complessità delle procedure informatiche e il loro crescente utilizzo, ai fini della tutela e della sicurezza, risultano di rilevante interesse le misure minime adottate dall'Azienda nel trattamento delle banche dati informatiche quali di seguito elencate:

- configurazioni atte a garantire la continuità di servizio (cluster, doppio alimentatore, doppia scheda di rete, ecc.);
- configurazioni delle memorie di massa con mirroring e raid;
- dispositivo di backup per ogni server o centralizzato di dimensione e velocità adeguate;
- procedure di backup eseguite su supporti in linea ad alta velocità e i dati trasferiti su supporti removibili;
- i supporti fisici contenenti i backup sono conservati in luogo sicuro e diverso da quello dove risiede il server corrispondente (per minimizzare la probabilità di distruzione contestuale di server e dati salvati) in armadi ignifughi chiusi a chiave;
- è adottato un set minimo di supporti per i salvataggi a rotazione (es. un supporto per ogni giorno della settimana) e viene effettuato un backup non sovrascrivibile almeno una volta al mese;
- il trattamento di dati personali con strumenti elettronici è consentito ai soli incaricati dotati di credenziali di autenticazione;
- user/password dei super-utenti conservati in luogo sicuro ad accesso controllato (chiuso a chiave)
- le credenziali di autenticazione sono costituite da un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure da un dispositivo di autenticazione in possesso e ad uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave;
- ad ogni incaricato possono essere assegnate una o più credenziali per l'autenticazione;
- gli incaricati ricevono istruzioni riguardanti le cautele necessarie ad assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi utilizzati dall'incaricato;
- la parola chiave è composta da almeno otto caratteri o, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; è modificata dall'incaricato al primo utilizzo e, successivamente, almeno ogni sei mesi; in caso di trattamento dati sensibili e giudiziari la parola chiave è modificata almeno ogni tre mesi.
- il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi;
- le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;
- le credenziali sono disattivate anche in caso di perdita delle mansione che giustificano l'accesso ai dati personali;

- sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento;
- quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente tramite password di autenticazione, sono impartite disposizioni scritte volte a specificare le modalità per assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato;
- le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non sono applicate ai trattamenti dei dati personali destinati alla diffusione.
- sistema di autorizzazioni idoneo a supportare gli incaricati che hanno profili di autorizzazione di ambito diverso;
- i profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento
- le gestioni locali dei dati informatici tendono ad essere sostituite da quelle centralizzate su server per quelle esistenti al tutela dei dati è demandata all'utente finale che ha il compito di effettuare salvataggi su supporti magnetici (con frequenza almeno settimanale) e di conservare gli stessi in luogo idoneo (sotto chiave, in contenitori ignifughi, .).
- server e workstation sono dotati di software antivirus ed antispam aggiornato a cadenza giornaliera
- il profilo abilitativo di ogni utente è configurato in modo da non consentire l' installazione di programmi non autorizzati .

1.5 Tutela fisica dei sistemi informatici

Le adeguate misure di tutela fisica dei server e degli apparati di rete prevedono un corretto inventario delle attrezzature ed una adeguata collocazione come di seguito elencato

- i server sono collocati in locali chiusi ad accesso controllato, con alimentazione elettrica tutelata, condizionamento ed impianto antincendio;
- gli apparati di rete sono collocati in armadi chiusi a chiave in modo da garantire valori corretti di alimentazione elettrica, temperatura, polverosità ed umidità.

Per salvaguardare l'impianto di sicurezza del sistema sono state adottate le seguenti misure:

- configurazione ottimale del firewall e del ras che sono configurati e gestiti da personale certificato;
- configurazione ottimale dei server dedicati all'autenticazione dell'utente (server di dominio, …) e dei sistemi dedicati al backup dei dati, minimizzando il numero di funzionalità in uso su di essi;
- sessioni di amministrazione di sistema e di concessione/revoca/modifica di abilitazioni applicative non effettuate in locale sul server rese completamente immuni da azioni di intercettazione sulla rete e da fraudolenta impersonificazione;
- password di amministrazione con lunghezza minima di 8 caratteri, maiuscoli ,minuscoli e segni di punteggiatura con scadenza massima imposta pari ad un mese senza possibilità di ripetizione.

Per salvaguardare le funzionalità applicative del sistema sono state adottate le seguenti misure:

- per la sicurezza della autenticazioni né la password né le informazioni che possano essere utilizzate per una fraudolenta impersonificazione viaggiano in chiaro sulla rete ;
- non viaggia in chiaro sulla rete neppure la configurazione dei server che forniscono funzionalità applicative .

Le misure sopra descritte tendono a minimizzare le indisponibilità del servizio,intercettazione e modifica di dati in rete e la fraudolenta impersonificazione.

1.6 Amministratori di sistema aziendali e norme regolamentari

In relazione al provvedimento adottato dal Garante per la protezione dei dati personali il 27 novembre 2008 l'Azienda, e per essa la S.C. Infrastrutture Informatiche e Telecomunicazione, ha provveduto ad individuare una serie di figure che possono concettualmente qualificarsi 'Amministratori di Sistema' quali di seguito rubricate e disciplinate in ragione dell'attività e dei compiti attribuiti a ciascuno.

a) Sistemisti di piattaforma UNIX/Linux

Gli Amministratori di Sistema qualificabili come 'amministratore di piattaforma UNIX' sono autorizzati ad operare su tutti i sistemi di tale piattaforma e sono tenuti a svolgere le seguenti attività:

- sorvegliare il corretto funzionamento dei sistemi in senso generale (monitoraggio) e dei sottosistemi specifici in particolare (CPU, memorie, sistemi dischi, storage, schede di rete, sistema di alimentazione e di ventilazione, etc.);
- sorvegliare il corretto funzionamento dei sistemi applicativi a bordo della piattaforma tramite il monitoraggio di log e messaggi prodotti dal sistema operativo e dal software di base;
- intervenire in caso di malfunzionamento, guasto o anomalia funzionale sui sistemi, sul software applicativo a bordo dei medesimi, sui servizi erogati tramite la piattaforma, per diagnosticare il problema e ripristinare il corretto funzionamento;
- intervenire periodicamente per verificare e, compatibilmente con i vincoli introdotti dai sistemi applicativi ospiti, aggiornare il sistema operativo, i driver di periferiche, ed ogni componente del software di base per garantire l'allineamento della piattaforma con le versioni emesse dal produttore / costruttore;
- provvedere alla configurazione ottimale del sistema per garantire il migliore equilibrio fra le prestazioni erogate, la sicurezza operativa, la complessità/onerosità di gestione e mantenimento nel tempo delle funzioni;
- verificare quotidianamente il buon esito dei salvataggi dei dati giornalieri (backup) gestiti dallo specifico sistema, definire e garantire il salvataggio periodico delle configurazioni della piattaforma in particolar modo quando vi siano state modifiche;
- intervenire prontamente in situazioni di emergenza o, in caso di manutenzione ordinaria /straordinaria, segnalare i bisogni dell'organizzazione ai fornitori esterni deputati all'assistenza tecnica, coordinare e seguire i relativi interventi, informare utenti e strutture tecniche coinvolte;
- segnalare eventuali problemi inerenti i sistemi o disfunzioni ai dirigenti del SI;
- definire e configurare gli utenti, gli account che devono operare sul sistema ed i relativi parametri, attribuendo loro il profilo di autorizzazione indicato dal Responsabile del Trattamento cui il sistema è di supporto;
- cooperare all'installazione dei sistemi, monitorare la loro continuità operativa, la fruibilità continuativa dei servizi da parte degli utenti;
- verificare la funzionalità delle interfacce, attivare e/o disattivare i singoli processi software al fine di garantire la continuità di servizio in relazione agli specifici contesti operativi;
- attuare operazioni sui file dei file system e sui file system stessi (installazione, add, move, change, copy, ecc.) esclusivamente per la manutenzione del sistema, l'indagine diagnostica, l'installazione di applicazioni o di tool diagnostici o gestionali, il tuning, il salvataggio, anche temporaneo, di dati e configurazioni, il ripristino delle normali condizioni di funzionamento.

b) Sistemisti piattaforma Windows/VmWare

Gli Amministratori di Sistema qualificabili come amministratori di piattaforma Windows/VmWare sono autorizzati ad operare su tutti i sistemi di tale piattaforma Windows/VmWare e sono tenuti a svolgere le seguenti attività:

- sorvegliare in generale il corretto funzionamento dei sistemi (monitoraggio) ed, in particolare, quello dei sottosistemi specifici (CPU, memorie, sistemi dischi, storage, schede di rete, sistema di alimentazione e di ventilazione, ecc.);
- sorvegliare il corretto funzionamento dei sistemi applicativi a bordo della piattaforma tramite il monitoraggio di log e messaggi prodotti dal sistema operativo e dal software di base;
- intervenire in caso di malfunzionamento, guasto o anomalia funzionale sui sistemi, sul software applicativo a bordo dei medesimi, sui servizi erogati tramite la piattaforma, per diagnosticare il problema e ripristinare il corretto funzionamento;
- intervenire periodicamente per verificare e, compatibilmente con i vincoli introdotti dai sistemi applicativi ospiti, aggiornare il sistema operativo, i driver di periferiche, ed ogni componente del software di base per garantire l'allineamento della piattaforma con le versioni emesse dal produttore / costruttore;
- provvedere alla configurazione ottimale del sistema per garantire il migliore equilibrio fra le prestazioni erogate, la sicurezza operativa, la complessità/onerosità di gestione e mantenimento nel tempo delle funzioni;
- verificare quotidianamente il buon esito dei salvataggi dei dati giornalieri (backup) gestiti dallo specifico sistema, definire e garantire il salvataggio periodico delle configurazioni della piattaforma in particolar modo quando vi siano state modifiche;
- intervenire prontamente in situazioni di emergenza o, in caso di manutenzione ordinaria /straordinaria segnalare i bisogni dell'organizzazione ai fornitori esterni deputati dell'assistenza tecnica, coordinare e seguire i relativi interventi, informare utenti e strutture tecniche coinvolte;
- segnalare eventuali problemi dei sistemi o situazioni anomale ai dirigenti del SI;

- definire e configurare gli utenti, gli account che devono operare sul sistema ed i parametri relativi, attribuendo loro il profilo di autorizzazione indicato dal Responsabile del Trattamento cui il sistema è di supporto;
- cooperare all'installazione dei sistemi, monitorare la loro continuità operativa e la fruibilità continuativa dei servizi da parte degli utenti,
- verificare la funzionalità delle interfacce, attivare e/o disattivare i singoli processi software per garantire la continuità di servizio in relazione agli specifici contesti operativi;
- attuare operazioni sui file dei file system e sui file system stessi (installazione, add, move, change, copy, ecc.) per soli scopi di manutenzione del sistema, indagine diagnostica, installazione di applicazioni o di tool diagnostici o gestionali, tuning, salvataggio, anche temporaneo, di dati e configurazioni, ripristino di condizioni normali di funzionamento.

c) Sistemisti amministratori di rete

Gli Amministratori di Sistema qualificabili quali amministratori di rete sono autorizzati ad operare su tutti i sistemi di rete compresi i sistemi di servizio (Radius, DHCP, DNS, VPN Server, WCS, ecc.) e sono tenuti a svolgere le seguenti attività:

- sorvegliare in senso generale il corretto funzionamento dei sistemi (monitoraggio) ed in particolare quello dei sottosistemi specifici (CPU, memorie, sistemi dischi, storage, schede di rete, sistema di alimentazione e di ventilazione, ecc.);
- sorvegliare il corretto funzionamento dei servizi applicativi erogati attraverso i sistemi di rete tramite il monitoraggio di log e messaggi prodotti dal sistema operativo e dal software di base;
- intervenire in caso di malfunzionamento, guasto o anomalia funzionale sui sistemi, sul software di servizio a bordo dei medesimi, sui servizi erogati tramite l'infrastruttura di rete, per diagnosticare il problema e ripristinare il corretto funzionamento;
- intervenire periodicamente per verificare e, compatibilmente con i vincoli introdotti dallo hardware di sistema e dalle licenze disponibili, aggiornare il sistema operativo, i driver di periferiche, incluso ogni componente del software di base per garantire l'allineamento della piattaforma con le versioni emesse dal produttore / costruttore;
- provvedere alla configurazione ottimale del sistema per garantire il migliore equilibrio fra le prestazioni erogate, la sicurezza operativa, la complessità/onerosità di gestione e mantenimento nel tempo delle funzioni;
- verificare quotidianamente il buon esito dei salvataggi dei dati giornalieri (backup) gestiti dallo specifico sistema, definire e garantire il salvataggio periodico delle configurazioni della piattaforma in particolar modo quando siano state operate modifiche;
- intervenire prontamente in situazioni di emergenza o, in caso di manutenzione ordinaria o straordinaria, segnalare i bisogni dell'organizzazione ai fornitori esterni deputati all'assistenza tecnica, coordinare e seguire i relativi interventi, informare utenti e strutture tecniche coinvolte;
- segnalare eventuali problemi dei sistemi o situazioni anomale ai dirigenti del SI;
- definire e configurare gli utenti, gli account che devono operare sul sistema ed i parametri relativi, attribuendo loro il profilo di autorizzazione indicato dal Responsabile del Trattamento cui il sistema è di supporto;
- cooperare all'installazione dei sistemi, monitorare la loro continuità operativa e la fruibilità continuativa dei servizi da parte degli utenti;
- verificare la funzionalità delle interfacce, attivare e/o disattivare i singoli processi software per garantire la continuità di servizio in relazione agli specifici contesti operativi;
- attuare operazioni sui file dei file system e sui file system stessi (installazione, add, move, change, copy, ecc.) esclusivamente per la manutenzione del sistema, l'indagine diagnostica, l'installazione di applicazioni, di tool diagnostici o gestionali, il tuning, il salvataggio, anche temporaneo, di dati e configurazioni ed il ripristino di condizioni normali di funzionamento.

d) Amministratori di database Oracle – DBA Oracle

Gli Amministratori di Sistema qualificabili come amministratori di databases sono autorizzati ad operare su tutti i sistemi database Oracle e sono tenuti a svolgere le seguenti attività:

- sorvegliare il corretto funzionamento dei sistemi RDBMS, delle varie istanze e delle utenze relative;
- sorvegliare il corretto funzionamento dei sistemi applicativi afferenti alla base di dati tramite il monitoraggio di log e messaggi prodotti dal sistema database;
- intervenire in caso di malfunzionamento, guasto o anomalia funzionale, sui sistemi database, sul software applicativo che vi afferisce, sui servizi che li usano, per diagnosticare il problema e ripristinare il corretto funzionamento del sistema RDBMS;

- intervenire periodicamente per verificare e, compatibilmente con i vincoli introdotti dai sistemi applicativi ospiti, aggiornare il sistema database ed ogni suo componente per garantire l'allineamento del sistema con le versioni emesse dal produttore / costruttore;
- provvedere alla configurazione ottimale del sistema per garantire il migliore equilibrio fra le prestazioni erogate, la sicurezza operativa, la complessità/onerosità di gestione e il mantenimento nel tempo delle funzioni;
- verificare quotidianamente il buon esito dei salvataggi dei dati giornalieri (backup) gestiti dallo specifico sistema, definire e garantire il salvataggio periodico delle configurazioni della piattaforma in particolar modo quando siano state operate modifiche;
- intervenire prontamente in situazioni di emergenza o, in caso di manutenzione ordinaria/straordinaria segnalare i bisogni dell'organizzazione ai fornitori esterni dell'assistenza tecnica, coordinare e seguire i relativi interventi, informare utenti e strutture tecniche coinvolte;
- segnalare eventuali problematiche dei sistemi o situazioni anomale ai dirigenti del SI;
- definire e configurare gli utenti, gli account che devono operare sul sistema ed i parametri relativi, attribuendo loro un profilo coerente con il profilo di autorizzazione indicato dal Responsabile del Trattamento per il trattamento relativo;
- cooperare all'installazione dei sistemi, monitorare la loro continuità operativa e la fruibilità continuativa dei servizi da parte degli utenti,
- verificare la funzionalità delle interfacce, attivare e/o disattivare i singoli processi software per garantire la continuità di servizio in relazione agli specifici contesti operativi;
- attuare operazioni sulle strutture interne del RDBMS (installazione, add, move, change, copy, ecc.) esclusivamente per la manutenzione del sistema, l'indagine diagnostica, l'installazione di tablespace o di tool diagnostici o gestionali, il tuning, ilsalvataggio, anche temporaneo, di dati e configurazioni, ed il ripristino delle normali condizioni di funzionamento.

e) Sistemisti Amministratori di RDBMS

Gli Amministratori di Sistema qualificabili come sistemisti amministratore di RDBMS sono autorizzati ad operare sui sistemi RDBMS non standard per APSS (diversi da Oracle) come ad esempio (MS SQL Server, MySQL, ecc) utilizzati per trattare i dati aziendali e sono tenuti a svolgere le seguenti attività:

- sorvegliare il corretto funzionamento dei sistemi RDBMS, delle varie istanze e delle relative utenze;
- sorvegliare il corretto funzionamento dei sistemi applicativi afferenti alla base di dati tramite il monitoraggio di log e messaggi prodotti dal sistema database;
- intervenire in caso di malfunzionamento, guasto o anomalia funzionale, sui sistemi database, sul software applicativo che vi afferisce, sui servizi che li usano, per diagnosticare il problema e ripristinare il corretto funzionamento del sistema RDBMS;
- intervenire periodicamente per verificare e, compatibilmente con i vincoli introdotti dai sistemi applicativi ospiti, aggiornare il sistema database ed ogni suo componente per garantire l'allineamento del sistema con le versioni emesse dal produttore / costruttore;
- provvedere alla configurazione ottimale del sistema per garantire il migliore equilibrio fra le prestazioni erogate, la sicurezza operativa, la complessità/onerosità di gestione e il mantenimento nel tempo delle funzioni;
- verificare quotidianamente il buon esito dei salvataggi dei dati giornalieri (backup) gestiti dallo specifico sistema, definire e garantire il salvataggio periodico delle configurazioni del RDBMS, in particolar modo quando siano state eperate modifiche;
- intervenire prontamente in situazioni di emergenza o, in caso di manutenzione ordinaria/ straordinaria, segnalare i bisogni dell'organizzazione ai fornitori esterni deputati all'assistenza tecnica, coordinare e seguire i relativi interventi, informare utenti e strutture tecniche coinvolte;
- segnalare eventuali problemi ai sistemi o situazioni anomale ai dirigenti del SI;
- definire e configurare gli utenti, gli account che devono operare sul sistema ed i parametri relativi, attribuendo loro un profilo coerente con il profilo di autorizzazione indicato dal Responsabile del Trattamento per il relativo trattamento;
- cooperare all'installazione dei sistemi, monitorare la loro continuità operativa e la fruibilità continuativa dei servizi da parte degli utenti;
- verificare la funzionalità delle interfacce, attivare e/o disattivare i singoli processi software per garantire la continuità di servizio in relazione agli specifici contesti operativi;
- attuare operazioni sulle strutture interne del RDBMS (installazione, add, move, change, copy, ecc.) esclusivamente per la manutenzione del sistema, l'indagine diagnostica, l'installazione di tablespace, di tool diagnostici o gestionali, il tuning, il salvataggio, anche temporaneo, di dati e configurazioni ed il ripristino delle normali condizioni di funzionamento.

f) Amministratori di sistema in pronta disponibilità

Gli Amministratori di Sistema qualificabili come amministratori di sistema in condizioni di personale in pronta disponibilità sono autorizzati ad operare su tutti i sistemi server di qualsiasi piattaforma, su tutti i sistemi databases e su tutti i sistemi di rete, limitatamente alle operazioni svolte per diagnosticare i problemi segnalati e per correggere i malfunzionamenti e/o ripristinare il servizio anche in modo parziale. Per gli eventi relativi ai sistemi critici devono essere seguite le procedure, le istruzioni e le indicazioni riportate nella documentazione ufficiale prodotta dagli "owners" e disponibile a tutti sulla procedura 'Documenti lavoro del SSI'. Gli amministratori di sistema in pronta disponibilità sono tenuti a svolgere le seguenti attività:

- intervenire prontamente qualra venga evidenziato un malfunzionamento, un guasto o una anomalia funzionale sui sistemi, sul software applicativo che vi afferisce, sui servizi che li usano, al fine di verificarne l'origine, di diagnosticare il problema e, se possibile, ripristinare il corretto funzionamento del sistema;
- provvedere alla tracciatura delle operazioni effettuate e alla documentazione di quanto eseguito in condizioni in pronta disponibilità per rendicontare gli amministratori di sistema, di piattaforma, di rete o di database l'intervento e consentire loro di rendere definitive/strutturali le eventuali modifiche introdotte;
- eseguire, sotto la supervisione di altri amministratori di sistema competenti in materia, eventualmente in connessione telefonica o telematica, le operazioni sui sistemi suggerite da questi ultimi;
- intervenire prontamente in situazioni di emergenza o, in caso di manutenzione ordinaria o straordinaria,
- segnalare i bisogni dell'organizzazione ai fornitori esterni, deputati all'assistenza tecnica, coordinare e seguire i relativi interventi ed informare utenti e strutture tecniche coinvolte;
- segnalare eventuali problematiche dei sistemi o situazioni anomale ai dirigenti del SI;
- attuare operazioni di monitoraggio dei singoli sistemi di cui si sospetta il malfunzionamento e, qualora sia diagnosticato un problema connesso direttamente al sistema, provvedere al fermo ed al riavvio, verificando l'esito del restart.

g) Amministratori di sistema Referenti Applicativi

Gli Amministratori di Sistema qualificabili come Referente Applicativo sono autorizzati ad operare sui sistemi utilizzati dal trattamento di cui sono referenti applicativi e tenuti a svolgere le seguenti attività:

- sorvegliare in generale il corretto funzionamento dei sistemi che sono utilizzati dal trattamento/applicazione ed, in particolare, dei sottosistemi specifici (CPU, memorie, sistemi dischi, storage, schede di rete, sistema di alimentazione e di ventilazione, ecc.);
- sorvegliare il corretto funzionamento del sistema applicativo principale e di quelli ad esso interconnessi tramite il monitoraggio di log e messaggi prodotti dal sistema applicativo e dal software di base su cui è montato;
- intervenire in caso di malfunzionamento, guasto o anomalia funzionale sui sistemi, sul software applicativo a bordo dei medesimi, sui servizi erogati tramite la piattaforma, per diagnosticare il problema e ripristinare il corretto funzionamento del trattamento. Qualora il referente applicativo non disponesse delle necessarie competenze sui sottosistemi tecnologici è tenuto a segnalare il problema agli amministratori di sistema, di database, di piattaforma o di rete competenti;
- intervenire periodicamente per verificare la compatibilità del trattamento/applicazione con gli aggiornamenti del sistema operativo, dei driver di periferiche e di ogni componente del software di base per garantire l'allineamento della piattaforma con le versioni dei sistemi operativi e dei software di base emesse dai produttore / costruttori;
- provvedere alla configurazione ottimale del sistema, compatibilmente con le indicazioni del fornitore, per garantire il migliore equilibrio fra le prestazioni erogate, la sicurezza operativa, la complessità/onerosità di gestione e mantenimento nel tempo delle funzioni;
- verificare quotidianamente il buon esito dei salvataggi dei dati giornalieri (backup), gestiti dallo specifico sistema, definire e garantire il salvataggio periodico delle configurazioni del trattamento/ applicazione in particolar modo quando siano state apportate modifiche;
- intervenire prontamente in situazioni di emergenza o, in caso di manutenzione ordinaria / straordinaria
- segnalare i bisogni dell'organizzazione ai fornitori esterni deputati all'assistenza tecnica, coordinare e seguire i relativi interventi ed informare utenti e strutture tecniche coinvolte;
- segnalare eventuali problemi dei sistemi o situazioni anomale ai dirigenti del SI;
- definire e configurare gli utenti (o richiederne la configurazione se il servizio è gestito in outsourcing), gli account che devono operare sul sistema ed i parametri relativi, attribuendo loro il profilo di autorizzazione indicato dal Responsabile del Trattamento cui il sistema è di supporto;

- cooperare all'installazione dei sistemi, monitorare la loro continuità operativa e la fruibilità continuativa dei servizi da parte degli utenti,
- verificare la funzionalità delle interfacce, attivare e/o disattivare i singoli processi software per garantire la continuità di servizio in relazione agli specifici contesti operativi;
- attuare operazioni sui dati (accesso, installazione di file o file systems, add, move, change, copy, ecc.) esclusivamente per la manutenzione del sistema, l'indagine diagnostica, l'installazione di moduli applicativi, di tool diagnostici o gestionali, il tuning, il salvataggio, anche temporaneo, di dati e configurazioni ed il ripristino delle normali condizioni di funzionamento.

1.7 Amministratori di sistema

Considerate le disposizioni del Garante in materia, l'Azienda ha provveduto, entro il 31.12.2009, a censire gli Amministratori di Sistema, interni ed esterni. Questa sezione dà conto di tale rilevazione e si articola, pertanto, in due tabulati: il primo dedicato agli amministratori di sistema, appartenenti a società esterne incaricate della manutenzione di software o hardware, rubricati in ragione di società e procedura informatica mentre il secondo riporta gli amministratori di sistema individuati tra gli operatori interni in ragione delle mansioni svolte. I dati sono stati aggiornati con la collaborazione della S.C. Sistemi Informativi

1) amministratori di sistema appartenenti a società esterne

Società	Procedura	Amministratore di sistema
Engineering SpA	OliAmm	Ugolini Giordano
	Manutenzione Sistemi	
	PerseWeb	Ugolini Giordano e Leite Massimiliano
Noemalife SpA	DnLab Manutenzione/Gestione	Visani Alessandro, Boarini Claudio
	DnWeb Manutenzione/Gestione	Maraldi Valentina, Apparuti Paolo
	WindoPath Manutenzione/Gestione	Cattaneo Riccardo, Tullo Umberto
Dedalus SpA	Ingenius D.I.S.P. , Praecordiis, OrmaWin, OrmaWeb	Serena Ruiba, Perrone Luigi
Ciditech SRL	MFP Sert	Bertero Corrado
Infogest SRL	Archivio/Protocollo	Rosciano, Caviglia
S.T.S.SRL	Delibere	Davide Bruzzone
Mondoedp SRL	Iris Win	Pilat Alberto
C2S SRL	Optiplan, Db	Alberti Gianni
Cespa SRL	Cespapel, Pulsar7, TFR	Pisano Mario
El.co. SRL	RIS PACS Polaris, SIO Manutenzione Software e Unysis	Bagnasco Manuela
General Computer SpA x Telecom SpA	Manutenzione Hardware	Raimondi Paolo, Vasconi Andrea, Franchin Gianluca, Bellani Stefano, Cozzi Marco, Vigorito Antonio, Ferrari Davide
Datasiel	Sistema informativo ospedaliero e Pronto soccorso	Andrea Maineri
Giada Progetti	Sigeco e Formazione	Laura Gasparini
Proveco	MAP Gestione Autoparco	Dario Cazzaniga
Insiel Mercato	Emonet gestione da remoto	Pascale Maria, Carla Perusin,Barbara Bulfon,Antonio Tognon
Millenium	Millewin	Silvia Tronci

2) amministratori di sistema individuati tra gli operatori interni

Piattaforma	Dipendente
Unix Linus	Tomasini Michele, Galati Antonio, Lanfranco Stefano
Window/VmWare	Tomasini Michele, Galati Antonio, Lanfranco Stefano, De Rosa Rosellina, Pescio Giorgio.
Sistemi di rete e Radius, Dhcp, Dns, Vpn Server, Wcs	Tomasini Michele, Pescio Giorgio, Fogliacco Guido
Oracle , Dba Oracle	Tomasini Michele, Galati Antonio, Lanfranco Stefano
Sistemi RDBMS	Tomasini Michele, Galati Antonio, Aresco Simona, Pescio Giorgio, Fogliacco Guido
Pronta Disponibilità	Cotta Sergio, Mantero Giuliano
Referenti Applicativi	Romita Marco, Ferro Daniela, Mercuri Ileana, Peirone Elia, Altieri Salvatore, Di Toma Cecilia,

1.8 Iniziative e azioni aziendali

L'Azienda nel perseguire l'obiettivo di tutela del diritto alla privacy, nel 2009, ha rivisto funditus dell'intera materia. Attraverso la Struttura Gestione Privacy si è provveduto a rivedere il relativo regolamento aziendale approvato con Provvedimento n. 931 del 15 ottobre 2009. Sono stati definiti i diversi livelli di responsabilità degli operatori coinvolti nell'applicazione delle disposizioni sulla privacy ed è stata distribuita la nuova modulistica unificata. Nel 2010 si è provveduto ad aggiornare gli amministratori di sistema afferenti a società esterne cui è affidata la manutenzione/gestione di software/sistemi ed a confermare quelli interni già censiti 31.12.2009 ed a mantenere le elaborate norme regolamentari per la corretta esecuzione dell'attività già in parola.
Anche per il 2010 il percorso informativo/formativo volto alla creazione di una cultura della riservatezza e del rispetto dell'utente avviato già da diversi anni. Si sono svolte infatti tre edizioni del corso "trattamento dati sensibili e supersensibili" mirato agli operatori sanitari ed amministrativi appartenenti al dipartimento di salute mentale e dipendenze, alle SS.CC. Assistenza Anziani e Disabili del Dipartimento Cure Primarie ed Attività Distrettuali, alle SS.CC. Neurologia di Savona e Pietra Ligure del Dipartimento di Medicina, alle SS.CC. Assistenza Consultoriale, Ostetricia e Ginecologia di Savona e Pietra Ligure del Dipartimento Materno Infantile, con responsabilità o incarico nel trattamento dei dati. Per l'anno 2011 è stato proposto, senza esito , un corso dal taglio operativo organizzato in pù sessioni volto ad integrare le regole in materia di privacy, con quelle informatiche ed organizzative. Resta costante, in materia, l'utilizzo del sito aziendale, periodicamente aggiornato e l' implementazione del sistema privacy con l' indiduazione graduale dei responsabili esterni. Nell'ottica dell'evoluzione della Privacy da adempimento formale a policy, si è provveduto al suo coordinamento con il sistema qualità ed i percorsi di accreditamento e ad approntare un progetto per l'informatizzazione del percorso volto ad acquisire il consenso al trattamento dati personali e sensibili una tantum, anche attraverso, la creazione della relativa banca dati consultabile da tutte le strutture aziendali.Progetto che tuttavia non ha trovato ancora concretezza .