ESTRATTO DELLA SEDUTA DEL 05/03/2009

DELIBERAZIONE del CONSIGLIO DI AMMINISTRAZIONE

n. 7 del 05/03/2009

Oggetto: **Decreto legislativo 30 giugno 2003, n. 196 (*Codice in materia di protezione dei dati personali*) e ss.mm. – Documento programmatico sulla sicurezza – Aggiornamento 2009.**

Presenti i consiglieri:
Giovanni Barbagli (Presidente), Allasia Gioachino, Biancalani Luigi, Biggeri Annibale, Cima Antonio Ettore, Palumbo Pasquale,

Assenti giustificati i consiglieri:
Naldoni Simone, Persiani Niccolò, Zubbani Angelo Andrea

E' presente:
- il Direttore dell'ARS: Dott.ssa Laura Tramonti

Dirigente Responsabile: Direttore

Estensore: Sara Salti

Pubblicazione su B.U.R.T.: Atto non soggetto a pubblicazione

ALLEGATI n.: 1

Strutture interessate:
DIREZIONE
OSSERVATORIO DI EPIDEMIOLOGIA
OSSERVATORIO PER LA QUALITA' E L'EQUITA'
SETTORE: TUTTI

Parere favorevole in ordine alla regolarità tecnico-amministrativa
Il Direttore (Dott.ssa Laura Tramonti)

IL CONSIGLIO DI AMMINISTRAZIONE

Vista la legge regionale 24 febbraio 2005, n. 40 (Disciplina del servizio sanitario regionale) e successive modifiche ed integrazioni;

Visto il Regolamento generale di organizzazione dell'ARS, approvato dalla Giunta regionale con deliberazione n. 29 del 21.01.2008;

Visto il decreto legislativo 30 giugno 2003 (Codice in materia di protezione di dati personali) e successive modificazioni ed integrazioni, di seguito denominato "Codice";

Richiamato, in particolare, il combinato disposto degli articoli da 33 a 36 del citato "Codice" con il quale, nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti a adottare le misure minime individuate dal "Codice" medesimo, volte ad assicurare un livello minimo di protezione dei dati personali, mediante la predisposizione di un documento programmatico della sicurezza, di seguito denominato DPS;

Valutato che il DPS deve essere aggiornato entro il 31 marzo di ogni anno in relazione all'evoluzione tecnica e all'esperienza maturata nel settore, secondo le decisioni adottate con Decreto del Ministro di grazia e giustizia assunte di concerto con il Ministro per le innovazioni e le tecnologie;

Richiamata la propria deliberazione n. 18 del 28/06/2004 e successive modificazioni ed integrazioni, con la quale si è proceduto alla nomina dei responsabili del trattamento e, specificatamente l'allegato 1, paragrafo 6, della medesima, che detta istruzioni in merito all'adozione delle misure minime di sicurezza;

Richiamati altresì i seguenti atti:

a) determina del direttore n. 12 del 10/03/2008 con la quale si è provveduto alla nomina degli incaricati dei trattamenti di dati personali di competenza della Direzione;
b) determina del coordinatore dell'osservatorio di epidemiologia n. 4 del 15/01/2008 con la quale si è provveduto alla nomina degli incaricati dei trattamenti di dati personali di competenza dell'osservatorio di epidemiologia;
c) determina del coordinatore dell'osservatorio per la qualità e l'equità n. 1 del 15/01/2008 con la quale si è provveduto alla nomina degli incaricati dei trattamenti di dati personali di competenza dell'osservatorio per la qualità e l'equità;

Richiamate le proprie deliberazioni:

a) n. 35 del 27/12/2004 con la quale si è provveduto, in ottemperanza alle disposizioni del "Codice" sopra richiamate, ad approvare il documento programmatico sulla sicurezza contenuto nell'Allegato sub. lett. A, parte integrante e sostanziale della citata deliberazione, stabilendo in conformità alla disciplina recata dall'allegato B, punto 19, del "Codice", il suo aggiornamento, anche in relazione all'evoluzione tecnica e all'esperienza maturata nel settore;
b) n. 7 del 03.04.2006, con cui si è proceduto ad approvare le integrazioni e modificazioni al DPS che costituiscono aggiornamento del DPS medesimo, già approvato con la richiamata deliberazione 35/2004;
c) n. 11 del 26.04.2007, con cui si è provveduto ad approvare gli aggiornamenti del DPS per l'anno 2007;
d) n. 18 del 30.04.2008 con cui si è provveduto ad approvare gli aggiornamenti del DPS per l'anno 2008;

Considerato, pertanto, necessario procedere ad aggiornare il DPS, approvato con la citata deliberazione 35/2004, e successivamente integrato, modificato ed aggiornato, sulla base del processo di consolidamento promosso dall'Agenzia, attraverso l'azione costante del Gruppo Privacy, finalizzata a diffondere una rinnovata cultura della riservatezza, che esprime nel nostro ordinamento un atto di alta civiltà, introducendo alcune sostanziali modifiche, così come risulta dal documento contenuto nell'allegato sub. lett. A, parte integrante e sostanziale del presente atto;

Ritenuto, altresì, di approvare il nuovo DPS, così come aggiornato, nel testo contenuto nell'Allegato sub. lett. A, parte integrante e sostanziale del presente atto;

Visto il parere favorevole espresso dal Direttore in ordine alla regolarità tecnico-amministrativa del presente atto;

A voti unanimi.

DELIBERA

1. di approvare, per le motivazioni espresse in narrativa, le integrazioni e modificazioni al Documento programmatico sulla sicurezza (DPS), già approvato con propria deliberazione n. 35 del 27/12/2004, così come modificata dalle deliberazioni n. 7 del 03/04/2006, n. 11 del 26/04/2007 e n. 18 del 30/04/2008, di cui al di cui al testo contenuto nell'allegato sub. lett. A, parte integrante e sostanziale del presente atto;

2. di disporre che:
   a) i responsabili del trattamento di dati sensibili nominati con la propria deliberazione n. 18 del 28/06/2004 e successive modificazioni, attuino le disposizioni contenute nel DPS impartendo specifiche prescrizioni agli incaricati del trattamento;
   b) il Direttore provveda a dare notizia dell'avvenuto aggiornamento del DPS nella relazione di accompagnamento al bilancio d'esercizio;
   c) il "Gruppo privacy":
      - attui gli adempimenti indicati nell'aggiornamento del DPS, attivando opportune azioni di monitoraggio circa il mantenimento delle condizioni di sicurezza ivi contenute;
      - curi la tenuta del DPS ai fini delle verifiche sia dell'Autority sia della Guardia di Finanza che collabora alle attività ispettive secondo quanto disposto nel protocollo siglato con lo stesso Garante in data 11/11/2005;

3. di assicurare, ai sensi dell'art. 1 della legge 7 agosto 1990, n. 241 e successive modificazioni, la pubblicità integrale del presente provvedimento mediante:
   a) inserimento nella apposita sezione "Atti amministrativi" sul sito web dell'ARS (www.arsanita.toscana.it);
   b) affissione all'Albo dei provvedimenti dell'Agenzia.

Il Direttore
Dott.ssa Laura Tramonti

Il Presidente
Dott. Giovanni Barbagli

Allegato A
Documento Programmatico sulla Sicurezza 2009

Agenzia Regionale di Sanità Toscana

Indice

1 Introduzione **3**
1.1 Gli strumenti di coordinamento, monitoraggio e aggiornamento delle attività in materia di privacy 5

2 Politiche di sicurezza e protezione dei dati **9**

3 Elenco dei trattamenti **13**
3.1 Elenco dei trattamenti: informazioni di base. 13
3.2 Elenco dei trattamenti: informazioni tecniche. 15
3.3 Trattamenti affidati all'esterno 17

4 Strutture e settori preposti ai trattamenti **19**

5 Analisi dei rischi **25**

6 Misure in essere e da adottare **29**

7 Profili di Rischio **33**

8 Piani formativi **39**

1 Introduzione

Questo documento è redatto in conformità alle disposizioni del decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".

In particolare l'articolo 34, nelle modalità indicate nel disciplinare tecnico contenuto nell'allegato B), prevede la tenuta di un aggiornato documento programmatico sulla sicurezza come precondizione obbligatoria per poter effettuare trattamenti di dati personali con strumenti elettronici.

Il Documento Programmatico sulla Sicurezza, aggiornato annualmente, definisce, sulla base dell'analisi dei rischi, della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento, i seguenti elementi:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare 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 di cui al punto 23 dell'allegato B del "Codice", come indicato nella Tabella 1 che segue;
- la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
- 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 del titolare;
- per i dati sensibili e giudiziari di cui ai punti da 20 a 24 dell'allegato B del "Codice" (si veda Tabella 1), l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

20	I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.
21	Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
22	I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
23	Sono adottate idonee misure 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.
24	Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Tabella 1: Ulteriori misure in caso di trattamento di dati sensibili o giudiziari.

Il presente documento descrive le misure adottate in relazione alla tipologia delle varie banche dati utilizzate nell'ambito delle finalità istitutive dell'Agenzia Regionale di Sanità (ARS) della Toscana, disciplinata con legge regionale 24 febbraio 2005, n. 40 (Disciplina del Servizio sanitario regionale) e successive modificazioni ed integrazioni.

L'ARS per effetto delle disposizioni su richiamate è ente strumentale e funzionale della Regione, dotato di personalità giuridica pubblica. La richiamata l.r. 40/2005 e successive modificazioni attribuisce all'ARS importanti funzioni di supporto e consulenza al Consiglio e alla Giunta regionale, alle Aziende sanitarie, alle società della salute e agli Enti locali, nonché altri soggetti pubblici o privati.

La tipologia dell'attività svolta dall'Agenzia può rientrare:

1. *nell'ambito della disciplina del trattamento dei dati sensibili* per l'esercizio delle funzioni di cui al Titolo VII, Capo I, della l.r. 24 febbraio 2005, n. 40 (Disciplina del Servizio sanitario regionale) e successive modificazioni; l'ARS infatti rientra a pieno titolo nell'ambito della predetta disciplina, o forse sarebbe più opportuno dire "naturaliter", cioè per sua vocazione naturale. Specificatamente:

    a) *per le funzioni generali di studio e ricerca per scopi statistici o scientifici* alla stessa attribuite ed esercitate attraverso gli Osservatori di Epidemiologia e per la Qualità (cfr. al disposto di cui al Capo III, agli articoli 104 e seguenti del "Codice");

b) *per le funzioni di ricerca scientifica in campo medico, biomedico o epidemiologico* prevista da un programma di ricerca biomedica o sanitaria di cui all'art. 12 bis del d.lgs. 502/'92 e successive modificazioni (cfr. alla disciplina recata dal Capo III, articolo 110);

2. *nell'ambito delle disposizioni relative al trattamento dati di tipo sanitario* (organismo sanitario pubblico), contenute nel Titolo V, Capo I, art. 76 del "Codice", per perseguire finalità collettive, "riguardanti un terzo o la collettività '. L'A.R.S., ancorché non eroghi prestazioni sanitarie, puó rientrare tra gli organismi sanitari pubblici qualora tratti dati di tipo sanitario per perseguire finalità d'interesse pubblico che riguardi un terzo o la collettività. La legge regionale, infatti, attribuisce alla stessa, tra l'altro, funzioni di supporto in materia di programmazione regionale, valutazione della sanità regionale, valutazione della programmazione, analisi dei modelli organizzativi e gestionali;

3. *nell'ambito della disciplina del trattamento di dati sensibili e giudiziari* per l'esercizio dell'attività amministrativa prevista dal Tit. VII, Capo I, della l.r. 40/2005 e successive modificazioni.

Ai fini predetti nel paragrafo 3, "Elenco dei trattamenti", la finalità degli stessi è contrassegnata dai numeri: **1a**, **1b**, **2** o **3**, secondo la tipologia dell'attività svolta.

1.1 Gli strumenti di coordinamento, monitoraggio e aggiornamento delle attività in materia di privacy

Nel corso del biennio 2004/2005 l'ARS si è dotata di strumenti di coordinamento, monitoraggio e aggiornamento delle attività in materia di privacy, che il CdA ha disposto per una corretta e attenta applicazione delle disposizioni del "Codice" con il duplice obiettivo di:

- adempiere agli obblighi normativi;
- favorire una costante crescita, all'interno dell'Agenzia, di una nuova cultura della riservatezza.

Gruppo Privacy

Con deliberazione n. 18 del 28/06/2004 il CdA ha istituito in seno all'Agenzia un gruppo di lavoro denominato "Gruppo Privacy", stante l'impatto trasversale del "Codice" la cui applicazione richiede una serie di adempimenti a rilevanza interna ed esterna ed un'approfondita attività di monitoraggio, attraverso il coinvolgimento di più soggetti, con competenze e formazione diversificati.

Il Gruppo rappresenta un elemento di novità rispetto al "Codice" sulla privacy, la cui costituzione si è imposta per motivi di opportunità strategica. L'idea di far germinare in seno all'ARS un gruppo costituito da personale interno è apparsa come lo strumento più idoneo a promuovere un cambiamento di cultura e mentalità all'interno dell'Agenzia e a raggiungere tutti gli operatori, che hanno il proprio riferimento all'interno del gruppo. Infatti, si tratta di una struttura di staff a carattere multidisciplinare, in quanto costituito da diverse professionalità (giuridiche, organizzative, tecniche, informatiche, statistiche ecc.) a supporto dello svolgimento dei compiti prescritti dal Codice.

Il CdA ha attribuito al Gruppo Privacy i seguenti compiti:

- segnala le novità normative;
- tiene ed aggiorna:
  - la notificazione, le autorizzazioni (ove necessarie), le comunicazioni al Garante;
  - il censimento dei trattamenti dei dati personali sensibili/giudiziari (CE.TRA) sulla base delle comunicazioni effettuate dai Responsabili e dagli incaricati del trattamento;
  - l'elenco degli archivi cartacei e/o magnetici dei dati personali e/o sensibili/giudiziari custoditi dall'Agenzia;
  - l'anagrafe dei Responsabili e degli incaricati;
  - il registro delle convenzioni/protocolli d'intesa/contratti relativi all'affidamento all'esterno del trattamento dei dati di cui è titolare ARS;
  - il registro delle convenzioni/protocolli d'intesa/accordi/contratti stipulati con altri enti ai fini dell'accesso da parte dell'A.R.S. a flussi di dati attinenti alla salute ovunque collocati o per l'accesso da parte di altri enti ai dati di ARS;
- aggiorna le procedure;
- assicura, in collaborazione con il Titolare ed i responsabili dei trattamenti, l'aggiornamento del documento programmatico sulla sicurezza;
- collabora con i Responsabili ai processi di formazione e informazione, al fine di sostenere la nascita e la crescita di una cultura del rispetto e della riservatezza a livello di Agenzia.

Al Gruppo sono, altresì attribuiti compiti di monitoraggio con specifico riguardo alle tipologie di banche dati detenute, sia elettroniche sia cartacee, agli strumenti elettronici utilizzati per il trattamento (elaboratori stand-alone, computer collegati in rete locale, connessione a rete aperta ecc.), ai flussi informativi verso l'esterno e quelli infra-strutture e all'ambito di comunicazione e di diffusione dei dati.

CE.TRA.

L'A.R.S. ha istituito il censimento dei trattamenti (CE.TRA.) al fine di monitorizzare costantemente le attività Il CE.TRA. contiene la rilevazione dei trattamenti dei dati suddivisi per tipologie e per strutture organizzative ed è tenuto a cura del Gruppo Privacy. Le informazioni che contiene sono:

- i trattamenti e le strutture dove avvengono le operazioni;
- la natura dei dati trattati e gli strumenti elettronici utilizzati;
- i luoghi di custodia dei supporti elettronici;
- la tipologia degli strumenti di accesso e le modalità di interconnessione alla rete.

Il Gruppo provvede ad aggiornare il CE.TRA., qualora siano comunicati da parte del Titolare o dei Responsabili del trattamento casi di attivazione di un nuovo trattamento o cessazione di un trattamento in essere.

Anagrafe Responsabili e Incaricati

Il "Codice", per garantire l'effettivo esercizio dei diritti dell'interessato, impone al titolare del trattamento di adottare idonee misure volte, in particolare:

- ad agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi strumenti;
- a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente. Allo scopo di adempiere alle disposizioni del Codice, l'Agenzia ha istituito l'anagrafe dei Responsabili e degli Incaricati al trattamento, onde agevolare e semplificare l'accesso alle informazioni che l'interessato può richiedere.

L'istituzione dell'Anagrafe dei Responsabili e degli Incaricati del trattamento costituisce, altresì una modalità operativa che consente di monitorare costantemente la situazione in essere, anche al fine di corrispondere ad ogni richiesta che possa pervenire dall'Ufficio del Garante o dalle autorità ispettive preposte (Guardia di Finanza).

Registro convenzioni affidamento trattamento dati all'esterno

L'istituzione dei Registri, di cui al presente paragrafo, la cui tenuta e aggiornamento è affidato al Gruppo Privacy, corrisponde all'esigenza di monitorare costantemente l'evoluzione delle azioni da porre in essere in adempimento alle disposizioni del "Codice", con particolare riguardo all'osservanza degli obblighi nei confronti del Garante e degli adempimenti correlati alle attività rilevanti connesse ai trattamenti di dati sensibili.

Portale "Privacy"

Per favorire la più ampia trasparenza e correttezza nei confronti degli utenti e il pieno rispetto dei principi del Codice, in linea con il processo di innovazione della pubblica amministrazione introdotto con la riforma della cosiddetta "Legge Bassanini", l'ARS ha deciso di aprire uno specifico "Portale Privacy" con il duplice scopo di:

- consentire agli interessati ai trattamenti eseguiti da ARS di accedere liberamente e fruire di tutte le informazioni utili per l'esercizio dei propri diritti;
- promuovere la circolazione delle informazioni tra i soggetti che a vario titolo operano per perseguire il consolidamento della cultura della riservatezza, nel rispetto delle libertà fondamentali dell'individuo e della dignità della persona.

Il portale sarà realizzato nel corso del 2009.

2 Politiche di sicurezza e protezione dei dati

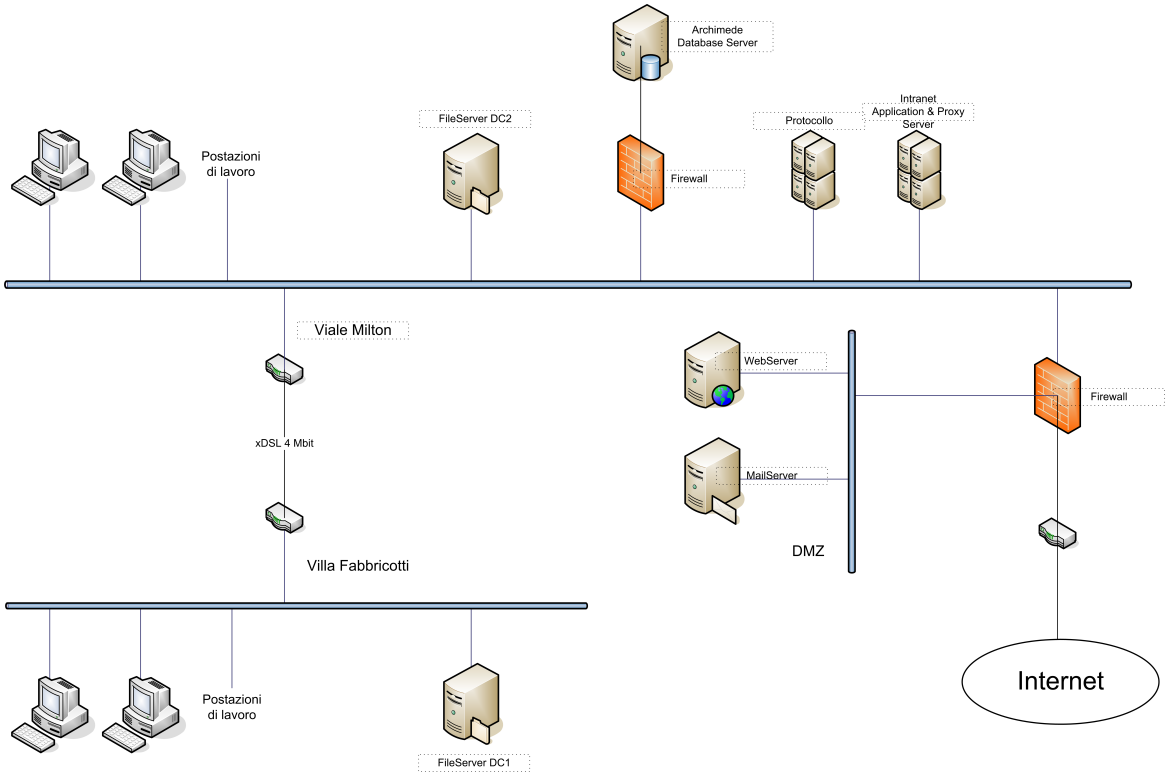

Figura 1: Descrizione dell'infrastruttura

Le politiche di sicurezza implementate nella rete dell'ARS seguono alcune linee guida generali. Gli account di rete ed i vari servizi sono centralizzati per poter distribuire gli opportuni permessi alle risorse condivise, applicare generali politiche di controllo e accesso, ed avere maggiori garanzie sulla consistenza ed integrità dei dati. I server ed i servizi di rete possono essere amministrati solo dal personale dell'U.O. Sistemi Informatici e solo da postazioni espressamente autorizzate: di norma è necessario un livello di autenticazione ma per amministrare alcuni servizi o server sono necessari ulteriori livelli.

La continua manutenzione, svolta dall'U.O. Sistemi Informatici, dei server e dei servizi di rete contribuisce a ridurre i rischi per la sicurezza causati da errori nei vari programmi e sistemi operativi utilizzati: la rete dell'ARS è continuamente oggetto di processi di messa in sicurezza e monitoraggio.

La rete dell'ARS si compone di una rete (locale) non accessibile dall'esterno ed una rete (DMZ) che invece è accessibile da Internet: tutto il traffico dati tra la rete locale, la DMZ ed Internet è filtrato da un firewall. Attualmente sono presenti due server nella DMZ (Mail e WebServer) che forniscono servizi di posta, proxy, server web e controllo

antivirus su tutto il traffico HTTP SMTP ed FTP. Per ogni servizio antivirus le definizioni dei virus sono aggiornate ogni ora: ogni mese viene controllato se sono stati rilasciati altri aggiornamenti da installare manualmente. Gli accessi da Internet sono possibili solamente mediante procolli criptati. Non sono consentite connessione di tipo peer to peer verso Internet, ed in generale qualunque tipo di connessione non necessaria.

Ogni account per accedere alla rete è centralizzato su un servizio di directory, e gli utenti non possono modificare la configurazione di accesso ad Internet, né installare o rimuovere software, né modificare la configurazione dei computer in uso. La configurazione hardware dei computer non è modificabile dagli utenti ed è protetta da una password. E' implementata una politica di gestione delle autenticazioni che soddisfa tutte le prescrizioni dettate dal Codice e gli utenti sono obbligati a cambiare la propria password ogni sessanta giorni. Inoltre, per evitare che il personale non autorizzato abbia accesso ai dati nel caso in cui una postazione si trovi accidentalmente a non essere presidiata, oltre alle disposizioni date agli incaricati, si è provveduto a impostare su ogni computer uno screensaver con password che si attiva automaticamente dopo pochi minuti.

L'accesso ai database presenti sul server Oracle, Archimede, è protetto ulteriormente da un firewall interno (come rappresentato in Fig. 1), che consente connessioni solo dalle postazioni degli incaricati. In ogni postazione solo ad alcuni utenti è concesso di avviare il software di connessione, per cui è possibile sapere chi e da quale computer si è connesso al server Archimede. E' inoltre previsto un ulteriore servizio di autenticazione, distinto dal servizio di directory della rete locale, per permettere l'accesso ai database e il monitoraggio delle autorizzazioni.

Nelle rete locale, su ogni computer e server è installato un apposito software antivirus amministrato tramite due server centralizzati. Gli aggiornamenti critici e di sicurezza dei sistemi operativi sono distribuiti automaticamente mediante un apposito server appena vengono rilasciati dalla casa software.

Per quanto riguarda le politiche di protezione dei dati, è stato implementato un doppio livello di sicurezza. I server su cui risiedono i dati sono dotati di batterie di dischi ridondate in configurazione RAID: nel caso di malfunzionamento di uno dei dischi è possibile ripristinare tutti i dati in poche ore sostituendo il disco in questione. Tutte le banche dati, inoltre, sono salvate quotidianamente su nastri attraverso un sistema di backup centralizzato. Copie degli archivi su nastro vengono conservate in cassaforte ignifuga nella sede di Viale Milton n 7. Il personale incaricato delle U.O. Sistemi Informatici e Centro Statistico Elaborazione Dati custodiscono il codice di apertura della cassaforte. Una ulteriore copia di emergenza del codice è depositata, in busta chiusa, nella cassaforte di Villa Fabbricotti. L'U.O. Sistemi Informatici è l'unica responsabile dei processi di backup e ripristino dei dati ed effettua regolarmente verifiche di consistenza degli archivi e prove di ripristino.

I server che contengono i dati personali e sensibili sono distribuiti nelle due sedi dell'ARS: Villa Fabbricotti in Via Vittorio Emanuele II e viale Milton n 7 a Firenze. Le apparecchiature di viale Milton (server Archimede e FileServer-dc2) sono concentrate in una stanza seminterrata protetta da una porta metallica con serratura e inferriate alla finestra; in Villa Fabbricotti (server FileServer-dc1) sono disposte dentro un armadio metallico di tipo rack chiuso a chiave. Entrambe le sedi sono costantemene presidiate durante l'orario di apertura dell'ARS.

3 Elenco dei trattamenti

3.1 Elenco dei trattamenti: informazioni di base.

ID	Nome	Descrizione e interessati	Finalità
1	sdo	schede dimissione ospedaliera 1996-2006	1a
2	spa	specialistica ambulatoriale 2001-2006	1a
3	rmr	registro mortalità 1988-2005	1a
4	spr	prestazioni riabilitazione 2000-2006	1a
5	spf	prescrizioni farmaceutiche 2003-2006	1a
6	sea	anagrafe esenzioni patologia 2002	1a
7	asa	anagrafe assistibili	1a
8	abs	archivio aborti spontanei 2000-2006	1a
9	ivg	interruzioni volontarie gravidanza 2000-2006	1a
10	cap	certificato assistenza parto 2000-2006	1a
11	inail	infortuni inail 2000-2003	1a
12	morti caldo	dati individuali di mortalita relativi a 53 comuni Toscani. anno 2003	1a
13	archivio rir	pazienti con diagnosi retinoblastoma	1a
14	registro aids	registro dei casi di AIDS notificati in Toscana	1a
15	euroscore	indicatori esito delle cardiochirurgie 2003	1a
16	Sorveglianza attiva	promozione degli interventi di salute nei confronti degli anziani fragili	1a
17	linfrev	risultati esami istologici	1a
18	ripo	registro regionale impiantologia protesica	1a
19	progetto stroke	interviste pazienti, familiari e medici	1a
20	dialisi	registro dialisi e trapianti - fonte cspo	1a
21	unità spinale	archivio pazienti Unità Spinale - Firenze	1a
22	vis	database georeferenziato stato di salute Firenze, Campi Bisenzio, Sesto Fiorentino	1a
23	chiamate 118	archivio chiamate 118 nella provincia di Firenze 1999-2000	1a
24	coorte alcolisti	utenti alcolisti -centro alcologico asl10, SERT Arezzo e U.O. Tossicologia careggi 1970-2000	1a
25	coorte tossicodipendenti	utenti SERT Regione Toscana 1970-2000	1a
26	coorte utenti pronto soccorso	accessi per incidente stradale ai 4 p.s. dell'asl10	1a
27	stili di vita	indagine postale/telefonica sugli stili di vita in 6 aree della Toscana	1a
28	gambling	indagine sul comportamento al gioco nella zona valdinievole 2002	1a
29	studio vedette	verifica ed efficacia dei trattamenti dei tossicodipendenti da eroina (utenti di 5 SERT toscani)	1a
30	ricoveri alcol correlati	schede dimissioni ospedaliere AO careggi 1977-1995	1a
31	cronos	dati relativi ai soggetti reclutati per il progetto	1b
32	domus	dati relativi ai soggetti reclutati per il progetto	1a
33	assi	dati relativi ai soggetti reclutati per il progetto ASSI-RSA	1b
34	alzheimer	dati relativi ai soggetti con alzheimer individuati da altri studi o da archivio sdo	1b

ID	Nome	Descrizione e interessati	Finalità
35	omega care	archivio dei medici di base arruolati per il progetto e raccolta dei questionari	1b
36	Registro Ec/Acv	Registro nazionale eventi cerebrovascolari	1a
37	Archivio midollolesi	Archivio dei casi notificati di midollolesioni	1a
38	Progetto menopausa	archivio dati relativi ai soggetti reclutati per il progetto	1a
39	Buste paga	Gestione informatizzata globale della posizione giuridica e del trattamento economico del personale	1a
40	Mamma e Lavoro	archivio dati relativi ai soggetti reclutati per il progetto	1a
41	sapere II	dati relativi ai pazienti colpiti da ictus e ai relativi medici di base (progetto Sapere II)	1a
42	ulcere	dati relativi a pazienti ricoverati negli ospedali ed in carico ai distretti	1a
43	GCLA	dati estratti da cartelle cliniche di pazienti cerebrolesi 2003 in 3 strutture toscane	1a
44	Gravidanza e lavoro	dati individuali sulla storia lavorativa di una coorte di donne con libretto di gravidanza	1a
45	Action II	dati individuali di follow-up sulla casistica ACTION I	1b
46	Action I	dati individuali sui gravemente prematuri e sugli operatori	1b
47	Progetto menopausa Italia	dati individuali di un gruppo di donne trattate con agopuntura per i disturbi della menopausa	1a
48	Cadute	Dati relativi a pazienti ricoverati	1a
49	Dolore	Cartelle cliniche dei pazienti ricoverati	1a
50	CVC	Pazienti con CVC	1a
51	Mamma informata	dati relativi ai soggetti reclutati per il progetto	1a
52	Mortalità prematura Infantile	dati individuali di mortalità	1a
53	Archivio PV	Utenti centro alcologico integrato	1a
54	Incidenti balneari	Archivio incidenti balneari in Toscana	1a
55	Elettroschock	Dati cartelle cliniche pazienti con elettroschock	1a
56	Vita indipendente	Dati sullo stato di disabilità di portatori di handicap partecipanti alla sperimentazione	1a
57	Pagamento	Pagamento indennità, rimborsi spese ai membri degli organi e trattamento economico del personale	3
58	progetto InChianti	coorte di anziani residenti in Chianti (questionari, dati clinici, accesso ai servizi)	1a
59	Protocollo	Archivio del protocollo in entrata/uscita	1a
60	Segreteria	Gestione pratiche varie di segreteria	1a
61	Segreteria (personale e organi)	Amministrazione di informazioni sensibili e giudiziarie riguardanti il personale e gli organi di ARS	3
62	Segreteria (Attività contratt.)	Amministrazione di informazioni sensibili e giudiziarie riguardanti l'attività contrattuale di ARS	3
63	Progetto ADI	dati sull'assistenza domiciliare	1a
64	Sorveglianza sanitaria ARS	dati per l'attività di sorveglianza sanitaria dei lavoratori ARS	3

Tabella 2: Elenco dei trattamenti: informazoni di base.

3.2 Elenco dei trattamenti: informazioni tecniche.

ID	Natura dei dati	E/ C	Luogo	Struttura	Profilo di rischio	Protezione
1	Sensibili	E	archimede	CSED[1] e TI[2]	PR003	Separazione/ Cifratura
2	Sensibili	E	archimede	CSED e TI	PR003	Separazione/ Cifratura
3	Sensibili	E	archimede	CSED e TI	PR003	Separazione/ Cifratura
4	Sensibili	E	archimede	CSED e TI	PR003	Separazione/ Cifratura
5	Sensibili	E	archimede	CSED e TI	PR003	Separazione/ Cifratura
6	Sensibili	E	archimede	CSED e TI	PR003	Separazione/ Cifratura
7	Sensibili	E	archimede	CSED e TI	PR003	Separazione/ Cifratura
8	Sensibili	E	archimede	CSED e TI	PR003	Separazione/ Cifratura
9	Sensibili	E	archimede	CSED e TI	PR003	Separazione/ Cifratura
10	Sensibili	E	archimede	CSED e TI	PR003	Separazione/ Cifratura
11	Sensibili	E	archimede	CSED e TI	PR003	Separazione/ Cifratura
12	Sensibili	E	cassaforte	Oss. Epidem.	PR005	Separazione
13	Sensibili	E/C	cassaforte	Oss. Qualità	PR005	Separazione
14	Sensibili	E/C	archimede	Oss. Epidem.	PR003, PR005	Separazione/ Cifratura
15	Sensibili	E	fileserver	Oss. Qualità	PR001	Cifratura
16	Sensibili	E	fileserver	Oss. Epidem.	PR001	Cifratura
17	Sensibili	E	cassaforte	Oss. Qualità	PR005	Separazione
18	Sensibili	E/C	webserver	Oss. Qualità	PR001, PR005	Separazione
19	Sensibili	E/C	fileserver	Oss. Qualità	PR001, PR005	Cifratura
20	Sensibili	E	fileserver	Oss. Qualità	PR001	Cifratura
21	Sensibili	E	fileserver	Oss. Epidem.	PR001	Cifratura
22	Sensibili	E	fileserver	Oss. Epidem.	PR001	Cifratura
23	Sensibili	E	fileserver	Oss. Epidem.	PR001	Cifratura
24	Sensibili	E	fileserver	Oss. Epidem.	PR001	Cifratura
25	Sensibili	E	fileserver	Oss. Epidem.	PR001	Cifratura
26	Sensibili	E	fileserver	Oss. Epidem.	PR001	Cifratura
27	Sensibili	E/C	fileserver	Oss. Epidem.	PR001, PR005	Cifratura
28	Sensibili	E	fileserver	Oss. Epidem.	PR001	Cifratura

[1]Centro Statistico Elaborazione Dati.
[2]Tecnologie dell'Informazione.

ID	Natura dei dati	E/C	Luogo	Struttura	Profilo di rischio	Protezione
29	Sensibili	E/C	fileserver	Oss. Epidem.	PR001, PR005	Cifratura
30	Sensibili	E	fileserver	Oss. Epidem.	PR001	Cifratura
31	Sensibili	E	fileserver	Oss. Epidem.	PR001	Cifratura
32	Sensibili	E/C	fileserver	Oss. Epidem.	PR001, PR005	Cifratura
33	Sensibili	E	fileserver	Oss. Epidem.	PR001	Cifratura
34	Sensibili	E/C	fileserver	Oss. Epidem.	PR001, PR005	Cifratura
35	Sensibili	E/C	fileserver	Oss. Epidem.	PR001, PR005	Cifratura
36	Sensibili	E/C	Esterno	Asl 10,Oss. Epidem.		
37	Sensibili	E	fileserver	Oss. Epidem.	PR001	Cifratura
38	Sensibili	E/C	fileserver	Oss. Epidem.	PR001, PR005	Cifratura
39	Sensibili	E	Esterno	Sigma Informatica SpA		
40	Sensibili	E	fileserver	Oss. Epidem.	PR001	Cifratura
41	Sensibili	E/C	archimede	Oss. Qualità	PR003, PR005	Separazione/ Cifratura
42	Sensibili	E/C	archimede	Oss. Qualità	PR003, PR005	Separazione/ Cifratura
43	Sensibili	E/C	archimede	Oss. Qualità	PR003, PR005	Separazione/ Cifratura
44	Sensibili	E	fileserver	Oss. Epidem.	PR001	Cifratura
45	Sensibili	E/C	fileserver	Oss. Epidem.	PR001, PR005	Cifratura
46	Sensibili	E/C	fileserver	Oss. Epidem.	PR001, PR005	Cifratura
47	Sensibili	E/C	fileserver	Oss. Epidem.	PR001, PR005	Cifratura
48	Sensibili	E/C	archimede	Oss. Qualità	PR003, PR005	Cifratura
49	Sensibili	E/C	fileserver	Oss. Qualità	PR001, PR005	Cifratura
50	Sensibili	E/C	fileserver	Oss. Qualità	PR001, PR005	Cifratura
51	Sensibili	E/C	cassaforte	Oss. Epidem.	PR005	Separazione
52	Sensibili	E/C	fileserver	Oss. Epidem.	PR001, PR005	Cifratura
53	Sensibili	E	cassaforte	Oss. Epidem.	PR005	Separazione
54	Sensibili	E	fileserver	Oss. Epidem.	PR001	Cifratura
55	Sensibili	E/C	fileserver	Oss. Epidem.	PR001, PR005	Cifratura
56	Sensibili	E/C	fileserver	Oss. Epidem.	PR001, PR005	Cifratura
57	Sensibili	E	Esterno	Monte dei Paschi di Siena		
58	Sensibili	E	Esterno	Asl 10, Oss. Epidem		
59	Sensibili	E/C	Server protocollo	Segreterie	PR001, PR005	Separazione

ID	Natura dei dati	E/ C	Luogo	Struttura	Profilo di rischio	Protezione
60	Sensibili	E/C	ARS	Segreterie	PR001, PR005	Separazione
61	Sensibili/ Giudizia- ri	E/C	ARS	U.O. Personale e C., U.O. Contabilità e Bilancio	PR001, PR005	Separazione
62	Sensibili/ Giudizia- ri	E/C	ARS	U.O. Contratti e Forniture	PR001, PR005	Separazione
63	Sensibili	E	fileserver	Oss. Epidem.	PR001	Cifratura
64	Sensibili	C	Esterno	Medico competente		

Tabella 3: Elenco dei trattamenti: informazioni tecniche.

3.3 Trattamenti affidati all'esterno

I trattamenti n. 39 e 57 dell'U.O. "Personale e Convenzioni" sono svolti in concorso con soggetti esterni. Rispettivamente con:

1. la ditta Sigma Informatica SpA, per il pagamento delle indennità e rimborsi spese ai membri degli organi e del trattamento economico personale dipendente, convenzionato, a contratto;

2. il Monte dei Paschi di Siena SpA, per il pagamento delle indennità e rimborsi spese ai componenti degli organi e del trattamento economico personale dipendente, convenzionato, a contratto.

I trattamenti n. 36 e 58 dell'Osservatorio di Epidemiologia sono svolti in concorso con soggetti esterni. Rispettivamente con:

1. Dott. Alessandro Barchielli (Asl 10, Unità di Epidemiologia) per i dati relativi agli archivi toscani di patologia cardiovascolare;

2. Dott.ssa Stefania Bandinelli (Dirigente UO Geriatria ASF Firenze, responsabile scientifico per Azienda USL n. 10 di Firenze) per il Progetto denominato "Studio InChianti", di cui al contratto sottoscritto in data 30.11.2004 da ARS e National Institutes of Health di Bethesda di Maryland (USA). Il progetto è condotto nei Comuni di Greve in Chianti e Bagno a Ripoli ed ha ad oggetto uno studio epidemiologico sull'invecchiamento.

Il trattamento n.64 è svolto in concorso con:

1. Dott. Pier Giovanni Manescalchi, per l'attività di sorveglianza sanitaria dei lavoratori ARS.

Come stabilito dalla deliberazione del CdA dell'ARS n. 18 del 28/6/2004 e successive modificazioni, all'atto dell'affidamento è richiesta la sottoscrizione dell'impegno ad

osservare i principi e le disposizioni del "Codice" e dei Codici di deontologia e buona condotta, nonché le specifiche istruzioni impartite dal Titolare dei trattamenti dell'ARS ai Responsabili degli stessi, secondo il disposto di cui all'allegato sub. lett. B della già citata deliberazione 18/2004.

4 Strutture e settori preposti ai trattamenti

Osservatorio di Epidemiologia:

Descrizione compiti e finalità
L'Osservatorio svolge le funzioni previste dall'articolo 82-bis *(Compiti e attribuzioni)* della l.r. 24/2/2005, n. 40 e successive modificazioni.
In particolare l'Osservatorio svolge attività di ricerca applicata alla realtà toscana nell'ambito della epidemiologia di sanità pubblica e dei servizi sanitari.
L'Osservatorio è costituito da un gruppo di operatori con competenze epidemiologiche e statistiche che collabora con funzioni di coordinamento, nell'ambito di progetti condivisi, con le numerose competenze epidemiologiche e statistiche presenti in Toscana.
L'Osservatorio collabora con diversi Dipartimenti della Regione Toscana, in particolare con il Dipartimento Diritto alla Salute e Politiche di Solidarietà e con il Dipartimento dell'Ambiente. Per quanto riguarda il Dipartimento Diritto alla Salute e Politiche di Solidarietà la collaborazione comprende la stesura di documenti preparatori per gli atti di programmazione regionale, oltre al contributo alla realizzazione delle relazioni sanitarie annuali. L'Osservatorio si avvale dei flussi informativi correnti che vengono trasmessi dal Dipartimento nella loro forma consolidata ed inseriti nel Sistema Informativo dell'Agenzia.

Questo Osservatorio effettua i trattamenti indicati in Tabella 4 nelle modalità e responsabilità indicate dal Responsabile nell'atto di nomina degli incaricati, secondo il profilo e l'ambito di competenza assegnato.

ID	Nome	Descrizione
12	morti caldo	dati individuali di mortalita relativi a 53 comuni Toscani. anno 2003
14	registro aids	registro dei casi di AIDS notificati in Toscana
16	Sorveglianza attiva	promozione degli interventi di salute nei confronti degli anziani fragili
21	unità spinale	archivio pazienti Unità Spinale - Firenze
22	vis	database georeferenziato stato di salute Firenze, Campi Bisenzio, Sesto Fiorentino
23	chiamate 118	archivio chiamate 118 nella provincia di Firenze 1999-2000
24	coorte alcolisti	utenti alcolisti -centro alcologico asl10, SERT Arezzo e U.O. Tossicologia careggi 1970-2000
25	coorte tossicodipendenti	utenti SERT Regione Toscana 1970-2000
26	coorte utenti pronto soccorso	accessi per incidente stradale ai 4 p.s. dell'asl10
27	stili di vita	indagine postale/telefonica sugli stili di vita in 6 aree della Toscana
28	gambling	indagine sul comportamento al gioco nella zona valdinievole 2002
29	studio vedette	verifica ed efficacia dei trattamenti dei tossicodipendenti da eroina (utenti di 5 SERT toscani)
30	ricoveri alcol correlati	schede dimissioni ospedaliere AO careggi 1977-1995
31	cronos	dati relativi ai soggetti reclutati per il progetto
32	domus	dati relativi ai soggetti reclutati per il progetto
33	assi	dati relativi ai soggetti reclutati per il progetto ASSI-RSA
34	alzheimer	dati relativi ai soggetti con alzheimer individuati da altri studi o da archivio sdo
35	omega care	archivio dei medici di base arruolati per il progetto e raccolta dei questionari
37	Archivio midollolesi	Archivio dei casi notificati di midollolesioni
38	Progetto menopausa	archivio dati relativi ai soggetti reclutati per il progetto
40	Mamma e Lavoro	archivio dati relativi ai soggetti reclutati per il progetto
44	Gravidanza e lavoro	dati individuali sulla storia lavorativa di una coorte di donne con libretto di gravidanza
45	Action II	dati individuali di follow-up sulla casistica ACTION I
46	Action I	dati individuali sui gravemente prematuri e sugli operatori
47	Progetto menopausa Italia	dati individuali di un gruppo di donne trattate con agopuntura per i disturbi della menopausa
51	Mamma informata	dati relativi ai soggetti reclutati per il progetto
52	Mortalità prematura Infantile	dati individuali di mortalità
53	Archivio PV	Utenti centro alcologico integrato
54	Incidenti balneari	Archivio incidenti balneari in Toscana
55	Elettroschock	Dati cartelle cliniche pazienti con elettroschock
56	Vita indipendente	Dati sullo stato di disabilità di portatori di handicap partecipanti alla sperimentazione
63	Progetto ADI	dati sull'assistenza domiciliare

Tabella 4: Elenco dei trattamenti dell'Osservatorio di Epidemiologia.

Osservatorio per la Qualità:

Descrizione compiti e finalità
L'Osservatorio svolge le funzioni previste dall'articolo 82-bis *(Compiti e attribuzioni)* della l.r. 24/2/2005, n. 40 e successive modificazioni. In particolare l'Osservatorio per la Qualità ha funzioni di:
- orientamento, supporto formativo e metodologico, facilitazione e consulenza di processo alla realizzazione di progetti ed interventi di miglioramento della qualità dell'assistenza;
- supporto all'applicazione di strumenti e metodi di provata efficacia per la valutazione di processo e di risultato in singoli settori e processi assistenziali e gestionali;
- documentazione su conoscenze ed esperienze in materia di qualità dei servizi.

Questo Osservatorio effettua i trattamenti indicati in Tabella 5 nelle modalità e responsabilità indicate dal Responsabile nell'atto di nomina degli incaricati, secondo il profilo e l'ambito di competenza assegnato.

ID	Nome	Descrizione
13	archivio rir	pazienti con diagnosi retinoblastoma
15	euroscore	indicatori esito delle cardiochirurgie 2003
17	linfrev	risultati esami istologici
18	ripo	registro regionale impiantologia protesica
19	progetto stroke	interviste pazienti, familiari e medici
20	dialisi	registro dialisi e trapianti - fonte cspo
41	sapere II	dati relativi ai pazienti colpiti da ictus e ai relativi medici di base (progetto Sapere II)
42	ulcere	dati relativi a pazienti ricoverati negli ospedali ed in carico ai distretti
43	GCLA	dati estratti da cartelle cliniche di pazienti cerebrolesi 2003 in 3 strutture toscane
48	Cadute	Dati relativi a pazienti ricoverati
49	Dolore	Cartelle cliniche dei pazienti ricoverati
50	CVC	Pazienti con CVC

Tabella 5: Elenco dei trattamenti dell'Osservatorio per la Qualità:

U.O. Sistemi Informatici:

Descrizione compiti e finalità:
L'U.O. Sistemi Informatici si occupa, in relazione alle banche dati di:
Definizione di regole, processi e standard nell'ambito della sicurezza informatica.
Gestione e manutenzione delle infrastrutture di sicurezza.
Amministrazione dati.
Salvaguardia dati e gestione degli strumenti di backup.
Controllo di accesso ai dati.
Progetto, sviluppo e manutenzione di configurazioni di rete.

Gestione di Database e Applications server.
Assistenza agli utenti.

Questa U.O. effettua i trattamenti presenti in Agenzia Regionale di Sanità nelle modalità e responsabilità indicate dal Responsabile nell'atto di nomina degli incaricati, secondo il profilo e l'ambito di competenza assegnato.

U.O. Tecnologie dell'Informazione:

Descrizione compiti e finalità:
Implementazione e manutenzione della base dati centrale; architettura della base dati, analisi delle sue prestazioni e risoluzione problemi, implementazione di procedure di manipolazione dati complesse. Provvede alla realizzazione di applicativi Internet/Intranet per la pubblicazione e acquisizione di dati.

U.O. Centro Statistico Elaborazione Dati:

Descrizione compiti e finalità:
Implementazione e manutenzione della base dati centrale; controllo dati acquisiti, assistenza sulle modalità d'accesso e sui contenuti della base dati, realizza la documentazione a supporto dell'utenza. Provvede all'elaborazione di dati che richiedono periodicità nel calcolo o tecniche di analisi complesse.

Queste due ultime U.O. effettuano i trattamenti indicati in Tabella 6 nelle modalità e responsabilità indicate dal Responsabile nell'atto di nomina degli incaricati, secondo il profilo e l'ambito di competenza assegnato.

ID	**Nome**	**Descrizione**
1	sdo	schede dimissione ospedaliera 1996-2006
2	spa	specialistica ambulatoriale 2001-2006
3	rmr	registro mortalità 1988-2005
4	spr	prestazioni riabilitazione 2000-2006
5	spf	prescrizioni farmaceutiche 2003-2006
6	sea	anagrafe esenzioni patologia 2002
7	asa	anagrafe assistibili
8	abs	archivio aborti spontanei 2000-2006
9	ivg	interruzioni volontarie gravidanza 2000-2006
10	cap	certificato assistenza parto 2000-2006
11	inail	infortuni inail 2000-2003

Tabella 6: Elenco dei trattamenti CSED e TI.

U.O. Personale e Convenzioni:

Descrizione compiti e finalità:
Gestione amministrativa, economica, giuridica e previdenziale del personale. Reclutamento del personale e tenuta dei relativi fascicoli. Contratti relativi a tutte le tipologie di personale. Convenzioni con Enti e Istituti.

Questa U.O. effettua i trattamenti indicati in Tabella 7 nelle modalità e responsabilità indicate dal Responsabile nell'atto di nomina degli incaricati, secondo il profilo e l'ambito di competenza assegnato.

ID	Nome	Descrizione
61	Segreteria (personale e organi)	Amministrazione di informazioni sensibili e giudiziarie riguardanti il personale e gli organi di ARS

Tabella 7: Elenco dei trattamenti dell'U.O. Personale e Convenzioni.

U.O. Patrimonio Contratti e Forniture:

Descrizione compiti e finalità:
Attività connesse all'acquisizione ed amministrazione di beni e servizi. Attività contrattuale dell'Ente e forniture di beni. Amministrazione dei beni mobili del patrimonio e rapporti con i consegnatari.

Questa U.O. effettua i trattamenti indicati in Tabella 8 nelle modalità e responsabilità indicate dal Responsabile nell'atto di nomina degli incaricati, secondo il profilo e l'ambito di competenza assegnato.

ID	Nome	Descrizione
62	Segreteria (Attività contratt.)	Amministrazione di informazioni sensibili e giudiziarie riguardanti l'attività contrattuale di ARS

Tabella 8: Elenco dei trattamenti dell'U.O. Patrimonio Contratti e Forniture.

U.O. Contabilità e Bilancio:

Descrizione compiti e finalità:
Gestione, ai fini contabili, delle indennità e retribuzioni agli Organi e al personale.

Questa U.O. effettua i trattamenti indicati in Tabella 9 nelle modalità e responsabilità indicate dal Responsabile nell'atto di nomina degli incaricati, secondo il profilo e l'ambito di competenza assegnato.

ID	Nome	Descrizione
61	Segreteria (personale e organi)	Amministrazione di informazioni sensibili e giudiziarie riguardanti il personale e gli organi di ARS

Tabella 9: Elenco dei trattamenti dell'U.O. Contabilità e Bilancio.

5 Analisi dei rischi

Codice evento	Nome evento	Descrizione evento	Impatto sulla sicurezza
E-001	Sottrazione di credenziali di autenticazione	Le credenziali (userID/Password) possono essere sottratte al legittimo possessore con vari metodi, anche grazie alla negligenza nella conservazione da parte del possessore stesso.	Altri soggetti possono accedere alle banche dati protette con tali credenziali sostituendosi in tutto e per tutto al soggetto possessore delle stesse. Il sistema di protezione non può in principio sapere dell'occorrenza di tale furto.
E-002	Errore materiale	A causa di negligenza, scarsa conoscenza degli strumenti a disposizione o distrazione, gli addetti al trattamento possono compiere operazioni errate o specificare dati errati.	Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati.
E-003	Comportamenti illegali conseguenti a minacce su operatori	In conseguenza di pressioni di vario tipo (es. minacce, ricatti pressioni psicologiche) gli incaricati del trattamento possono compiere operazioni illecite sulla banca dati interessata l'evento.	Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito di dati.
E-004	Comportamenti sleali e/o fraudolenti	Con comportamento consapevole, derivate potenzialmente da vari fattori quali (risentimenti verso l'Ente, il perseguimento di fini personali, etc.) gli incaricati del trattamento possono compiere operazioni illecite sulla banca dati interessata l'evento.	Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito di dati.

Tabella 10: Eventi relativi a comportamento degli operatori

Codice evento	Nome evento	Descrizione evento	Impatto sulla sicurezza
E-005	Virus informatici	Sul sistema su cui si trova la banca dati interessata all'evento o il software utilizzato per accedervi, può essere venirsi ad installare o essere semplicemente eseguito del software spurio del tipo virus informatico.	Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito di dati.
E-006	Spamming	Il sistema di posta utilizzato dagli incaricati del trattamento potrebbe essere obiettivo di invii di posta spuria generata anche con strumenti automatizzati. Tali messaggi possono contenere false notizie.	Gli incaricati del trattamento possono erroneamente prendere in considerazione tali notizie ed operare interventi sulle banche dati non regolari.
E-007	Accesso da stazioni non autorizzate	Soggetti in possesso di credenziali di accesso al sistema, o intenzionati a sferrare un attacco informatico ad uno dei sistemi HW /SW da cui e possibile intervenite su una banca dato obiettivo, possono accedere al sistema individuato da una postazione non utilizzata in condizioni normali di operatività per accedere a tale sistema.	Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito di dati.
E-008	Intercettazione di informazioni transitanti sulla rete	Soggetti malintenzionati possono catturare, mediante vari sistemi fisici, parte delle informazioni che transitano sulla rete informatica dell'Ente. Ciò può avvenire in un qualunque tra il sistema utilizzato e il sistema HW /SW degli incaricati.	Nei casi più gravi, mediante varie tecniche, si può giungere alla distruzione o manipolazione dei dati. In generale si può avere una sottrazione di dati da parte dei malintenzionati.
E-009	Malfunzionamento apparecchiature	I sistemi HW/SW con i quali vengono manipolati i dati oggetto dell'evento da parte degli incaricati, possono avere malfunzionamenti da cui possono derivare azioni reali sui dati parzialmente o totalmente diverse da quelle che si volevano operare.	Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati.

Codice evento	Nome evento	Descrizione evento	Impatto sulla sicurezza
E-010	Degrado apparecchiature	I sistemi HW /SW con i quali vengono manipolati i dati oggetto dell'evento da parte degli incaricati, possono essere soggetti a degrado naturale conseguente all'uso o al solo funzionamento.Da ciò possono derivare azioni reali sui dati parzialmente o totalmente diverse da quelle che si volevano operare.	Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati.

Tabella 11: Eventi relativi agli strumenti

Codice evento	Nome evento	Descrizione evento	Impatto sulla sicurezza
E-011	Accesso non autorizzato a locali da cui si può accedere ai dati	Un soggetto autorizzato allo scopo, può comunque accedere fisicamente ai locali presso dai quali è accessibile e manipolabile la banca dati interessata all'evento.	Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito di dati.
E-012	Sottrazione di strumenti contenenti dati e/o programmi	I sistemi HW /SW e/o i supporti di memorizzazione, nei quali sono immagazzinati i dati relativi alla banca dati interessata all'evento, possono venire sottratti illecitamente da parte di altri soggetti non aventi diritto di accedere a tale banca dati.	L'evento comporta la sottrazione, in modo illecito, di dati.
E-013	Eventi distruttivi naturali/artificiali accidentali o volontari	I sistemi HW/SW e/o i supporti di memorizzazione, nei quali sono immagazzinati i dati relativi alla banca dati interessata all'evento, possono essere interessati da eventi distruttivi di origine sia fortuita che dolosa.	Dall'evento può derivare la distruzione totale o parziale della banca dati.

Codice evento	Nome evento	Descrizione evento	Impatto sulla sicurezza
E-014	Guasto ai sistemi complementari	I sistemi ausiliari necessari al corretto funzionamento degli apparati HW /SW con i quali viene trattata o che contiene la banca dati interessata all'evento possono avere malfunzionamenti in conseguenza di varie cause	Dall'evento può derivare la distruzione totale o parziale della banca dati.

Tabella 12: Eventi relativi al contesto

6 Misure in essere e da adottare

Nella Tabella 13 sono riportate, in forma sintetica, le misure in essere e da adottare per contrastare i rischi individuati nelle Tabelle 10, 11 e 12.

ID misura	**Descrizione sintetic**a	**Descrizione estesa**
M-001	Ingresso presidiato	I locali interessati alla misura sono dotati di servizio di portineria presidiata da personale addetto. Il personale addetto, mediante procedura di identificazione delle persone che accedono ai locali, può inibire l'accesso agli stessi. Tale inibizione di accesso può essere basata su fasce orarie nell'arco della giornata lavorativa.
M-002	Via di accesso dotata di inferriate o blindature	La via di accesso agli spazi interessati alla misura è dotata di protezione fisica tipo inferriate o blindature in grado di impedire o comunque rendere difficile l'ingresso agli stessi senza la disponibilità della relativa chiave.
M-003	Protezione con serratura	L'accessibilità agli spazi interessati alla misura è assoggettata alla utilizzazione di una apposita chiave disponibile solo per i soggetti appositamente autorizzati.
M-004	Armadi a pareti ignifughe	Per la protezione da danni derivanti da incendi viene utilizzato un tipo di armadio di contenimento con pareti in grado di resistere al fuoco ed alle alte temperature per un tempo sufficiente a porre in sicurezza i contenuti dello stesso prima del loro deterioramento.
M-005	Estintori	I locali/vani sono dotati di appositi estintori da utilizzarsi per l'estinzione delle fiamme in caso di incendio.
M-006	Gruppo statico di continuità (UPS)	Il carico elettrico da proteggere è alimentato attraverso un gruppo statico di continuità in grado di erogare, senza interruzione, la potenza elettrica necessaria per un tempo sufficiente a porre in sicurezza il carico stesso.
M-007	Linea elettrica dedicata	Al fine di eliminare interruzioni al carico da proteggere derivanti da problemi relativi al alti carichi. Questi viene alimentato con linea elettrica separata e dedicata dal quadro generale più vicino.
M-008	Climatizzazione	Il locale o vano oggetto della protezione è opportunamente climatizzato per poter assicurare il mantenimento di temperature operative compatibili durante tutto il periodo dell'anno.
M-009	Password condivisa di accesso alla stazione	L'accesso alla risorsa fisica in questione è assoggettato alla conoscenza di una password sufficientemente robusta e costituita da un segreto conosciuto da più persone abilitate all'accesso.
M-010	Password personale di accesso alla stazione	L'accesso alla risorsa fisica in questione è assoggettato alla conoscenza di una password sufficientemente robusta e costituita da un segreto conosciuto dalla sola persona a cui è stato affidato da parte dell'Amministratore del sistema.
M-011	Password condivisa di accesso alla procedura informatica	L'accesso alla procedura informatica in questione è assoggettato alla conoscenza di una password sufficientemente robusta e costituita da un segreto conosciuto da più persone abilitate all'accesso. La password viene sostituita con regolarità.

ID misura	Descrizione sintetica	Descrizione estesa
M-012	Password personale di accesso alla procedura informatica	L'accesso alla procedura informatica in questione è assoggettato alla conoscenza di una password sufficientemente robusta e costituita da un segreto conosciuto solo dalla sola persona a cui è stato affidato da parte dell'Amministratore del sistema.
M-013	Sistema di autorizzazione basato su profili	Il modulo software utilizzato per il trattamento dei dati oggetto della misura di protezione è basato su un sistema di profilazione dell'utenza che prevede di differenziare le possibili operazioni di trattamento eseguibili dai vari utenti in base al profilo/i specifico/i ad essi assegnati
M-014	Accesso mediante controllo dell'indirizzo di rete	L'accesso alla risorsa informatica dalla rete cui è connessa avviene mediante il controllo dell'indirizzo di rete della stazione accedente. L'accesso viene consentito solo se tale indirizzo appartiene ad una lista predefinita di stazioni
M-015	Logging	L'accesso alla risorsa informatica in questione è assoggettato a tracciature delle operazioni effettuate con la registrazione di: - epoca dell'operazione - indirizzo di rete della stazione accedente (se definito) - descrizione dell'operazione fatta - identificativo dell'utente che compie l'operazione Tali file di log sono accuratamente conservati per l'eventuale loro controllo
M-016	Crittografia	I dati sono crittografati mediante tecniche di cifratura adatte al livello di confidenzialità necessario in relazione alla natura dei dati in questione.
M-017	Backup	I dati o programmi in questione sono copiati con regolarità su supporti fisici diversi che sono poi conservati in locali separati opportunamente protetti da accessi non autorizzati.
M-018	Copie multiple	Le procedure di backup sono effettuate producendo copie multiple che sono poi conservate in locali diversi ciascuno soggetti ad opportune restrizioni di accesso.
M-019	Filtraggi del traffico di rete	Il traffico di rete che attraverso la risorsa informatica in questione è assoggettato ad opportuni controlli di congruità in termini di indirizzi e porte sorgenti e destinatarie sulla base di opportune tabelle (access list) pre-configurate in base al livello di protezione desiderato.
M-020	Cancellazione dei supporti fisici contenenti dati non più necessari	Il supporto fisico contenente i dati in questione che non risultano più necessari e quindi oggetto di protezione, viene cancellato mediante le opportune tecniche dipendenti dalla natura del supporto stesso. Tali operazioni di cancellazioni renderanno il contenuto di tale supporto non più leggibile con strumenti informatici di normale uso in ambito informatico.
M-021	Informazione/formazione specifica sul rischio	Gli incaricati del trattamento sulla banca oggetto della misura sono stati resi edotti, in modo specifico e puntuale, degli eventi dannosi relativi a quella banca dati e sulle misure adottate per contrastare il rischio derivante. Sono state poi date istruzioni operative dettagliate sul come rendere operative le misure di contrasto del rischio.

ID misura	Descrizione sintetica	Descrizione estesa
M-022	Antivirus	Sui sistemi interessati al trattamento dei dati in questione sono stati installati opportuni software di protezione dai virus informatici. Tali software sono costantemente aggiornati, in modo automatico, con frequenza almeno giornaliera. In certe situazioni il sistema provvede ad aggiornamenti più frequenti.
M-023	Black list per posta elettronica	Il sistema di smistamento della posta è stato configurato in modo da individuare siti mittenti che sono considerabili come emettitori di SPAM. Inoltre possono essere attivati, in caso di necessità, funzionalità di filtraggio del traffico in base a vari criteri.
M-024	Manutenzione Preventiva	Sui sistemi HW/SW oggetto della misura sono state attivate opportune azioni di manutenzione di tipo preventivo e pianificato al fine di poter prevenire il più possibile il manifestarsi dei guasti più ricorrenti ed evitare sospensioni di servizio conseguenti al verificarsi di tali guasti.
M-025	Manutenzione Correttiva	Sulle apparecchiature HW/SW interessate alla misura sono stati attivati contratti di manutenzione correttiva esterni ricorrendo alle ditte fornitrici degli stessi o a ditte specializzate. In alcuni casi sono state attivate gruppi interni specializzati in grado di risolvere i guasti in questione.
M-026	Modifica periodica delle credenziali	Le credenziali di accesso, quali password o certificati digitali, vengono rinnovate con una frequenza idonea a garantire le banche dati accedute da utilizzo delle stesse da parte di soggetti non autorizzati che abbino sottratto o generato, con opportune procedure di password-cracking, le stesse.
M-027	Utilizzazione di sistemi switch per realizzazione di reti Ethernet	La porzione di rete interessata alla misura è stata realizzata mediante la tecnologia switch invece di quella Hub per diminuire la probabilità di intercettazione delle informazioni transitanti in rete da parte di soggetti non autorizzati.
M-028	Firewall di secondo livello	La porzione di rete interessata alla misura è stata protetta mediante un apparato firewall per diminuire la probabilità di accesso alle informazioni da parte di soggetti non autorizzati.

Tabella 13: Misure per contrastare i rischi individuati.

7 Profili di Rischio

ID profilo	PR001	Descrizione sintetica	File server su sistemi localizzati presso il Centro Elaborazione Dati
Descrizione estesa			
Banche dati informatiche costituite da file di varia natura immagazzinati su directory di rete localizzate su una qualunque piattaforma installata presso la sala macchine del CED.			
Localizzazione ambienti		Sala server CED presso V. Milton 7, FIRENZE	
Condizioni ambientali		Sala macchine dedicata con sistema di sicurezza ed impianto di climatizzazione	
Misure sicurezza accessi		Locali non direttamente accessibili dall'esterno, sorveglianza della Reception. Porta metallica con chiusura a chiave e finestra con sbarre.	
Eventi applicabili		Misure corrispondenti adottate	
E-001		M-012, M-015	
E-002		M-013, M-015, M-017	
E-003		M-013, M-015	
E-004		M-015	
E-005		M-022	
E-006		M-022, M-023	
E-007		M-015, M-019	
E-008		M-027	
E-009		M-017, M-024, M-025	
E-010		M-025	
E-011		M-001, M-002, M-003, M-017	
E-012		M-001, M-002, M-003	
E-013		M-005, M-008, M-017, M-018	
E-014		M-006, M-007	

ID profilo	PR002	Descrizione sintetica	File server su sistemi localizzati sedi presidiate
Descrizione estesa			
Banche dati informatiche costituite da files di varia natura immagazzinati su directory di rete localizzate su una qualunque piattaforma installata presso una della sedi della ARS quali: uffici decentrati, sedi dipendenti a vario titolo. Nella sede è presente, all'ingresso, un servizio di custode o altro presidio.			
Localizzazione ambienti		Sala server CED presso V. Fabbricotti, FIRENZE	
Condizioni ambientali		Sala non necessariamente dedicata, con impianto elettrico apposito e sistemi di climatizzazione	
Misure sicurezza accessi		Locali non direttamente accessibili dall'esterno, presenza di personale.	
Eventi applicabili		Misure corrispondenti adottate	
E-001		M-012, M-015	
E-002		M-013, M-015, M-017	
E-003		M-013, M-015	
E-004		M-015	
E-005		M-022	
E-006		M-022, M-023	
E-007		M-015, M-019	
E-008		M-027	
E-009		M-017, M-024, M-025	
E-010		M-025	
E-011		M-001, M-002, M-017	
E-012		M-001, M-002	
E-013		M-005, M-008, M-017, M-018	
E-014		M-006, M-007	

ID profilo	PR003	Descrizione sintetica	Server scientifico di immagazzinamento dati
Descrizione estesa			
Banche dati informatiche costituite da database immagazzinati su piattaforma UNIX installata presso la sala macchine del CED.			
Localizzazione ambienti		Sala server CED presso V. Milton 7, FIRENZE	
Condizioni ambientali		Sala macchine dedicata con sistema di sicurezza ed impianto di climatizzazione	
Misure sicurezza accessi		Locali non direttamente accessibili dall'esterno, sorveglianza della Reception. Porta metallica con chiusura a chiave e finestra con sbarre.	
Eventi applicabili		Misure corrispondenti adottate	
E-001		M-012, M-015	
E-002		M-013, M-015, M-017	
E-003		M-013, M-015	
E-004		M-015	
E-005		M-022	
E-006		M-022, M-023	
E-007		M-015, M-019	
E-008		M-027	
E-009		M-017, M-024, M-025	
E-010		M-025	
E-011		M-001, M-002, M-003, M-017	
E-012		M-001, M-002, M-003	
E-013		M-005, M-008, M-017, M-018	
E-014		M-006, M-007	

ID profilo	PR004	Descrizione sintetica	Dati mantenuti in vario modo su PC stand alone in locali presidiati
Descrizione estesa			
I dati sono contenuti in file di varia natura e vengono acceduti con vari pacchetti software. Sia i dati che il software risultano risiedere sul personal computer dell'incaricato del trattamento. L'accesso ai dati avviene mediante la specifica di credenziali alle quali possono corrispondere o meno vari profili operativi caratterizzati da diritti di accesso/modifica a i dati differenziati. I locali sono presidiati.			
Localizzazione ambienti	Locale normalmente adibiti ad ufficio.		
Condizioni ambientali	Condizioni varie corrispondenti a quelle dell'ufficio in cui si trova il personal computer		
Misure sicurezza accessi	Locali non direttamente accessibili dall'esterno, presenza di personale.		
Eventi applicabili	Misure corrispondenti adottate		
E-001	M-012, M-015		
E-002	M-013, M-015		
E-003	M-013, M-015		
E-004	M-015		
E-005	M-022		
E-006	M-022, M-023		
E-007	M-015, M-019		
E-008	M-027		
E-009	M-024, M-025		
E-010	M-024, M-025		
E-011	M-001, M-002		
E-012	M-001, M-002		
E-013	M-005, M-008 M-018		
E-014	M-006, M-007		

ID profilo	PR005	Descrizione sintetica	Dati mantenuti su supporti cartacei.
Descrizione estesa			
I dati sono conservati all'interno di un armadio blindato o cassaforte nei locali di ARS. I locali sono presidiati. Le chiavi sono prese in consegna dagli incaricati.			
Localizzazione ambienti		Locale normalmente adibiti ad ufficio	
Condizioni ambientali		Condizioni varie corrispondenti a quelle dell'ufficio in cui si trovano i raccoglitori	
Misure sicurezza accessi		Locali non direttamente accessibili dall'esterno, presenza di personale.	
Eventi applicabili		Misure corrispondenti adottate	
E-002		M-013, M-015, M-017	
E-003		M-013, M-015	
E-004		M-015	
E-011		M-001, M-002, M-003, M-017	
E-012		M-001, M-002, M-003	
E-013		M-005, M-008, M-017, M-018	
E-014		M-006, M-007	

8 Piani formativi

Nel corso degli anni passati sono stati svolti interventi formativi agli incaricati ed ai responsabili dei trattamenti con il duplice obiettivo di diffondere la cultura del rispetto della privacy e fornire le informazioni per l'attuazione delle disposizioni di legge e l'applicazione delle regole di cui l'ARS si è dotata.

Nel 2009 continuerà l'attività del Gruppo Privacy di sostegno costante alle strutture per il consolidamento del sistema di riservatezza. Gli interventi formativi saranno rivolti sia agli incaricati al momento dell'ingresso in servizio, sia a quelli in servizio, nonché in occasione di cambiamenti di mansioni o di introduzione di nuovi strumenti rilevanti per il trattamento, relativamente a:

- rischi che incombono sui dati;
- misure disponibili per prevenire eventi dannosi;
- profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività;
- responsabilità che ne derivano;
- modalità per aggiornarsi sulle misure minime adottate dal Titolare.

I corsi e la costante attività di formazione vengono svolti dal Gruppo Privacy. In particolare la parte tecnica dei corsi viene svolta dai membri afferenti alle U.O. Sistemi informatici, Centro statistico Elaborazione Dati e Tecnologie dell'Informazione; la parte giuridica da quelli afferenti all'U.O. Personale e convenzioni.