SERVIZIO SANITARIO NAZIONALE – REGIONE SARDEGNA

Azienda U.S.L. n° 7

Carbonia

Deliberazione n. 325

1 APR. 2009

adottata dal Direttore Generale in data .....

Oggetto: "Codice in materia di protezione dei dati personali" art. 34 e Allegato B, regola 19, del d.lgs. 30 giugno 2003, n. 196 – Approvazione del Documento Programmatico sulla Sicurezza anno 2009.

Il Direttore Generale

Richiamata la precedente deliberazione n. 2380 del 11.12.2000 con la quale si era adottato un preliminare documento teso ad identificare le modalità di adozione delle misure minime di sicurezza per il trattamento dei dati personali secondo lo stato organizzativo e le dotazioni di sistemi informativi del periodo;

Richiamate le precedenti delibere n. 435 del 24/03/2007 e n. 374 del 10/04/2008, con le quali in ottemperanza al disposto normativo di cui al D.lgs. n. 196/2003 "Codice in materia di protezione dei dati personali", si era adottato il documento programmatico sulla sicurezza dei dati;

Richiamato il D.lgs. n. 196/2003 "Codice in materia di protezione dei dati personali" atto a garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dei soggetti interessati, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, e teso a disciplinare il trattamento dei dati personali al fine di assicurare un elevato livello di tutela dei diritti e delle libertà del cittadino nonché gli obblighi da parte dei titolari del trattamento;

Preso atto del disposto legislativo di cui al richiamato D.lgs. n. 196/2003, nonché del termine ultimo disposto al fine della adozione di un idoneo Documento Programmatico sulla Sicurezza da predisporsi con i contenuti di cui alla regola 19 riportata nell'Allegato B al suddetto D.lgs. n. 196/2003, documento tendente a regolamentare le modalità di trattamento dei dati personali con impiego di strumenti elettronici altrimenti non consentiti dal disposto legislativo di cui all'art. 24 del richiamato D.lgs. n. 196/2003;

Preso atto delle prescrizioni del Garante – art. 154, 1 c) del Codice – emanate il 09 novembre 2005, ed espressamente predisposte per regolamentare la condotta delle strutture sanitarie affinché, nell'ambito del trattamento dei dati personali, operino nel pieno rispetto della dignità delle persone, garantendo al cittadino che entra in contatto con le strutture sanitarie per diagnosi, cure, prestazioni mediche o operazioni amministrative, la più assoluta riservatezza ed il più ampio rispetto dei suoi diritti fondamentali e della sua dignità;

Vista la Deliberazione N. 19/1 del 12.05.2006 della Regione Autonoma della Sardegna ed il *Regolamento per il trattamento dei dati sensibili e giudiziari* ad essa allegato;

Considerato che la predisposizione ed adozione di un nuovo Documento Programmatico sulla Sicurezza costituisce per l'Azienda non solo puro adempimento legislativo, bensì anche occasione di revisione delle modalità organizzative e responsabilità connesse all'utilizzo dei sistemi informativi ed alla riservatezza, tutela e protezione dei dati raccolti ed elaborati con mezzi elettronici;

Visto il Documento Programmatico sulla Sicurezza per l'anno 2009 predisposto dal servizio Sistemi Informativi che si allega al presente atto deliberativo;

Preso atto che, per la quantità dei dati trattati da questa Azienda, e di cui ne è soggetto titolare, si rende opportuno identificare i singoli responsabili del trattamento nei Responsabili dei Servizi interessati al trattamento dei dati stessi per quanto di singola competenza;

Considerato che l'adozione delle specifiche misure minime di sicurezza richiede lo svolgimento di particolari attività formative per il personale, necessita di interventi di adeguamento ed integrazione dei sistemi informatici stessi finalizzati alla sicurezza, protezione dei dati, controllo e regolamentazione degli accessi e delle abilitazioni per gli utenti utilizzatori, il tutto come meglio richiamato nello specifico Piano di intervento per la sicurezza che accompagnava la stesura del Documento Programmatico sulla Sicurezza, anno 2007 e anno 2008;

Ritenuto opportuno destinare pertanto le necessarie risorse finanziarie per l'attuazione degli interventi necessari a garantire le misure di sicurezza, da adottare ad integrazione di quanto già in essere;

Sentiti il Direttore amministrativo e il Direttore sanitario;

DELIBERA

per i motivi esposti in premessa:

- DI APPROVARE il Documento Programmatico sulla Sicurezza predisposto dal servizio Sistemi Informativi ed allegato alla presente deliberazione;
- DI INCARICARE al Responsabile del servizio Sistemi Informativi di provvedere a periodica revisione, integrazione ed aggiornamento in relazione ai processi organizzativi aziendali, alla crescita del sistema informativo aziendale e alla disponibilità di nuove tecnologie a supporto della protezione e sicurezza dei dati;
- DI INDIVIDUARE le figure di Responsabili del trattamento dei dati nei Responsabili dei Servizi interessati al trattamento dei dati stessi per quanto di singola competenza.

Il Direttore Generale
Dr. Pietro Pasquale Chessa

DIR. AMM/

DIR. SAN/

RESP. Sistemi Informativi/

Il Responsabile del Servizio Affari Generali

Attesta che la deliberazione

N° 325 del - 1 APR. 2009

è stata pubblicata

nell'Albo pretorio dell'Azienda USL n° 7

a partire dal - 1 APR. 2009 al 16 APR. 2009

Resterà in pubblicazione per 15 giorni consecutivi

ed è stata posta a disposizione per la consultazione.

Il Responsabile del Servizio

Affari Generali

Allegati n° _____

Destinatari:

Collegio dei Sindaci

Serv. Sistemi Informativi

Servizio Bilancio

Servizio Acquisti

AZIENDA SANITARIA LOCALE N. 7

CARBONIA

Nome del Documento:	**Documento Programmatico per la Sicurezza Aggiornamento anno 2009**
Acronimo del Documento:	***DPS 2009***
Azienda:	**A.S.L. n. 7 - Carbonia**
Data di stesura:	20 Marzo 2009

Redazione

	Nome
Redatto da:	Andrea Alimonda

Registrazione modifiche al documento

Edizione	*Data*	*Descrizione*
V0.1	18.03.2009	Versione 0.1

Indice dei Contenuti

1 INTRODUZIONE

1.1 Generalità

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 allegato B del D.Lgs. 196/03", vista la Deliberazione N. 19/1 del 12.05.2006 della Regione Autonoma della Sardegna ed il *Regolamento per il trattamento dei dati sensibili e giudiziari* ad essa allegata.
Le citate disposizioni impongono la predisposizione e l'aggiornamento, con cadenza almeno annuale (entro il 31 marzo di ogni anno), di un Documento Programmatico sulla Sicurezza dei dati (DPS), 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:

1. l'elenco dei trattamenti di dati personali;
2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
3. l'analisi dei rischi che incombono sui dati;
4. 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;
5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
6. 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;
7. 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;
8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Tale documento deve essere obbligatoriamente predisposto nel caso di trattamento di dati sensibili o giudiziari. Questo è il caso della A.S.L. n. 7 di Carbonia che tratta, per la gestione delle incombenze di legge ed i servizi istituiti in favore della cittadinanza, una molteplicità di dati fra cui sicuramente dati definiti dalla normativa "sensibili", principalmente legati alle informazioni relative allo stato di salute dei pazienti.
Il presente documento dà conto di tutte le misure adottate in relazioni alla tipologia delle varie banche dati.

1.2 Strutturazione del documento

La specifica degli elementi che obbligatoriamente devono essere previsti nel DPS avverrà mediante la strutturazione del documento progettuale nelle seguenti sezioni:

1. censimento di tutti i trattamenti effettuati e delle banche dati costituite presso gli uffici dell'Azienda o in strutture esterne con la loro tipizzazione ai fine dell'individuazione di tutte le misure di sicurezza da adottare;

2. descrizione dell'organizzazione e delle strutture che fanno capo ai trattamenti e distribuzione dei compiti e delle responsabilità;
3. analisi dei rischi connessi alla gestione delle banche dati;
4. indicazione di un piano delle principali contromisure di controllo necessarie per i rischi individuati e delle attività di verifica della loro applicazione;
5. individuazione delle procedure seguite a tutela dei dati e dei programmi informatici, con particolare riferimento alle copie di sicurezza (backup) ed ai sistemi di ripristino (recovery);
6. un programma di informazione e formazione di tutti i soggetti interessati.

Laddove non indicato diversamente valgono le considerazioni e le indicazioni fornite nella precedente versione del DPS (anno 2008), di cui il presente documento costituisce l'integrazione e aggiornamento.
Per una migliore lettura del documento le sezioni principali contengono le informazioni essenziali, riportando nelle appendici gli aspetti e le descrizioni di dettaglio.

1.3 Passi seguiti per il censimento dei trattamenti

Partendo dalle rilevazioni effettuate nella precedente edizione del DPS (anno 2008), ed inoltre prendendo atto del Regolamento per il trattamento dei dati sensibili e giudiziari emanato ai sensi degli artt. 20- 21 D-Lgs. 196/2003 dalla Regione, che individua tutti i trattamenti effettuati dalle Aziende Sanitarie sono state aggiornate le informazioni con le variazioni intervenute, relativamente ai trattamenti in carico alle strutture.

In particolare si sono rilevate, per ciascuna banca dati, informazioni circa:

1. Il trattamento/i per il quale viene impiegata
2. la tipologia e natura dei dati trattati
3. i soggetti ai quali i dati si riferiscono
4. le operazioni di trattamento eseguite su di esse
5. le modalità di trattamento dei dati contenuti con varie tipologie di strumenti e mezzi
6. i soggetti interessati e le eventuali comunicazioni dei dati contenuti ad altri soggetti
7. l'eventuale diffusione dei dati
8. l'eventuale intervento di terzi nella manipolazione della banca dati
9. la correttezza comportamentale nel trattamento dei dati contenuti
10. i soggetti coinvolti, a vario titolo, nella manipolazione dei dati contenuti
11. le modalità di gestione delle copie dei dati (ove necessarie)
12. i trattamenti affidati all'esterno dell'Ente

Le informazioni non vogliono costituire, nell'ambito del presente documento, una immagine in tempo reale della realtà aziendale, cosa impossibile da ottenersi dato che molti aspetti organizzativi e di gestione evolvono nel tempo, bensì una "fotografia" della realtà informativa ed organizzativa della ASL che consente di individuare meglio i fattori di criticità in termini di rischio ed organizzare, se non presenti, le contromisure opportune.

1.4 Piani formativi

Nella sezione del DPS che tratta dell'informazione e formazione del personale interessato dal trattamento dei dati sono riportate tutte le informazioni necessarie ad individuare il quadro sintetico degli interventi formativi che si prevede di svolgere.
Si descrivono sinteticamente gli obiettivi e le modalità dell'intervento formativo, in relazione a quanto previsto dalla regola 19.6 dell'allegato B del D.lgs. 196 del 2003, si individuano le classi omogenee di incarico a cui l'intervento è destinato e/o le tipologie di incaricati interessati, anche in
riferimento alle strutture di appartenenza, si indicano poi anche i tempi previsti per lo svolgimento degli interventi formativi.

1.5 Relazione di accompagnamento al bilancio di esercizio

Il D.lgs n. 196 del 2003, per rendere meglio edotti gli organi di vertice del titolare del trattamento e responsabilizzarli in materia di sicurezza, prevede l'obbligo di riferire nella Relazione di accompagnamento di ciascun bilancio di esercizio l'avvenuta redazione o aggiornamento del DPS che sia obbligatorio come "misura minima" o che sia comunque adottato (regola 26 Allegato B).

2 TRATTAMENTI DEI DATI PERSONALI

2.1 Trattamenti interni

In questa sezione sono individuati i trattamenti effettuati dal titolare, direttamente o attraverso collaborazioni esterne, con l'indicazione della natura dei dati e della struttura (ufficio, funzione, ecc.) interna od esterna operativamente preposta, nonché degli strumenti elettronici impiegati.

Per ciascun trattamento vengono indicate le seguenti informazioni secondo il livello di sintesi determinato dal titolare:

Descrizione sintetica: finalità perseguita o attività svolta (es., fornitura di beni o servizi, gestione del personale, ecc.) e categorie di persone cui i dati si riferiscono (clienti o utenti, dipendenti e/o collaboratori, fornitori, ecc.).

Ad es. Servizio Acquisti - gestione pratiche amministrative su acquisizione di beni e servizi - richieste preventivi, dati ditte concorrenti, espletamento gare, contratti e deliberazioni-certificazioni antimafia e comunicazioni verso prefettura e altri enti.

Natura dei dati trattati: dati personali comuni, sensibili o giudiziari.

Struttura di riferimento e/o altre strutture che concorrono al trattamento: struttura (ufficio, funzione, ecc.) all'interno della quale viene effettuato il trattamento. In caso di strutture complesse si è indicata la macro-struttura (direzione, dipartimento o servizio del personale), oppure gli uffici specifici all'interno della stessa (ufficio contratti, sviluppo risorse, controversie sindacali, amministrazione-contabilità.) .

Ad es. Servizio Bilancio, Acquisti e magazzino.

Descrizione degli strumenti elettronici utilizzati: elaboratori o p.c. anche portatili, collegati o meno in una rete locale, geografica o Internet; sistemi informativi più complessi.

Banche dati ed archivi cartacei: archivio cartaceo o banca dati con le relative applicazioni, in cui sono contenuti i dati. Se il trattamento richiede l'utilizzo di dati che risiedono in più di una banca dati è indicata la specificazione delle stesse.

Luogo di custodia dei supporti di memorizzazione: luogo in cui risiedono fisicamente i dati, ovvero dove si trovano (in quale sede, centrale o periferica, o presso quale fornitore di servizi, ecc.) gli elaboratori sui cui dischi sono memorizzati i dati, i luoghi di conservazione dei supporti magnetici utilizzati per le copie di sicurezza (nastri, CD, ecc.) ed ogni altro supporto rimovibile.

Tipologia di dispositivi di accesso: elenco e descrizione sintetica degli strumenti utilizzati dagli incaricati per effettuare il trattamento: pc, terminale non intelligente, palmare, telefonino, ecc.

Tipologia di interconnessione: descrizione sintetica e qualitativa della rete che collega i dispositivi d'accesso ai dati utilizzati dagli incaricati: rete locale, geografica, Internet, ecc.

Ai fini della descrizione delle classi di trattamento si fa riferimento alla classificazione adottata nel precedente documento programmatico per la sicurezza per l'anno 2006, ed in particolare la tabella **Elenco dei trattamenti di dati personali (Regola 19.1)** che viene riportata nel seguito.

2.1.1 Elenco dei trattamenti di competenza della ASL

Si riporta nel seguito l'elenco dei trattamenti di competenza della ASL. Il dettaglio di ogni singolo trattamento è riportato nelle schede numerate da SC 01 a SC 41 allegate al presente documento.

Numerazione	Nome scheda
1	TUTELA DAI RISCHI INFORTUNISTICI E SANITARI CONNESSI CON GLI AMBIENTI DI VITA E DI LAVORO
2	SORVEGLIANZA EPIDEMIOLOGICA DELLE MALATTIE INFETTIVE E DIFFUSIVE E DELLE TOSSINFEZIONI ALIMENTARI
3	VACCINAZIONI E VERIFICA ASSOLVIMENTO OBBLIGO VACCINALE
4	PROGRAMMI DI DIAGNOSI PRECOCE
5	ATTIVITÀ FISICA E SPORTIVA
6	GESTIONE ATTIVITÀ SOCIOSANITARIA A FAVORE DI FASCE DEBOLI DI POPOLAZIONE
7	MEDICINA DI BASE - PEDIATRIA DI LIBERA SCELTA - CONTINUITÀ ASSISTENZIALE (GUARDIA MEDICA NOTTURNA E FESTIVA, GUARDIA TURISTICA)
8	ASSISTENZA SANITARIA DI BASE: RICONOSCIMENTO DEL DIRITTO ALL'ESENZIONE PER PATOLOGIA/INVALIDITÀ/REDDITO E GESTIONE ARCHIVIO ESENTI
9	ASSISTENZA SANITARIA DI BASE: ASSISTENZA SANITARIA IN FORMA INDIRETTA
10	ASSISTENZA SANITARIA DI BASE: CURE ALL'ESTERO
11	ASSISTENZA SANITARIA DI BASE: ASSISTENZA AGLI STRANIERI IN ITALIA (PARTICOLARI CATEGORIE)
12	ASSISTENZA INTEGRATIVA (FORNITURA DI PRODOTTI DIETETICI A CATEGORIE PARTICOLARI E DI PRESIDI SANITARI A SOGGETTI AFFETTI DA DIABETE MELLITO).
13	ASSISTENZA PROTESICA
14	ASSISTENZA DOMICILIARE PROGRAMMATA E INTEGRATA
15	ATTIVITÀ DI ASSISTENZA RIABILITATIVA RESIDENZIALE E SEMIRESIDENZIALE AD ANZIANI NON AUTOSUFFICIENTI, DISABILI PSICHICI E SENSORIALI E MALATI TERMINALI
16	ASSISTENZA TERMALE
17	ATTIVITÀ AMMINISTRATIVA, PROGRAMMATORIA, GESTIONALE E DI VALUTAZIONE RELATIVA ALLA ASSISTENZA IN REGIME DI RICOVERO OSPEDALIERO E DOMICILIARE
18	ATTIVITÀ AMMINISTRATIVA, PROGRAMMATORIA, GESTIONALE E DI VALUTAZIONE CONCERNENTE L'ATTIVITÀ IMMUNO-TRASFUSIONALE
19	ATTIVITA' AMMINISTRATIVA, PROGRAMMATORIA, GESTIONALE E DI VALUTAZIONE CONCERNENTE IL TRAPIANTO D'ORGANI.
20	SOCCORSO SANITARIO DI EMERGENZA/URGENZA SISTEMA "118". ASSISTENZA SANITARIA DI EMERGENZA
21	ASSISTENZA SPECIALISTICA AMBULATORIALE E RIABILITAZIONE
22	PROMOZIONE E TUTELA DELLA SALUTE MENTALE
23	DIPENDENZE (TOSSICODIPENDENZE E ALCOODIPENDENZE)

24	ASSISTENZA SOCIO-SANITARIA PER LA TUTELA DELLA SALUTE MATERNO-INFANTILE ED ESITI DELLA GRAVIDANZA
25	ASSISTENZA FARMACEUTICA TERRITORIALE E OSPEDALIERA
26	SPERIMENTAZIONE CLINICA DEI MEDICINALI
27	FARMACOVIGILANZA E RILEVAZIONI REAZIONI AVVERSE A VACCINO
28	EROGAZIONE A TOTALE CARICO DEL SERVIZIO SANITARIO NAZIONALE, QUALORA NON VI SIA ALTERNATIVA TERAPEUTICA VALIDA, DI MEDICINALI INSERITI IN APPOSITO ELENCO PREDISPOSTO DALLA COMMISSIONE UNICA DEL FARMACO
29	ASSISTENZA A FAVORE DELLE CATEGORIE PROTETTE (MORBO DI HANSEN)
30	ATTIVITÀ AMMINISTRATIVA, PROGRAMMATORIA, GESTIONALE E DI VALUTAZIONE CONCERNENTE L'ASSISTENZA AI NEFROPATICI CRONICI IN TRATTAMENTO DIALITICO
31	ATTIVITÀ MEDICO - LEGALE INERENTE L'ISTRUTTORIA DELLE RICHIESTE DI INDENNIZZO PER DANNI DA VACCINAZIONI OBBLIGATORIE, TRASFUSIONI E SOMMINISTRAZIONE DI EMODERIVATI
32	ATTIVITÀ MEDICO - LEGALE INERENTE GLI ACCERTAMENTI FINALIZZATI AL SOSTEGNO DELLE FASCE DEBOLI (RICONOSCIMENTO DELLO STATO DI INVALIDITÀ CIVILE, CECITÀ CIVILE, SORDOMUTISMO, DELLA CONDIZIONE DI HANDICAP, ACCERTAMENTI PER IL COLLOCAMENTO MIRATO AL LAVORO DELLE PERSONE DISABILI)
33	ATTIVITÀ MEDICO - LEGALE INERENTE L'ACCERTAMENTO DELL'IDONEITÀ IN AMBITO DI DIRITTO AL LAVORO (ASSUNZIONE NEL PUBBLICO IMPIEGO; IDONEITÀ ALLO SVOLGIMENTO DI MANSIONI LAVORATIVE; CONTROLLO DELLO STATO DI MALATTIA DI DIPENDENTI PUBBLICI E PRIVATI)
34	ATTIVITÀ MEDICO - LEGALE INERENTE L'ACCERTAMENTO DELL'IDONEITÀ AL PORTO D'ARMI, AI FINI DELLA SICUREZZA SOCIALE
35	ATTIVITÀ MEDICO - LEGALE INERENTE L'ACCERTAMENTO DELL'IDONEITÀ ALLA GUIDA, AI FINI DELLA SICUREZZA SOCIALE
36	CONSULENZE E PARERI MEDICO-LEGALI IN TEMA DI RICONOSCIMENTO DELLA DIPENDENZA DA CAUSA DI SERVIZIO
37	CONSULENZE E PARERI MEDICO-LEGALI IN TEMA DI IPOTESI DI RESPONSABILITÀ PROFESSIONALE SANITARIA, DI SUPPORTO ALL'ATTIVITÀ DI GESTIONE DEL RISCHIO CLINICO, INFORMAZIONE E CONSENSO AI TRATTAMENTI SANITARI
38	ATTIVITÀ MEDICO - LEGALE IN AMBITO NECROSCOPICO
39	ATTIVITÀ DI PROGRAMMAZIONE, GESTIONE, CONTROLLO E VALUTAZIONE DELL'ASSISTENZA SANITARIA
40	GESTIONE E VERIFICA SULL'ATTIVITÀ SPECIALISTICA E DI RICOVERO DELEGATA ALLE STRUTTURE ACCREDITATE
41	VIDEOSORVEGLIANZA CON FINALITÀ DI SICUREZZA E PROTEZIONE DI BENI E PERSONE

2.1.2 Trattamenti con strumenti elettronici

Rif. **AA1**		*Denominazione:* **Anagrafe Assistiti**
Descrizione sintetica:		Raccoglie i dati identificativi della popolazione assistita e dei medici di base; il trattamento dei dati è inerente le operazioni di attribuzione, scelta e revoca del medico di base oltre che per la gestione delle esenzioni
Caratteristiche e natura del dato:		Si tratta generalmente di trattamento di dati anagrafici associati ad eventuali dati di carattere sanitario connessi alla applicazione delle esenzioni ticket. Sono dunque compresi dati sensibili
Struttura incaricata al trattamento:		Servizio Medicina di Base - I dati sono trattati dai due Distretti Sanitari di Carbonia e Iglesias
Altri incaricati al trattamento:		Servizio Sistemi informativi a riguardo delle attività di gestione dell'ambiente applicativo, di copia dei dati oltre che di elaborazioni connesse alla integrazione della banca dati con altri ambienti applicativi in uso nel complesso sistema informativo aziendale
Strumenti informatici utilizzati	*Hardware:*	Server applicativo in ambiente Microsoft Windows Server configurato con dischi in configurazione RAID e dotato di dispositivo per l'esecuzione delle copie di backup (Masterizzatore)
	Software:	Applicativo "Vitruvio" - "Anagrafe Assistiti" fornito da Daeduls Datamat S.p.A.
	Database:	Database relazionale in ambiente Oracle
Collegamenti LAN e telematici		L'applicativo è reso disponibile in rete locale ed è accessibile anche tramite i collegamenti remoti supportati dall'architettura di rete aziendale
Dispositivi di accesso del dato:		A livello applicativo tramite normale personal computer collegato in rete ed interfaccia grafica web-based. A livello di gestione con accesso diretto al server dislocato presso il CED del Servizio Sistemi Informativi. Accessibilità al database anche tramite modalità OLE, ODBC e DDE in funzione delle caratteristiche del database Oracle utilizzato
Modalità di accesso al dato:		Accesso a livello applicativo regolamentato da Identificativo Utente e Password. Accesso a livello di gestione ed amministrazione del database regolamentato da Identificativo Utente e Password.
Modalità di protezione del dato:		Accesso non consentito senza specifica identificazione utente e differenziazione dei profili di accesso
Modalità di conservazione del dato:		Memorizzazione corrente su archivio database su disco fisso gestito in configurazione ridondante RAID e in formattazione NTFS; posizionamento dell'archivio esclusivamente sul server applicativo senza distribuzione di copie (o copie parziali di dati) presso le postazioni periferiche. Aggiornamento in tempo reale in linea sul server applicativo;
Modalità di esecuzione delle copie:		Procedura automatica di backup eseguita giornalmente. Esecuzione mensile di backup operato manualmente e salvataggio su CD-Rom masterizzato
Modalità di custodia delle copie:		Supporti CD-ROM di copia conservati in cassaforte dotata di serratura di sicurezza e protezione ignifuga

Rif. **RO1**	*Denominazione:* **Flussi Informativi - Dati ricoveri ospedalieri - SDO e DRG**
Descrizione sintetica:	Raccoglie i dati relativi ai ricoveri presso i Presidi Ospedalieri Aziendali e relativi agli istituti di ricovero di altre strutture sanitarie. Vengono gestiti i dati anagrafici della popolazione assistiti correlati alle patologie e ai dati delle procedure sanitarie di ricovero o applicazione. I dati vengono raccolti ed elaborati per funzioni di controllo e monitoraggio e sono periodicamente inviati presso l'Assessorato regionale della Sanità
Caratteristiche e natura del dato:	Si tratta di dati anagrafici e dati sensibili
Struttura incaricata al trattamento:	Le singole Divisioni e Reparti di Ricovero
Altri incaricati al trattamento:	Servizio Sistemi informativi a riguardo delle attività di gestione dell'ambiente applicativo, di copia dei dati oltre che di elaborazioni connesse alla integrazione della banca dati, elaborazioni statistiche, produzione di report ed invio all'Assessorato regionale competente
Strumenti informatici utilizzati — *Hardware:*	Singole postazioni di racolta dei dati presso le Divisioni ed i Reparti; postazione server centrale di consolidamento ed elaborazione dei dati globali presso il CED Servizi Informativi
Software:	Applicativo sviluppato internamente alla struttura Sistemi Informativi in Visual Basic interfacciato con Grouper della 3M per la elaborazione del DRG
Database:	Database relazionale in ambiente Microsoft Access
Collegamenti LAN e telematici	L'applicativo opera su postazione singola con eventuale attività di LAN per il solo trasferimento e copia degli archivi
Dispositivi di accesso del dato:	A livello applicativo tramite normale personal computer ed interfaccia applicativa proprietaria. A livello di gestione con accesso tramite apposito applicativo di gestione ed elaborazione accessibile con solo profilo di amministratore.
Modalità di accesso al dato:	Protezione all'accesso locale al dato solo tramite utente e password di accesso al sistema operativo della postazione di lavoro
Modalità di protezione del dato:	Fornita dal solo sistema operativo; conservazione per almeno 6 mesi del log delle operazioni effettuate
Modalità di conservazione del dato:	Dati in linea ed aggiornamento in tempo reale sulla postazione di lavoro utente utilizzata; copia dei dati di archivio eseguita periodicamente e trasmessa su supporto di memorizzazione.
Modalità di esecuzione delle copie:	Con periodicità trimestrale operata dall'incaricato del CED sulla singola postazione di lavoro; accorpamento dei dati ed esecuzione del backup completo dell'intero database con memorizzazione su CD-ROM ed estrazione dati di copia con invio all'Assessorato regionale
Modalità di custodia delle copie:	Supporti CD-ROM di copia conservati in cassaforte dotata di serratura di sicurezza e protezione ignifuga

Rif. **AS1**	*Denominazione:* **Attività Specialistica**
Descrizione sintetica:	Raccoglie i dati relativi ai ricoveri presso i Presidi Ospedalieri Aziendali, strutture Sanitarie territoriali ASL e convenzionate. Vengono gestiti i dati anagrafici della popolazione assistiti correlati alle patologie e ai dati delle procedure sanitarie di attività specialistica o applicazione. I dati vengono raccolti ed elaborati per funzioni di controllo e monitoraggio e sono periodicamente inviati presso l'Assessorato regionale della Sanità
Caratteristiche e natura del dato:	Si tratta di dati anagrafici e dati sensibili
Struttura incaricata al trattamento:	Le singole Divisioni e Reparti Specialistici, strutture esterne convenzionate, ed altre strutture specialistiche territoriali della ASL
Altri incaricati al trattamento:	Servizio Sistemi informativi a riguardo delle attività di gestione dell'ambiente applicativo, di copia dei dati oltre che di elaborazioni connesse alla integrazione della banca dati, elaborazioni statistiche, produzioni di report ed invio all'Assessorato regionale competente
Strumenti informatici utilizzati — *Hardware:*	Singole postazioni di raccolta dei dati presso le Divisioni ed i Reparti e le varie struttura interessate; postazione server centrale di consolidamento ed elaborazione dei dati globali presso il CED Servizi Informativi
Software:	Applicativo sviluppato in ambiente Microsoft Access; modulo OASIS ambulatori
Database:	Database relazionale in ambiente Microsoft Access; Database Oracle
Collegamenti LAN e telematici	L'applicativo opera su postazione singola; trasferimento dei dati operato manualmente con copie su supporti di memorizzazione
Dispositivi di accesso del dato:	A livello applicativo tramite normale personal computer ed interfaccia applicativa proprietaria. A livello di gestione con accesso tramite apposito applicativo di gestione ed elaborazione accessibile con profilo di amministratore.
Modalità di accesso al dato:	Protezione all'accesso locale al dato tramite codice utente e password di accesso al sistema operativo della postazione di lavoro
Modalità di protezione del dato:	Fornita dal solo sistema operativo; conservazione per almeno 6 mesi del log delle operazioni effettuate.
Modalità di conservazione del dato:	Dati in linea ed aggiornamento in tempo reale sulla postazione di lavoro utente utilizzata; copia dei dati di archivio eseguita periodicamente e trasmessa su supporto di memorizzazione.
Modalità di esecuzione delle copie:	Con periodicità mensile con esecuzione da parte degli incaricati sulla singola postazione di lavoro e trasmissione al CED; accorpamento dei dati ed esecuzione del backup completo dell'intero database con memorizzazione su CD-ROM ed estrazione dati di copia con invio all'Assessorato regionale
Modalità di custodia delle copie:	Supporti CD-ROM di copia conservati in cassaforte dotata di serratura di sicurezza e protezione ignifuga

Rif. **CA1**	*Denominazione:* **CEDAP Certificati di Assistenza al Parto**
Descrizione sintetica:	Raccoglie i dati relativi alle certificazioni di assistenza al parto al fine del monitoraggio delle criticità
Caratteristiche e natura del dato:	Si tratta di dati di carattere sanitario relativi ai reparti di ostetricia e ginecologia che sono associati alla popolazione assistita per il tramite della codifica relativa all'identificativo di ricovero della paziente
Struttura incaricata al trattamento:	Le singole Divisioni e Reparti di Ostetricia e Ginecologia che operano a livello di raccolta cartacea dei dati
Altri incaricati al trattamento:	Servizio Sistemi informativi a riguardo delle attività di data-entry e gestione dell'ambiente applicativo, di copia dei dati oltre che di elaborazioni connesse alla integrazione della banca dati, elaborazioni statistiche, produzioni di report ed invio all'Assessorato regionale competente
Strumenti informatici utilizzati *Hardware:*	Singole postazioni di raccolta dei dati presso le Divisioni ed i Reparti e le varie struttura interessate; postazione server centrale di consolidamento ed elaborazione dei dati globali presso il CED Servizi Informativi
Software:	Applicativo sviluppato in ambiente Microsoft Access
Database:	Database relazionale in ambiente Microsoft Access
Collegamenti LAN e telematici	L'applicativo opera su postazione singola; trasferimento dei dati operato manualmente con copie su supporti di memorizzazione
Dispositivi di accesso del dato:	A livello applicativo tramite normale personal computer ed interfaccia applicativa proprietaria. A livello di gestione con accesso tramite apposito applicativo di gestione ed elaborazione accessibile con profilo di amministratore.
Modalità di accesso al dato:	Protezione all'accesso locale al dato solo tramite utente e password di accesso al sistema operativo della postazione di lavoro
Modalità di protezione del dato:	Fornita dal sistema operativo
Modalità di conservazione del dato:	Dati in linea ed aggiornamento in tempo reale sulla postazione di lavoro utente utilizzata; copia dei dati di archivio eseguita periodicamente e trasmessa su supporto di memorizzazione.
Modalità di esecuzione delle copie:	Con periodicità trimestrale con esecuzione da parte degli incaricati sulla singola postazione di lavoro e trasmissione al CED; accorpamento dei dati ed esecuzione del backup completo dell'intero database con memorizzazione su CD-ROM ed estrazione dati di copia con invio all'Assessorato regionale
Modalità di custodia delle copie:	Supporti CD-ROM di copia conservati in cassaforte dotata di serratura di sicurezza e protezione ignifuga

Rif. **CP1**		*Denominazione:* **CUP - Centro Unificato di Prenotazione**
Descrizione sintetica:		Raccoglie i dati relativi alla popolazione assistita correlati alla prenotazione di prestazioni ambulatoriali e di ricovero.
Caratteristiche e natura del dato:		Si tratta di dati anagrafici e dati sensibili
Struttura incaricata al trattamento:		Il Centro Unificato di Prenotazione con relativo responsabile e strutture operanti presso i distretti
Altri incaricati al trattamento:		RTI composta da Engineering Sanità Enti Locali SpA e Telecom Italia SpA Servizio Sistemi informativi a riguardo delle attività di gestione dell'ambiente applicativo, di copia dei dati oltre che di elaborazioni connesse alla integrazione della banca dati, elaborazioni statistiche, produzioni di report ed invio all'Assessorato regionale competente
Strumenti informatici utilizzati	*Hardware:*	Server centralizzato presso il CRESSAN (Centro Regionale per i Servizi Sanitari)
	Software:	Ambiente applicativo SGP sviluppato dalla RTI
	Database:	Database relazionale in ambiente Oracle
Collegamenti LAN e telematici		L'applicativo opera in modalità client-server con server centralizzato e funzionalità client accessibili via rete LAN locale e collegamento RTR verso il CRESSAN
Dispositivi di accesso del dato:		Tramite personal computer collegato in LAN dotato di interfaccia applicativa e specifica personalizzazione
Modalità di accesso al dato:		Protetto da identificativo Utente e password tramite interfaccia applicativa; possibilità di accesso agli archivi centralizzati via funzionalità e controlli di protezione del database Oracle
Modalità di protezione del dato:		Utente e password con definizione di diversi profili di accesso;
Modalità di conservazione del dato:		Dati in linea aggiornati in tempo reale su cluster di server applicativo; copia in tempo reale grazie alla funzionalità RAID.
Modalità di esecuzione delle copie:		Esecuzione automatica programmata delle copie di backup su nastro con periodicità giornaliera. La piattaforma utilizzata per il controllo della libreria di nastri è SUN StorEdge Enterprise Backup Software
Modalità di custodia delle copie:		

Rif. **LA1**	*Denominazione:* **Laboratorio Analisi**
Descrizione sintetica:	Raccoglie i dati relativi alla popolazione assistita correlati alle patologie di esenzione e le relative procedure prescritte.
Caratteristiche e natura del dato:	Si tratta di dati anagrafici e dati sensibili
Struttura incaricata al trattamento:	Il Servizio Laboratori di Analisi con trattamento differenziato (in via provvisoria) da parte della sede di Carbonia e di Iglesias
Altri incaricati al trattamento:	Il Servizio Sistemi Informativi, per ciò che riguarda l'effettuazione di copie di sicurezza e la manutenzione ordinaria sul server applicativo
Strumenti informatici utilizzati — *Hardware:*	Due server in ambiente Windows NT Server 2000, ciascuno dotato di unità di masterizzazione CD-ROM per backup dei dati
Strumenti informatici utilizzati — *Software:*	Dianoema fornito da Krenesiel S.p.A. che ne cura i servizi di assistenza e manutenzione
Strumenti informatici utilizzati — *Database:*	Database relazionale in ambiente Oracle
Collegamenti LAN e telematici	L'applicativo opera in modalità client-server con server centralizzato e funzionalità client accessibili via rete LAN locale e collegamenti remoti
Dispositivi di accesso del dato:	Tramite personal computer collegato in LAN dotato di interfaccia applicativa e specifica personalizzazione
Modalità di accesso al dato:	Protetto da identificativo Utente e password tramite interfaccia applicativa; possibilità di accesso agli archivi centralizzati via funzionalità e controlli di protezione del database Oracle
Modalità di protezione del dato:	Utente e password con definizione di diversi profili di accesso
Modalità di conservazione del dato:	Dati in linea aggiornati in tempo reale su ciascun server applicativo e vengono attualmente tenuti separati per la gestione dei due laboratori di Carbonia e Iglesias;
Modalità di esecuzione delle copie:	Esecuzione delle copie gestita manualmente a cura dell'operatore utente di Carbonia con riversamento su supporto CD-rom con periodicità settimanale; Backup giornaliero su diversa macchina e backup settimanale su DVD per istanza laboratorio di Iglesias
Modalità di custodia delle copie:	Supporti di memorizzazione su CD-ROM e DVD conservati dal singolo laboratorio di Carbonia e dal CED di Iglesias per quanto relativo a ciascuna struttura.

Rif. **CT1**		*Denominazione:* **Centri Trasfusionali**
Descrizione sintetica:		Raccoglie i dati relativi ai donatori di sangue ed ai riceventi
Caratteristiche e natura del dato:		Si tratta di dati anagrafici e dati sensibili
Struttura incaricata al trattamento:		Il Servizio Centri Trasfusionali
Altri incaricati al trattamento:		Il Servizio Sistemi Informativi opera esclusivamente la manutenzione ordinaria sul server applicativo
Strumenti informatici utilizzati	*Hardware:*	Server RISC IBM dotato di sistema operativo Unix AIX, dischi in configurazione RAID ed unità nastro per backup
	Software:	Emonet fornito da Krenesiel S.p.A. che ne cura i servizi di assistenza e manutenzione
	Database:	Database relazionale in ambiente Oracle
Collegamenti LAN e telematici		L'applicativo opera in modalità client-server con server centralizzato e funzionalità client accessibili via rete LAN locale e collegamenti remoti
Dispositivi di accesso del dato:		Tramite personal computer collegato in LAN dotato di interfaccia applicativa e specifica personalizzazione
Modalità di accesso al dato:		Protetto da identificativo Utente e password tramite interfaccia applicativa; possibilità di accesso agli archivi centralizzati via funzionalità e controlli di protezione del database Oracle
Modalità di protezione del dato:		Utente e password con definizione di diversi profili di accesso personalizzabili, ma attualmente non differenziati
Modalità di conservazione del dato:		Dati in linea aggiornati in tempo reale sul server applicativo; copia in tempo reale grazie alla funzionalità RAID.
Modalità di esecuzione delle copie:		Esecuzione automatica programmata delle copie di backup su nastro con periodicità giornaliera dell'intero database
Modalità di custodia delle copie:		Supporti di memorizzazione su nastro conservati in cassaforte dotata di serratura di sicurezza e protezione ignifuga

Rif. **DB1**	*Denominazione:* **Diabetologia**
Descrizione sintetica:	Raccoglie i dati relativi ai pazienti diabetici del territorio
Caratteristiche e natura del dato:	Si tratta di dati anagrafici e dati sensibili
Struttura incaricata al trattamento:	Il Servizio Diabetologico
Altri incaricati al trattamento:	Il Servizio Sistemi Informativi opera esclusivamente la manutenzione ordinaria sul server applicativo
Strumenti informatici utilizzati — *Hardware:*	Server su piattaforma Microsoft 2000 Server per il Distretto di Iglesias Personal computer con funzioni di server per il Distretto di Carbonia
Software:	Diabwin fornito da PentaSys Sistemi di Firenze per il Distretto di Iglesias Applicativo fornito da LifeScan di Torino per il Distretto di Carbonia
Database:	Database relazionale sviluppato in ambiente Borland Delphi per il Distretto di Iglesias Database relazionale SQL Server per il Distretto di Carbonia
Collegamenti LAN e telematici	L'applicativo opera in modalità client-server con server centralizzato e funzionalità client accessibili via rete LAN locale e collegamenti remoti
Dispositivi di accesso del dato:	Tramite personal computer collegato in LAN dotato di interfaccia applicativa e specifica personalizzazione
Modalità di accesso al dato:	Protetto da identificativo Utente e password tramite interfaccia applicativa; possibilità di accesso agli archivi centralizzati del database su server
Modalità di protezione del dato:	Utente e password con definizione di profilo unico di autorizzazione (possibilità prevista di personalizzazione per diverse tipologie di profilo utente)
Modalità di conservazione del dato:	Dati in linea aggiornati in tempo reale sul server applicativo
Modalità di esecuzione delle copie:	Esecuzione manuale della copia su CD-ROM eseguita dall'utente operatore con periodicità mensile per entrambi i distretti
Modalità di custodia delle copie:	Supporti di memorizzazione su CD-ROM conservati in armadio presso la struttura incaricata al trattamento

Rif. **SCR**	*Denominazione:* **Screening Oncologico**
Descrizione sintetica:	Possiede l'anagrafica della popolazione maschile e femminile del territorio della Asl7 utilizzandalola per l'analisi di prevenzione sullo screening del collo uterino, mammografico e del colon retto.
Caratteristiche e natura del dato:	Si tratta di dati anagrafici e dati sensibili
Struttura incaricata al trattamento:	Ostetricia e Ginecologia, Consultori territoriali.
Altri incaricati al trattamento:	Il Servizio Sistemi Informativi opera la gestione dell'intero sistema a riguardo del collegamento dei diversi operatori.
Strumenti informatici utilizzati — *Hardware:*	Rilevatori di presenza presso le strutture aziendali a badge magnetico e server centralizzato in ambiente Microsoft Windows NT Server
Software:	Screening gestito da elettronica professionale
Database:	Microsoft SQL server 2005
Collegamenti LAN e telematici	L'accesso applicativo avviene tramite PC in modalità da postazione singola interconnessa in rete LAN locale e remota con accesso al server centralizzato
Dispositivi di accesso del dato:	Tramite personal computer collegato in LAN; dotato di interfaccia applicativa e specifica personalizzazione
Modalità di accesso al dato:	Protetto da identificativo Utente e password tramite interfaccia applicativa con accesso controllato agli archivi centralizzati del database su server
Modalità di protezione del dato:	Utente e password con definizione di differenti profili di autorizzazione
Modalità di conservazione del dato:	Dati in linea direttamente su server applicativo e database server; configurazione in mirroring dei dischi per l'archivio su server
Modalità di custodia delle copie:	Locale protetto sistema di sorveglianza remota e porta blindata.

Rif. **RP1**		*Denominazione:* **Gestione Rilevazione Presenze**
Descrizione sintetica:		Gestisce i dati del personale, le presenze ed orari di lavoro, ferie e dati connessi alle giustificazioni
Caratteristiche e natura del dato:		Si tratta di dati anagrafici e dati sensibili
Struttura incaricata al trattamento:		Il Servizio del Personale
Altri incaricati al trattamento:		Il Servizio Sistemi Informativi opera la gestione dell'intero sistema a riguardo del collegamento dei rilevatori e la gestione applicativa del server
Strumenti informatici utilizzati	*Hardware:*	Rilevatori di presenza presso le strutture aziendali a badge magnetico e server centralizzato in ambiente Microsoft Windows NT Server
	Software:	IRIS Win fornito dalla Mondo EDP di Cuneo
	Database:	Database Oracle
Collegamenti LAN e telematici		L'applicativo opera la raccolta dati tramite rilevatori a badge magnetico, il consolidamento tramite server e l'accesso applicativo tramite PC in modalità da postazione singola interconnessa in rete LAN locale e remota con le restanti postazioni operative presso le strutture locali
Dispositivi di accesso del dato:		Tramite personal computer stand-alone e collegato in LAN per accesso ai dati delle strutture periferiche; dotato di interfaccia applicativa e specifica personalizzazione
Modalità di accesso al dato:		Protetto da identificativo Utente e password tramite interfaccia applicativa; possibilità di accesso agli archivi centralizzati del database su server
Modalità di protezione del dato:		Utente e password con definizione di differenti profili di autorizzazione
Modalità di conservazione del dato:		Dati con prima memorizzazione su dispositivo di rilevazione; dati in linea aggiornati in tempo reale sul server applicativo con allineamento operato quotidianamente a cura del Servizio del Personale; configurazione in mirroring dei dischi per l'archivio su server
Modalità di esecuzione delle copie:		Esecuzione delle copie con backup schedulato a giorni alterni sullo stesso disco ed esecuzione di copia su CD-ROM con periodicità mensile
Modalità di custodia delle copie:		Copia su CD-ROM conservata in armadio protetto da serratura

Rif. **PI1**		*Denominazione:* **Pensioni INPDAP**
Descrizione sintetica:		Gestisce i dati del personale ai fini pensionistici e della carriera lavorativa (fascicolo personale)
Caratteristiche e natura del dato:		Si tratta di dati anagrafici e dati sensibili
Struttura incaricata al trattamento:		Il Servizio del Personale
Altri incaricati al trattamento:		Il Servizio Sistemi Informativi opera la gestione applicativa e manutenzione
Strumenti informatici utilizzati	*Hardware:*	PC con funzionalità di server con condivisione archivio dati in rete LAN; sono presenti due configurazioni separate e singole per il Distretto Amm.vo di Carbonia e quello di Iglesias
	Software:	Pensioni S7 fornito da INPDAP sviluppato in ambiente applicativo Microsoft Access
	Database:	Microsoft SQL Server
Collegamenti LAN e telematici		Accesso applicativo tramite PC in modalità da postazione singola interconnessa in rete LAN locale e remota con le restanti postazioni operative presso le strutture locali
Dispositivi di accesso del dato:		Tramite personal computer stand-alone e collegato in LAN per accesso ai dati delle strutture periferiche; dotato di interfaccia applicativa e specifica personalizzazione
Modalità di accesso al dato:		Protetto da identificativo Utente e password tramite interfaccia applicativa; possibilità di accesso agli archivi centralizzati del database su server
Modalità di protezione del dato:		Utente e password con definizione di differenti profili di autorizzazione
Modalità di conservazione del dato:		Dati in linea aggiornati in tempo reale sul server applicativo
Modalità di esecuzione delle copie:		Esecuzione delle copie con backup eseguito manualmente senza procedure automatizzate con copia della cartella contenente l'archivio dati sul medesimo PC operante da server. Attualmente non eseguite copie su dispositivi esterni
Modalità di custodia delle copie:		Nessuna

Rif. **AM1**		*Denominazione:* **Pacchetto amministrativo - Personale**
Descrizione sintetica:		Gestisce i dati del personale, le presenze ed orari di lavoro, ferie oltre ai dati connessi alle giustificazioni
Caratteristiche e natura del dato:		Si tratta di dati anagrafici e dati sensibili
Struttura incaricata al trattamento:		Il Servizio del Personale
Altri incaricati al trattamento:		Il Servizio Sistemi Informativi opera la gestione dell'intero sistema a riguardo del collegamento dei rilevatori e la gestione applicativa del server
Strumenti informatici utilizzati	*Hardware:*	Rilevatori di presenza presso le strutture aziendali a badge magnetico e server centralizzato in ambiente Microsoft Windows NT Server
	Software:	ENCO fornito da ENCO di Verona
	Database:	Database Oracle
Collegamenti LAN e telematici		L'applicativo opera anche la raccolta e rilevazione dati lettori di codice a barre,; l'accesso applicativo avvienr tramite PC in modalità da postazione singola interconnessa in rete LAN locale e remota con accesso al server centralizzato
Dispositivi di accesso del dato:		Tramite personal computer collegato in LAN; dotato di interfaccia applicativa e specifica personalizzazione
Modalità di accesso al dato:		Protetto da identificativo Utente e password tramite interfaccia applicativa con accesso controllato agli archivi centralizzati del database su server
Modalità di protezione del dato:		Utente e password con definizione di differenti profili di autorizzazione
Modalità di conservazione del dato:		Dati in linea direttamente su serve applicativo e database server; configurazione RAID 0 con mirroring dei dischi per l'archivio su server
Modalità di esecuzione delle copie:		Esecuzione automatica programmata delle copie di backup su nastro con periodicità giornaliera dell'intero database
Modalità di custodia delle copie:		Supporti di memorizzazione su nastro conservati in cassaforte dotata di serratura di sicurezza e protezione ignifuga

Rif. AM2		*Denominazione:* **Pacchetto amministrativo - Bilancio**
Descrizione sintetica:		Gestisce i dati di contabilità, bilancio, magazzino, ordini
Caratteristiche e natura del dato:		Si tratta di dati anagrafici e dati sensibili
Struttura incaricata al trattamento:		Il Servizio Bilancio, Acquisti e Magazzino
Altri incaricati al trattamento:		Il Servizio Sistemi Informativi opera la gestione dell'intero sistema a riguardo del collegamento dei rilevatori e la gestione applicativa del server
Strumenti informatici utilizzati	*Hardware:*	Rilevatori di presenza presso le strutture aziendali a badge magnetico e server centralizzato in ambiente Microsoft Windows NT Server
	Software:	ENCO fornito da ENCO di Verona
	Database:	Database Oracle
Collegamenti LAN e telematici		L'applicativo opera anche la raccolta e rilevazione dati lettori di codice a barre,; l'accesso applicativo avvienr tramite PC in modalità da postazione singola interconnessa in rete LAN locale e remota con accesso al server centralizzato
Dispositivi di accesso del dato:		Tramite personal computer collegato in LAN; dotato di interfaccia applicativa e specifica personalizzazione
Modalità di accesso al dato:		Protetto da identificativo Utente e password tramite interfaccia applicativa con accesso controllato agli archivi centralizzati del database su server
Modalità di protezione del dato:		Utente e password con definizione di differenti profili di autorizzazione
Modalità di conservazione del dato:		Dati in linea direttamente su serve applicativo e database server; configurazione in mirroring dei dischi per l'archivio su server
Modalità di esecuzione delle copie:		Esecuzione automatica programmata delle copie di backup su nastro con periodicità giornaliera dell'intero database
Modalità di custodia delle copie:		Supporti di memorizzazione su nastro conservati in cassaforte dotata di serratura di sicurezza e protezione ignifuga

3 TRATTAMENTI ESTERNI

In questa sezione è riportato un quadro sintetico delle attività affidate a terzi che comportano il trattamento di dati, con l'indicazione sintetica del quadro giuridico o contrattuale (nonché organizzativo e tecnico) in cui tale trasferimento si inserisce, in riferimento agli impegni assunti, anche all'esterno, per garantire la protezione dei dati stessi.

Descrizione dell'attività "esternalizzata": viene indicata sinteticamente l'attività affidata all'esterno.

Trattamenti di dati interessati: vengono indicati i trattamenti di dati, sensibili o giudiziari, effettuati nell'ambito della predetta attività.

Soggetto esterno: la società, l'ente o il consulente cui è stata affidata l'attività, e il ruolo ricoperto agli effetti della disciplina sulla protezione dei dati personali (titolare o responsabile del trattamento).

Descrizione dei criteri per il corretto trattamento: eventuali dichiarazioni o documenti rilasciati dalla Società che effettua il trattamento, ovvero impegni anche su base contrattuale, con particolare riferimento, ad esempio, a:

1. trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto;
2. adempimento degli obblighi previsti dal Codice per la protezione dei dati personali;
3. rispetto delle istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o integrazione delle procedure già in essere;
4. impegno a relazionare periodicamente sulle misure di sicurezza adottate, anche mediante eventuali questionari e liste di controllo, e ad informare immediatamente il titolare del trattamento in caso di situazioni anomale o di emergenze.

Le informazioni sono riportate nella tabella **Trattamenti esterni** sotto riportata:

Rif. **RF1**	*Denominazione:* **Ricette Farmaceutiche**
Descrizione sintetica:	Attività di acquisizione digitale e archiviazione delle prescrizioni mediche. Elaborazioni ed analisi statistiche; determinazione di valori ed indici di spesa farmaceutica.
Caratteristiche e natura del dato:	Si tratta di dati anagrafici e dati sensibili
Soggetto esterno incaricato del trattamento:	Marno S.r.l. In Soft 2000 p.s.c.a.r.l.
Descrizione dei criteri per il corretto trattamento	Il soggetto è responsabile del trattamento e ha sottoscritto, attraverso l'accettazione di specifici obblighi contrattuali, l'ottemperanza alle norme di legge e delle disposizioni interne all'Azienda in tema di protezione dei dati personali.
Rif. **ADI**	*Denominazione:* **Assistenza Domiciliare Integrata**
Descrizione sintetica:	Attività di assistenza di pazienti inseriti nel servizio ADI
Caratteristiche e natura del dato:	Si tratta di dati anagrafici e dati sensibili
Soggetto esterno incaricato	Domi Sanitas s.r.l.

del trattamento:	
Descrizione dei criteri per il corretto trattamento	Il soggetto è responsabile del trattamento e ha sottoscritto, attraverso l'accettazione di specifici obblighi contrattuali, l'ottemperanza alle norme di legge e delle disposizioni interne all'Azienda in tema di protezione dei dati personali.

Rif. **OAS**	*Denominazione:* **Sistema Gestionale OASIS**
Descrizione sintetica:	Attività gestionale dei reparti, ambulatori, laboratori, CUP
Caratteristiche e natura del dato:	Si tratta di dati anagrafici e dati sensibili
Soggetto esterno incaricato del trattamento:	M@rp s.r.l.
Descrizione dei criteri per il corretto trattamento	Il soggetto è responsabile del trattamento e ha sottoscritto, attraverso l'accettazione di specifici obblighi contrattuali, l'ottemperanza alle norme di legge e delle disposizioni interne all'Azienda in tema di protezione dei dati personali.

Rif. **ENC**	*Denominazione:* **Gestionali amministrativi e farmacie**
Descrizione sintetica:	Gestione del personale, bilancio, farmacia
Caratteristiche e natura del dato:	Si tratta di dati anagrafici e dati sensibili
Soggetto esterno incaricato del trattamento:	Enco S.p.A.
Descrizione dei criteri per il corretto trattamento	Il soggetto è responsabile del trattamento e ha sottoscritto, attraverso l'accettazione di specifici obblighi contrattuali, l'ottemperanza alle norme di legge e delle disposizioni interne all'Azienda in tema di protezione dei dati personali.

Rif. **DED**	*Denominazione:* **Anagrafe assistiti**
Descrizione sintetica:	Gestione dell'anagrafe assistiti
Caratteristiche e natura del dato:	Si tratta di dati anagrafici e dati sensibili
Soggetto esterno incaricato del trattamento:	Dedalus
Descrizione dei criteri per il corretto trattamento	Il soggetto è responsabile del trattamento e ha sottoscritto, attraverso l'accettazione di specifici obblighi contrattuali, l'ottemperanza alle norme di legge e delle disposizioni interne all'Azienda in tema di protezione dei dati personali.

Rif **LAB**	*Denominazione:* **Laboratorio Analisi**
Descrizione sintetica:	Gestione delle analisi di laboratorio – software DNLab, DNWeb
Caratteristiche e natura del dato:	Si tratta di dati anagrafici e dati sensibili
Soggetto esterno incaricato del trattamento:	Noema Life
Descrizione dei criteri per il corretto trattamento	Il soggetto è responsabile del trattamento e ha sottoscritto, attraverso l'accettazione di specifici obblighi contrattuali, l'ottemperanza alle norme di legge e delle disposizioni interne all'Azienda in tema di protezione dei dati personali.

Rif. **TRAS**	*Denominazione:* **Trasfusionale**
Descrizione sintetica:	Gestione dei servizi trasfusionali – software Emonet
Caratteristiche e natura del dato:	Si tratta di dati anagrafici e dati sensibili

Soggetto esterno incaricato del trattamento:	Krenesiel S.p.a.
Descrizione dei criteri per il corretto trattamento	Il soggetto è responsabile del trattamento e ha sottoscritto, attraverso l'accettazione di specifici obblighi contrattuali, l'ottemperanza alle norme di legge e delle disposizioni interne all'Azienda in tema di protezione dei dati personali.

Rif.	**ENG**	*Denominazione:*	**Sistema Sanitario Regionale SISaR**
Descrizione sintetica:	Sistema CUP, Amministrativo Contabile, Gestione Veterinaria, Ambulatoriale, Sistema Ospedaliero		
Caratteristiche e natura del dato:	Si tratta di dati anagrafici e dati sensibili		
Soggetto esterno incaricato del trattamento:	RTI composta da Engineering Sanità Enti Locali SpA e Telecom Italia SpA		
Descrizione dei criteri per il corretto trattamento	Il soggetto è responsabile del trattamento e ha sottoscritto, attraverso l'accettazione di specifici obblighi contrattuali, l'ottemperanza alle norme di legge e delle disposizioni interne all'Azienda in tema di protezione dei dati personali.		

Rif.	**HTWC**	*Denominazione:*	**Re-hosting CED regionale**
Descrizione sintetica:	Migrazione dell'applicativo relativo alla convenzione farmaceutica		
Caratteristiche e natura del dato:	Si tratta di dati anagrafici e dati sensibili		
Soggetto esterno incaricato del trattamento:	HTWC Srl		
Descrizione dei criteri per il corretto trattamento	Il soggetto è responsabile del trattamento e ha sottoscritto, attraverso l'accettazione di specifici obblighi contrattuali, l'ottemperanza alle norme di legge e delle disposizioni interne all'Azienda in tema di protezione dei dati personali.		

4 DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ

4.1 Ripartizione dei compiti

Per la descrizione di dettaglio dell'organizzazione e dei compiti assegnati ad ogni singolo servizio o divisione si fa riferimento ai documenti già predisposti (provvedimenti, ordini di servizio, regolamenti interni, circolari, atto aziendale), che possono essere reperiti presso i singoli uffici e le Direzioni Generali.

Si descrivono quindi i compiti e le responsabilità connessi al trattamento di dati personali di pertinenza nell'ambito di ogni singola struttura o classe di divisione o reparto.

In particolare si fa riferimento alle seguenti informazioni:

Strutture: Strutture e trattamenti di competenza di ciascuna struttura.

Compiti e responsabilità della struttura: descrizione sintetica dei compiti e le responsabilità della struttura rispetto ai trattamenti di competenza. Ad esempio: acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, manutenzione tecnica dei programmi, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc.).

4.1.1 Titolare del trattamento

Il TITOLARE del trattamento di dati personali della Azienda Unitaria Sanitaria Locale n. 7 è:

AZIENDA UNITARIA SANITARIA LOCALE n. 7 - Carbonia
Via Dalmazia 83 - 09013 CARBONIA (CA)
Cod. Fisc.: 02261310920

rappresentata dal Direttore Generale pro-tempore.

4.1.2 Responsabili del trattamento

Il titolare del trattamento può facoltativamente designare uno o più responsabili del trattamento che devono essere individuati tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Con deliberazione del Direttore Generale n° 2380 del 11/12/2000 sono stati a suo tempo delegati, quali Responsabili aziendali preposti al trattamento dei dati personali, i dirigenti aziendali pro-tempore responsabili delle articolazioni organizzative di riferimento dell'Azienda.

Alla luce delle variazioni intervenute nelle strutture aziendali i Responsabili di trattamento sono pertanto:

- Responsabile — Distretto Carbonia
- Responsabile — Distretto Iglesias
- Responsabile Amministrativo — Presidio ospedaliero Carbonia
- Responsabile Sanitario — Presidio ospedaliero Carbonia

- Responsabile Amministrativo Presidio ospedaliero Iglesias
- Responsabile Sanitario Presidio ospedaliero Iglesias
- Responsabile Dipartimento amministrativo
- Responsabile Dipartimento di prevenzione
- Responsabile Dip. di Salute Mentale e Dipendenze (SERT – CSM)
- Responsabile Ufficio Tecnico
- Responsabile Dip. Area Medica
- Responsabile Dip. Area Chirurgica
- Responsabile Dip. Area Servizi
- Responsabile Dip. Materno Infantile

I compiti affidati ai responsabili sono stati analiticamente specificati per iscritto; ciascuno di essi è tenuto ad effettuare il trattamento attenendosi alle istruzioni impartite dal titolare, che ha anche il compito specifico, tramite verifiche periodiche, di vigilare sulla puntuale osservanza delle disposizioni e delle proprie istruzioni.

4.1.3 Incaricati di trattamento

Gli incarichi di trattamento sono assegnati dai Responsabili aziendali di cui al precedente paragrafo, attraverso designazione effettuata per iscritto e tale da individuare puntualmente l'ambito di trattamento consentito.

Alternativamente l'incarico viene affidato all'atto della preposizione della persona fisica all'unità presso cui svolge la sua attività lavorativa e per la quale unità è individuato, per iscritto, l'ambito di trattamento consentito ai suoi componenti, come indicato nella tabella che segue:

Denominazione struttura	*Trattamenti operati dalla struttura:*	*Compiti e responsabilità della struttura::*
Servizio Sistemi Informativi	AA1 - Anagrafe Assistiti SP1 - Spesa Farmaceutica RO1 - Flussi Informativi - Dati ricoveri ospedalieri - SDO e DRG AS1 - Attività Specialistica CA1 - CEDAP Certificati di Assistenza al Parto CP1 - CUP Centro Unificato di Prenotazione LA1 - Laboratorio Analisi CT1 - Centri Trasfusionali DB1 - Diabetologia ST1 - SERT TD1 - Teleradiologia RP1 - Gestione Rilevazione Presenze PI1- Pensioni INPDAP AM1 - Pacchetto amministrativo - Personale AM2 - Pacchetto amministrativo – Bilancio SCR – Screening Oncologico	Installazione, gestione e manutenzione tecnica dei programmi, Gestione operativa delle basi dati Esecuzione di salvataggi, ripristini e copie di storicizzazione Esecuzione di report e statistiche tra i dati Correlazione tra le banche dati Importazione ed esportazione di banche dati Caricamento di dati anche con procedure batch Gestione e monitoraggio degli utenti del sistema

Denominazione struttura	*Trattamenti operati dalla struttura:*	*Compiti e responsabilità della struttura::*
Servizio Medicina di Base	AA1 - Anagrafe Assistiti	Acquisizione e caricamento dei dati Interrogazione e comunicazione agli interessati ed aventi diritto Elaborazioni statistiche e di monitoraggio I dati sono trattati separatamente dai due Distretti Sanitari di Carbonia e Iglesias
Servizio Farmaceutico Territoriale	SP1 - Spesa Farmaceutica	Acquisizione e caricamento dei dati Interrogazione e comunicazione agli interessati ed aventi diritto Elaborazioni statistiche e di monitoraggio
Singole Divisioni e Reparti di Ricovero	RO1 - Flussi Informativi - Dati ricoveri ospedalieri - SDO e DRG	Acquisizione e caricamento dei dati Interrogazione e comunicazione agli interessati ed aventi diritto Elaborazioni statistiche e di monitoraggio
Singole Divisioni e Reparti Specialistici, strutture esterne convenzionate, ed altre strutture specialistiche territoriali della ASL	AS1 - Attività Specialistica	Acquisizione e caricamento dei dati Interrogazione e comunicazione agli interessati ed aventi diritto Elaborazioni statistiche e di monitoraggio
Singole Divisioni e Reparti di Ostetricia e Ginecologia che operano a livello di raccolta cartacea dei dati	CA1 - CEDAP Certificati di Assistenza al Parto	Acquisizione e caricamento dei dati Interrogazione e comunicazione agli interessati ed aventi diritto Elaborazioni statistiche e di monitoraggio
Centro Unificato di Prenotazione e strutture operanti presso i distretti	CP1 - CUP Centro Unificato di Prenotazione	Acquisizione e caricamento dei dati Interrogazione e comunicazione agli interessati ed aventi diritto Elaborazioni statistiche e di monitoraggio
Servizio Laboratori di Analisi	LA1 - Laboratorio Analisi	Acquisizione e caricamento dei dati Interrogazione e comunicazione agli interessati ed aventi diritto Elaborazioni statistiche e di monitoraggio Trattamento differenziato (in via provvisoria) da parte delle sedi di Carbonia e di Iglesias
Servizio Centri Trasfusionali	CT1 - Centri Trasfusionali	Acquisizione e caricamento dei dati Interrogazione e comunicazione agli interessati ed aventi diritto Elaborazioni statistiche e di monitoraggio
Servizio Diabetologico	DB1 - Diabetologia	Acquisizione e caricamento dei dati Interrogazione e comunicazione agli interessati ed aventi diritto Elaborazioni statistiche e di monitoraggio
SERT	ST1 - SERT	Acquisizione e caricamento dei dati Interrogazione e comunicazione agli interessati ed aventi diritto Elaborazioni statistiche e di monitoraggio
Servizio Radiologia	TD1 - Teleradiologia	Acquisizione e caricamento dei dati Interrogazione e statistiche
Servizio del Personale	RP1 - Gestione Rilevazione Presenze PI1 - Pensioni INPDAP AM1 - Pacchetto amministrativo - Personale	Acquisizione e caricamento dei dati Interrogazione e comunicazione agli interessati ed aventi diritto Elaborazioni statistiche e di monitoraggio
Servizio Bilancio, Acquisti e Magazzino	AM2 - Pacchetto amministrativo – Bilancio	Acquisizione e caricamento dei dati Interrogazione e comunicazione agli interessati ed aventi diritto Elaborazioni statistiche e di monitoraggio
Servizio Igiene e Prevenzione	SCR – Screening Oncologico	Acquisizione e caricamento dei dati Interrogazione e comunicazione agli interessati ed aventi diritto Elaborazioni statistiche e di monitoraggio

4.2 Incarichi e istruzioni per il trattamento dei dati

Gli incarichi di trattamento sono assegnati dai Responsabili aziendali, individuati con deliberazione del Direttore Generale n. 2380 del 11/12/2000, attraverso designazione effettuata per iscritto e tale da individuare puntualmente l'ambito di trattamento consentito.

Alternativamente l'incarico viene affidato all'atto della preposizione della persona fisica all'unità presso cui svolge la sua attività lavorativa e per la quale unità è individuato, per iscritto, l'ambito di trattamento consentito ai suoi componenti.

In entrambi i casi all'incaricato di trattamento dovranno essere indicate le modalità con cui devono essere effettuati i trattamenti e le misure di sicurezza che gli incaricati devono adottare nel trattamento informatizzato dei dati personali, riportate nelle **Istruzioni per il trattamento dei dati con strumenti informatici** riportate nell'appendice 1 al presente documento.

5 ANALISI DEL RISCHIO

In questa sezione si elencano i principali eventi potenzialmente dannosi per la sicurezza dei dati, con una valutazione delle possibili conseguenze e la gravità in relazione al contesto di riferimento e al danno potenziale. In relazione a ciascun evento si valutano le principale conseguenze e la probabilità stimata, anche in termini sintetici (alta/media/bassa).

5.1 Eventi e valutazione del rischio

Gli eventi che possono verificarsi sono, in linea generale:

1) comportamenti degli operatori:
    a. sottrazione di credenziali di autenticazione
    b. carenza di consapevolezza, disattenzione o incuria
    c. comportamenti sleali o fraudolenti
    d. errore materiale

2) eventi relativi agli strumenti:
    a. azione di virus informatici o di programmi suscettibili di recare danno
    b. spamming o tecniche di sabotaggio malfunzionamento, indisponibilità o degrado degli strumenti
    c. accessi esterni non autorizzati
    d. intercettazione di informazioni in rete

3) eventi relativi al contesto fisico-ambientale:
    a. ingressi non autorizzati a locali/aree ad accesso ristretto
    b. sottrazione di strumenti contenenti dati, eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ...), nonché dolosi, accidentali o dovuti ad incuria
    c. guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.)
    d. errori umani nella gestione della sicurezza fisica

Gli elementi rilevati sono riportati nella tabella:

Tipologia degli rischi:	*Descrizione del tipo di rischio:*	*Analisi del rischio*	*Livello di probabilità del rischio*	*Livello di gravità sulla sicurezza*
degli operatoriComportamento	Sottrazione di credenziali di autenticazione	Possibilità da parte di estranei di entrare in possesso di codici utente e password	Medio, la gestione è centralizzata ed operata da personale competente ed attento. Permane però il rischio qualora non si rispettino idonee regole di generazione e conservazione delle password	Medio, sono comunque attive funzioni di registrazione di log e di controllo che possono monitorare eventi anomali
	Carenza di consapevolezza, disattenzione e incuria	Il rischio legato a disattenzione, incuria o errore materiale è la causa statisticamente più rilevante di perdita di dati personali	Alto per dati personali conservati nei sistemi client; Basso per dati conservati sui sistemi centralizzati (server)	Medio; in genere riferito ad utenti con credenziali limitate e per dati non condivisi
	Comportamenti sleali e fraudolenti	Il rischio è insito in atteggiamenti sleali e fraudolenti mirati a far danno o alla acquisizione di dati e informazioni riservate	Basso. Di norma il comportamento degli operatori è corretto, e sono attive funzioni di controllo nei sistemi centralizzati	Alto. Interventi dolosi possono provocare danni ingenti
	Errori umani nella gestione della sicurezza fisica	I comportamenti per cui è presente un maggior rischio per l'integrità fisica riguardano principalmente l'errato utilizzo dei sistemi oppure l'abbandono temporaneo della vigilanza sugli stessi.	Medio. La gestione è demandata a personale esperto che opera ormai con adeguate competenze e piena consapevolezza. Tuttavia l'intensità nell'utilizzo delle apparecchiature rende maggiore il rischio qualora non vengano applicate tutte le regole di salvaguardia dei sistemi e di tutela.	Alto
Eventi relativi agli strumenti e ai sistemi informatici e telematici	Azione virus informatici o di programmi atti specificatamente a recare danno	La diffusione dei virus informatici, anche propagati attraverso la posta elettronica, può portare alla perdita della riservatezza delle informazioni. La gestione centralizzata dei sistemi di posta e l'uso di un software antivirus limitano però il danno	Medio sulle postazioni utente. Basso sui sistemi server	Medio, nelle postazioni utente ha gravità limitata e circostanziata. Alto nelle postazioni server e database applicativi
	Spamming o tecniche di sabotaggio	Possibile accesso alla rete dall'esterno o invio di dati atti a saturare le funzionalità di rete o lo spazio di memorizzazione (attacchi di tipo Denial Of Service)	Basso, gli accessi sono controllati e riservati agli utenti muniti di opportune credenziale; funzioni di firewalling sono attive sulle connessioni esterne	Basso, l'effetto in caso di attacco è normalmente limitato nel tempo e circoscritto
	Malfunzionamento, guasti, degrado dei sistemi	Gli apparati sono dotati di un livello di ridondanza e resistenza ai guasti sufficiente in condizioni normali. Il rischio di indisponibilità dei sistemi è però elevato in condizioni rare ma non impossibili. La mancanza di un sistema automatizzato per la gestione delle procedure di backup e di disaster recovery rende critico un guasto ad apparati non sufficientemente ridondati	Medio. Sono stati adottati degli accorgimenti che però non riducono sufficientemente il rischio	Alto, interruzione della normale operatività. possibilità di perdita dei dati
	Accessi esterni non autorizzati	Connessioni da rete Internet o da parte di società di assistenza e manutenzione	Medio: è operativo un sistema di firewalling; le connessioni da postazioni esterne per servizi di assistenza sono precisamente identificate in termini di indirizzo IP univoco e comunque associate a profili di connettività protetti da password e dotati delle opportune credenziali e limitazioni. L'assenza di	Alto. L'accesso ad informazioni riservate da parte di soggetti non autorizzati costituisce grave violazione del sistema.

Tipologia degli rischi:	*Descrizione del tipo di rischio:*	*Analisi del rischio*	*Livello di probabilità del rischio*	*Livello di gravità sulla sicurezza*
			sistemi semi-automatici di controllo rende però difficoltosa l'analisi dei log degli accessi e l'individuazione tempestiva di tentativi di intrusione.	
	Intercettazione di informazioni sulla rete telematica	Attivazione di PC in rete non autorizzata; esplorazione delle risorse condivise	Basso: sono gestiti e controllati i singoli punti di cablaggio e le porte degli apparati di rete; le risorse condivise in rete, relativamente ai dati centralizzati sono protette da accesso	Medio
Eventi relativi al contesto fisico-ambientale	Mancato funzionamento del climatizzatore nel Data Center	Nel Data Center di Iglesias, che racchiude il maggior numero di apparecchiature server, ci sono due impianti di raffreddamento indipendenti. Gli impianti non sono però sotto continuità elettrica. Non è presente una configurazione di spegnimento dei server e di alert automatico in caso di innalzamento anomalo della temperatura.	Medio. In caso di interruzione della corrente elettrica entrambi i climatizzatori cessano di funzionare.	Alto. Il mancato raffreddamento degli ambienti comporta grave rischio per l'integrità fisita degli apparati.
	Interruzione della continuità elettrica	Il Data center di Iglesias è dotato di gruppo di continuità per i server e gli apparati di rete. Manca però un gruppo elettrogeno, per cui un'interruzione elettrica per più di 20-30 minuti comporta uno spegnimento dei sistemi	Alto. Un'interruzione nell'erogazione della corrente per più di 30 minuti comporta un'interruzione dei servizi	Alto. L'indisponibilità dei sistemi comporta il sostanziale blocco di alcuni reparti (ad esempio dei laboratori di analisi)
	Interruzione del collegamento in rete	Il servizio di collegamento in rete è gestito dall'operatore Telecom. Un'interruzione del servizio dati comporta sostanzialmente l'interruzione dei servizi erogati centralmente	Basso. Le statistiche di interruzione dei collegamenti in rete da parte dell'operatore indicano una bassa incidenza di casi	Alto. L'indisponibilità della rete comporta il sostanziale blocco di alcuni reparti (ad esempio dei laboratori di analisi)
	Attentato alla sicurezza fisica dei sistemi	Il Data Center di Iglesias dispone di impianto di allarme antiintrusione, è inoltre stato attivato un servizio di sorveglianza notturna. Gli apparati client sono in genere conservati in locali presidiati e protetti.	Per gli apparati client il rischio di furto o danneggiamento è normalmente basso. Il rischio di furto o danneggiamento per gli apparati server di Iglesias è medio basso	Alto. La distruzione o il furto di apparati server comporta perdita dei dati, della loro riservatezza, indisponibilità dei sistemi e dei servizi
	Sottrazione di strumenti o di supporti di memorizzazione contenenti dati	Le copie delle banche dati e dei server principali sono tenute in appositi spazi protetti e conservati in cassaforte ignifuga. La protezione di dati conservati su supporti rimovibili deve essere garantita dagli operatori attraverso l'applicazione delle politiche di sicurezza definite nell'Azienda.	Medio, relativamente a copie dei dati trasferiti su dischetti o CD-ROM o create per funzionalità di trasmissione, importazione o esportazione	Medio/Alto consente di avere accesso ad informazioni che non sono più protette ed anche facilmente leggibili in formati di interscambio dati (ASCII, TXT, CSV, ecc.)

Tipologia degli rischi:	*Descrizione del tipo di rischio:*	*Analisi del rischio*	*Livello di probabilità del rischio*	*Livello di gravità sulla sicurezza*
	Eventi distruttivi naturali, artificiali, nonché dolosi, accidentali o dovuti ad incuria	Si opera la copia dei dati su diversi supporti e dischi, con conservazione delle copie di backup su nastro entro spazi protetti anche con cassaforte a tenuta ignifuga	Medio, in quanto esistono installazioni distribuite di server, alcuni dei quali anche in ambienti particolarmente soggetti ad eventi accidentali	Alto

6 ANALISI DELLE CONTROMISURE

In questa sezione sono riportate, in forma sintetica, le misure in essere e quelle da adottare per contrastare i rischi individuati. Per misura si intende lo specifico intervento tecnico od organizzativo posto in essere per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia, come pure quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia.

6.1 Adozione di politiche di sicurezza e gestione del rischio

L'adozione e la verifica di politiche di sicurezza organiche e complessive per tutti i trattamenti costituisce una contromisura "trasversale" che responsabilizza tutti sulla necessità di operare in modo sicuro nei trattamenti che utilizzano dati personali.

La politica di sicurezza costituisce pertanto una contromisura che agisce su ogni evento dannoso.

Segue la raccolta organica delle misure di sicurezza e di gestione del rischio adottate presso la ASL n. 7 di Carbonia, e l'indicazione delle strutture responsabili dell'adozione o mantenimento delle misure stesse.

Il documento viene aggiornato con periodicità annuale contestualmente all'adozione del Documento Programmatico di Sicurezza, di cui costituisce parte integrante.

6.1.1 Azioni da porre in essere per il mantenimento della politica di sicurezza

- nomina (per iscritto) dei responsabili dei trattamenti e degli incaricati dei trattamenti;
- attuazione delle misure di sicurezza per la protezione delle aree e dei locali ove si svolge il trattamento dei dati personali e misure di tutela fisica e logica degli apparati in essi dislocati;
- attuazione delle misure di sicurezza per la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali;
- definizione delle procedure di continuità ed emergenza, al fine di supplire alla temporanea indisponibilità dei sistemi di elaborazione e calcolo;
- attuazione di copie di sicurezza periodiche del contenuto degli apparati utilizzati nel trattamento dei dati personali;
- applicazione delle regole di buon uso del sistema informativo aziendale;
- attuazione delle misure di contenimento dei virus informatici;
- attuazione delle misure organizzative e tecniche per la gestione dei documenti informatici;
- attuazione delle misure di informazione e formazione del personale aziendale sugli aspetti di sicurezza informatica;
- misure di sicurezza relative alla salvaguardia delle informazioni detenute su supporto cartaceo.

Sono responsabili della messa in atto delle azioni indicate e della gestione delle opportune tutele, ognuno per la parte di competenza, il Titolare, i Responsabili e gli Incaricati dei trattamenti di dati personali.

6.1.2 Custodia e archiviazione dei dati

Agli incaricati vengono impartite istruzioni per la gestione, la custodia e l'archiviazione dei documenti e dei supporti, sotto forma di direttive per:

1. il corretto accesso ai dati personali, sensibili e giudiziari;
2. la conservazione e la custodia di documenti, atti e supporti contenenti dati personali, sensibili e giudiziari;
3. la definizione delle persone autorizzate ad accedere ai locali archivio ed ai dati e le modalità di accesso.

È responsabile della definizione delle direttive relative ai dati acceduti tramite il sistema informatico il Servizio Sistemi Informativi; sono responsabili delle direttive relative alla gestione, custodia ed archiviazione dei dati conservati ed acceduti in altra forma i singoli Responsabili.

6.1.3 Politiche di gestione dei guasti

Per tutti i trattamenti che occorre tutelare da **minacce alla disponibilità** dei dati conservati in formato elettronico si adottano le seguenti misure.

Trattamenti per i quali il guasto bloccante è altamente probabile

- predisposizione di contratti di manutenzione per i server che garantiscano tempi di intervento compatibili con la velocità di ripristino necessaria o presenza di server "muletto" già configurati per la sostituzione dell'apparato guasto;
- predisposizione di stazioni di lavoro (client) alternative e di stazioni muletto da usare al bisogno;
- linee di rete WAN idonee a garantire la normale esecuzione di trattamenti che avvengono su sistemi distribuiti nel territorio e che, al fine di ridurre il rischio di guasti bloccanti, dispongano di adeguato backup, attraverso linee sostitutive anche a prestazioni ridotte;
- apparati di rete locale coperti da contratti di manutenzione che garantiscano un tempo di ripristino adeguato;

Trattamenti per i quali il guasto bloccante è mediamente probabile

- server: predisposizione di contratti di manutenzione che garantiscano tempi di intervento compatibili con la velocità di ripristino necessaria;
- client: predisposizione di stazioni di lavoro (client) alternative e di stazioni muletto da usare al bisogno;
- gli apparati di rete locale devono essere coperti da contratti di manutenzione che garantiscano un tempo di ripristino adeguato;

È responsabile della formulazione di adeguate politiche di gestione dei guasti il Servizio Sistemi Informativi. Sono responsabili della attuazione dei passi previsti dalle politiche di gestione dei guasti i vari incaricati per tali mansioni.

6.1.4 Misure minime di sicurezza logica

1. Il trattamento di dati personali è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo;

3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

4. Per trattamenti che utilizzano dati di particolare importanza o che è necessario proteggere con maggiore livello di sicurezza si prevedranno dispositivi di autenticazione sicuro (carte magnetiche, smart card) e/o dispositivi biometrici di riconoscimento.

5. Agli incaricati saranno consegnate le istruzioni per l'adozione delle misure di sicurezza e per l'accesso ai sistemi, nonché per l'adozione delle necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato. (D.L. 196/2003 Allegato B, punti 1, 2, 3,4). Sono impartite istruzioni per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi. Pertanto si dispone che ogni utente definito, non venga più cancellato, ma
disabilitato nel caso cessi di essere in uso, in maniera tale da evitarne il riutilizzo (D.L. 196/2003 Allegato B, punti 6).

7. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da questo ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi. Qualora il sistema operativo dell'elaboratore su cui risiede l'applicativo lo consenta, è abilitato il cambio password, che l'incaricato potrà autonomamente effettuare in un qualsiasi momento successivo al primo accesso, e in ogni altro momento successivo; per quei sistemi operativi per i quali non sia disponibile tale modalità di cambio password, o non sia comunque abilitabile per ragioni tecniche, è individuata una procedura organizzativa opportuna per il cambio password mediante l'ausilio del personale tecnico (D.L. 196/2003 Allegato B, punto 5);

8. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

9. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può
assicurare la disponibilità di dati o strumenti elettronici, in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire, per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato. (D.L. 196/2003 Allegato B, punti 7, 8, 9, 10)

11. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato
un sistema di autorizzazione.

12. 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.

13. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione. (D.L. 196/2003 Allegato B, punti 12, 13, 14).

14. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

15. 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.

16. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

17. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale (D.L. 196/2003 Allegato B, punti 15, 16, 20, 17, 18); per i dati di particolare importanza la frequenza del salvataggio è giornaliera.

18. Il reimpiego dei supporti di memorizzazione è vietato qualora siano serviti per la memorizzazione di dati personali o sensibili; è inoltre genericamente vietato l'utilizzo di supporti di memorizzazione rimovibili per lo scambio di dati sensibili (D.L. 196/2003 Allegato B, punti 21 e 22).

19. Comunque, anche se le norme prevedono particolari cautele solo per i supporti rimovibili contenenti dati sensibili e giuridici, la tutela per il trattamento viene estesa ai dati personali come segue:

- custodia dei supporti in contenitori chiusi a chiave in locali con accesso ai soli autorizzati
- cancellazione e/o distruzione del supporto una volta cessate le ragioni per la conservazione

20. I dati personali devono essere di norma tenuti separati dai dati sensibili. Quando si trasmettono per via telematica dati sensibili, ad esempio per la trasmissione dei flussi informativi per adempimenti di legge, si devono separare i dati personali in maniera tale il file contenente i dati sensibili sia reso anonimo e collegabile al soggetto a cui i dati si riferiscono solo attraverso un codice.

È responsabile della formulazione di opportune politiche di gestione dei sistemi di elaborazione che garantiscano il rispetto delle misure minime di sicurezza – e della messa in opera delle misure attuative, per la parte di competenza – il Servizio Sistemi Informativi.

6.1.5 Misure di contenimento del rischio

Al fine di contenere il rischio portandolo sotto una opportuna soglia di probabilità, relativamente all'importanza dei dati trattati ed alle modalità di trattamento, si adottano le seguenti misure di contenimento del rischio:

Apparati e sistemi informatici

- Gli apparati di rete e le apparecchiature server devono essere maneggiate da personale qualificato, dotato di certificazioni e competente in materia;
- i server che hanno un ruolo nel processo di autenticazione dell'utente [per es. server di dominio e similari], devono essere configurati minimizzando il numero di funzionalità in uso su di essi e adottando tutte le opportune tecniche di irrobustimento;
- vengono adottate analoghe tutele anche per i sistemi di elaborazione dedicati al backup dei dati;
- tutte le sessioni di amministrazione di sistema e di concessione/revoca/modifica di abilitazioni applicative che non si svolgano in locale sul server devono essere rese completamente immuni da azioni di intercettazione sulla rete e di fraudolenta impersonificazione – mediante tecniche opportune di gestione sicura della autenticazione del client e di crittografia di canale;
- le password di amministrazione devono avere almeno una lunghezza di almeno 8 caratteri, con possibilità di inserire sia maiuscole che minuscole e segni di punteggiatura, hanno una scadenza imposta massima di 1 mese e non possono essere ripetute;
- le autenticazioni devono essere effettuate in maniera sicura senza che la password viaggi in chiaro sulla rete, o che in rete viaggino informazioni che possano essere utilizzate per una fraudolenta impersonificazione ;
- si configurano nella maniera più sicura possibile tutti i server che forniscono funzionalità applicative, minimizzando il numero di funzionalità in uso su di essi e adottando tutte le opportune tecniche di irrobustimento;
- le password applicative, devono avere almeno una lunghezza di 8 caratteri, con possibilità di inserire sia maiuscole che minuscole e segni di punteggiatura, hanno una scadenza imposta massima di 6 mesi e non possono essere ripetute.
- Non vengono sistematicamente gestite – almeno all'interno del confine aziendale – misure tese a prevenire l'intercettazione e la modifica delle comunicazioni applicative considerando tali minacce poco rilevanti.
- Invece nel caso di comunicazioni che attraversino il confine aziendale occorre che siano adeguatamente tutelati anche questi aspetti adottando opportune tecniche di crittografia di canale.
- Vengono monitorati automaticamente gli accessi alla rete, nonché le operazioni eseguite sul gestionale sanitario OASIS. Tali log vengono acceduti dietro necessità legate alla sicurezza dei sistemi o ad indagini ispettive interne o dell'Autorità Giudiziaria.
- Vengono monitorati i sistemi attraverso l'applicativo Nagios, al fine di individuare tempestivamente errori e malfunzionamenti dei server e dei servizi.

L'attuazione delle misure tecniche sopra descritte sono di competenza del Servizio Informativo Aziendale.

Regole di buon uso

- È vietato l'uso di supporti di memorizzazione removibili per la memorizzazione di dati personali o sensibili. Deroghe a tale regola sono possibili solo nei casi in cui sia possibile dimostrare il corretto uso dei supporti di memorizzazione ai sensi del D.L. 196/2003 Allegato B, punti 21 e 22
- è possibile il reimpiego del supporto solo nel caso non siano più recuperabili le informazioni precedentemente memorizzate, in caso contrario, il supporto removibile dopo l'uso andrà distrutto
- in generale i supporti di memorizzazione – anche non removibili - che contengono dati personali o sensibili, nel caso non possano essere cancellati in maniera da renderne irrecuperabile il contenuto, una volta dimessi, dovranno essere distrutti o smaltiti in maniera tale che il contenuto non sia più recuperabile
- viene fatto esplicito e tassativo divieto di connettere in rete stazioni di lavoro se non dietro esplicita e formale autorizzazione del Servizio Sistemi Informativi. È altresì vietato alterare in qualsiasi modo la configurazione software della stazione di lavoro - o di altri dispositivi direttamente connessi alla rete, dati o fonia - per quanto attiene all'accesso alla rete. È anche fatto divieto di utilizzare in qualsiasi modo la rete aziendale per fini non espressamente autorizzati. In particolare tali divieti si possono tradurre, anche se non esaurire, nelle seguenti esplicite proibizioni: divieto di alterare la configurazione delle configurazioni di rete di stazioni di lavoro e altri dispositivi in rete (stampanti condivise, ecc...), comprendendo in ciò anche il divieto di aggiungere protocolli di rete o servizi in rete
- divieto di monitorare ciò che transita in rete
- è inoltre vietata l'installazione non autorizzata di Modem per linee analogiche o digitali che sfruttino il sistema di comunicazione in fonia per l'accesso a banche dati esterne o interne alla ASL
- è vietata l'installazione di hardware o software di qualsiasi tipo che consenta o faciliti il by pass delle misure di presidio del confine aziendale - per es. software di comunicazione che garantiscano accessi che non passino per i punti autorizzati e presidiati

Sono responsabili dell'attuazione delle misure sopra descritte tutti i dipendenti che utilizzano strumenti informatici nell'espletamento dei trattamenti che interessano dati personali.

Collegamento ai sistemi

- il dipendente è tenuto a conservare nella massima segretezza la parola di accesso ai sistemi e qualsiasi altra informazione legata al processo di autenticazione
- inoltre è tenuto a scollegarsi dal sistema ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro, o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima; alternativamente può adottare un dispositivo salvaschermo con password di sblocco, qualora l'accesso al sistema possa avvenire, a seguito di riavvio, solo attraverso l'inserimento di credenziali di autenticazione (userid e password)
- nella produzione di stampe su dispositivi posizionati in locali diversi occorre procedere quanto prima al recupero delle stesse
- il dipendente è tenuto a conservare con la massima cura eventuali dispositivi per l'accesso ai sistemi aziendali e ad usarli conformemente alle specifiche indicazioni d'uso. La perdita o danneggiamento degli stessi sarà sanzionata.

Sono responsabili dell'attuazione delle misure sopra descritte tutti i dipendenti che utilizzano strumenti informatici nell'espletamento dei trattamenti che interessano dati personali.

Protezione dei locali e degli archivi

E' necessario sensibilizzare gli operatori alla sorveglianza diretta degli archivi, al controllo delle persone che accedono ai locali in cui gli archivi stessi sono contenuti e all'adozione di regole di comportamento sicure, specialmente quando si abbandona temporaneamente la postazione di lavoro.

Per quanto concerne il rischio che i dati siano danneggiati o perduti a seguito di eventi distruttivi, i locali ove si svolge il trattamento di dati importanti e particolarmente soggetti a tutela sono protetti da:

- dispositivi antincendio previsti dalla normativa vigente
- gruppo di continuità dell'alimentazione elettrica
- impianto di condizionamento

I locali dove si conservano dati e strumentazioni utilizzati nel trattamento dovranno essere forniti di punti di accesso controllabili e forniti di serratura.

Per i locali ove si svolge il trattamento di dati importanti e particolarmente soggetti a tutela si dovrà prevedere un impianto d'allarme antintrusione e/o un servizio di vigilanza o videosorveglianza.
All'interno dei locali, se accessibili al pubblico, dovranno essere contenuti degli armadi o cassetti per la conservazione degli archivi cartacei, protetti con serratura.

Il personale in servizio nei locali e nelle aree dove si svolgono i trattamenti ha compito di vigilanza al fine di garantire la riservatezza e l'integrità dei dati e dei supporti in cui gli stessi sono conservati.

6.1.6 Comportamento degli operatori

Elemento importante di prevenzione degli eventi indesiderati è l'adozione di una opportuna azione di informazione degli operatori e l'adozione di politiche di comportamento sicure quali ad esempio:

- non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento;
- custodire i dispositivi di accesso agli strumenti informatici (username e password, eventuali badge o schede);
- obbligo di assoluta riservatezza
- effettuazione di copie di sicurezza dei dati
- conservare i documenti contenenti dati personali in luoghi sicuri ed armadi chiusi a chiave.

Un documento contenente, in forma sintetica, le principali misure di sicurezza che è obbligatorio adottare nel trattamento di dati con strumenti informatici viene consegnato agli incaricati di trattamento contestualmente all'incarico.
Il documento che attualmente si adotta è meglio specificato in **Istruzioni per il trattamento di dati con strumenti informatici** nell'appendice 1 al presente documento.

6.2 Misure adottate

6.2.1 Apparati hardware e software centralizzati

Le misure di sicurezza adottate per gli apparati ed i software utilizzati in modalità client-server e per le reti di collegamento telematiche sono le seguenti:

a) Ridondanza

I dispositivi ritenuti determinanti per il funzionamento della macchina sono duplicati (processori, alimentatori, schede di rete, ecc..), inoltre alcuni di questi dispositivi quali gli Hard Disk e gli alimentatori, in caso di guasto, possono essere sostituiti a caldo (Hot-Swap).

I Server più importanti sono configurati in cluster e garantiscono il funzionamento anche nell'ipotesi che uno dei due Server presenti malfunzionamento.

b) Alimentazione stabilizzata

I Server sono alimentati elettricamente tramite UPS (alimentatori stabilizzati) che proteggono le macchine da sbalzi di tensione, ed hanno in generale un'autonomia di circa 6-8 ore in assenza di alimentazione elettrica della rete.

c) Backup

I Server sono muniti di unità di back-up su nastro che permettono di salvare i dati su apposite cassette sia in modo automatico che manuale.

Inoltre i server in cluster sono configurati in modo da creare in automatico una copia intera dei dati (Raid 1) e viene utilizzata una SAN (Storage Area Network) per il salvataggio dei dati di applicazioni particolarmente critiche.

d) Accesso alle procedure

Tutti i software attualmente utilizzati nell'Azienda sono forniti di un modulo per il controllo e la sicurezza degli accessi, da parte degli utenti autorizzati ad aree specifiche del programma, tramite apposita UserID e Password; viene tenuta traccia informatica, per almeno 6 mesi, delle operazioni eseguite sui gestionali sanitari da parte degli operatori accreditati.

e) Preservazione di un microclima idoneo nei locali in cui sono posizionati i server principali

Nella sala server di Iglesias sono presenti due apparecchi di raffreddamento, di cui uno sotto continuità elettrica.

f) Controllo centralizzato degli accessi e misure di salvaguardia

Il controllo degli accessi avviene attraverso un domain server che serve tutta la rete aziendale. Il software antivirus è aggiornato automaticamente in modo centralizzato e gestito dalla Ditta Telecom. L'accesso Internet è centralizzato e il flusso da e verso l'esterno monitorato con un firewall.

g) Misure per la continuità operativa: progetto obiettivo "Assistenza Informatica d'Urgenza"

L'Azienda ha rilevato l'urgente necessità di garantire nell'arco delle 24 ore l'assistenza tecnico/informatica da parte del Servizio Informativo al fine di garantire la disponibilità e la sicurezza in tempo reale di tutti i sistemi informatici aziendali attraverso le seguenti attività:

- azioni periodiche di monitoraggio e manutenzione dei sistemi

- analisi di possibili miglioramenti architetturali nell'ottica di ridurre i tempi di indisponibilità dei sistemi

- azioni eccezionali per attività di pronto intervento e ripristino qualora vi siano disservizi e guasti hardware o software che interessino le centrali telefoniche, i router e i server aziendali l'attività relativa all'assistenza tecnico/informatica suddetta in specie riguarda:

- l'assistenza tecnico informatica 24 ore su 24 (festività comprese) rivolta in particolare ai servizi di Laboratorio Analisi, Centro trasfusionale, Pronto Soccorso e Radiologia delle strutture ospedaliere aziendali;

- verifica e interventi tecnico/manutentivi sui sistemi e sulle apparecchiature informatiche in modo periodico e continuo nei momenti nei quali non vi è attività in corso e le stesse non sono utilizzate da personale in servizio;

- interventi tecnico/manutentivi 24 ore su 24 (festività comprese) per urgenze legate a inconvenienti tali da impedire il normale e regolare svolgimento dell'attività nella fascia oraria serale;

I programmi per la gestione della contabilità, degli utenti e degli stipendi sono aggiornati in modo da rispondere alle misure minime previste dal D.Lgl. 196/2003.

6.2.2 Rete aziendale

La ASL n. 7 dispone di una rete aziendale costituita da LAN interne alle principali strutture sul territorio collegate tra loro in VPN protetta, con gestione esternalizzata e linee di trasporto basate su ADSL. Si è di recentemente conclusa la transizione verso il Sistema Pubblico di Connettività che, oltre a garantire maggiore continuità nei servizi di trasporto, migliora, a parità di costo, le performance complessive dei sistemi.

Le comunicazioni tra sedi diverse attraverso la VPN sono crittografate. Le comunicazioni interne alle singole reti LAN non sono di norma crittografate.

È prevista l'autenticazione dell'utente per l'accesso alla rete aziendale.

6.2.3 Misure fisiche di protezione dei locali e degli archivi

Un elemento di rischio rilevato è quello di perdita della riservatezza e della possibile sottrazione dei dati che deriva dalla conservazione degli stessi in ambienti non idonei e non protetti.

Il Data Center di Iglesias, che contiene la maggior parte delle applicazioni e dei dati critici dell'Azienda, è posizionato in un edificio riservato, con porte blindate per l'accesso, sensori di rilevamento di intrusioni collegati al servizio di vigilanza.

I dati contenuti in archivi non centralizzati sono normalmente presidiati direttamente dagli operatori e posizionati in locali che di norma non sono accessibili al pubblico.

6.2.4 Stato di avanzamento piano di intervento 2007-2009

Nel DPS dell'anno 2007 è stato programmato un piano di intervento triennale il cui stato di attuazione è sinteticamente esposto nella tabella seguente:

Intervento	Descrizione intervento	Spesa prevista	Stato	Spesa effettuata
Gruppo elettrogeno	Installazione di un gruppo elettrogeno di potenza circa 30Kw nel Data Center di Iglesias	€ 20.000,00	In corso di attuazione	
Servizio vigilanza	Installazione di sistema di allarme antiintrusione o di videosorveglianza	€ 5.000,00	Convenzione con Inst. Di Vigilanza Cannas per il 2008, Delibera 235/2008	€ 2.160,00
Impianto antincendio e allarmi	Impianto di rilevazione fumi, rilevazione temperatura, allarme, spegnimento automatico	€ 12.000,00	Non attuato	
Ridondanza e consolidamento server applicativi e dati	Installazione di due server su cui virtualizzare tutti i server applicativi attualmente in utilizzo. Consolidamento del server dati in cluster; realizzazione di una nuova SAN; installazione di un server, e relativo software, per la gestione dei backup	€ 190.110,00	Attuato parzialmente: acquistato server per applicativo di laboratorio analisi ITACA	€ 5.016,00
Backup dati utente	Acquisto ed installazione per i client aziendali di unità di masterizzazione	€ 6.000.00	Non attuato	
Ridondanza firewall ed apparati attivi	Configurazione in cluster dei firewall; duplicazione dei dispositivi di rete (switch, collegamenti) del Data Center di Iglesias	€ 12.000.00	Attuato con delibera 1708 del 30-12-2008	€ 14.328,00
Formazione	Programmare corsi di formazione per il personale in tema di sicurezza e corretto utilizzo dei sistemi	€ 35.592,00	Corso per VmWare, delibera 1739 del 31.12.2008	€ 6.000,00
	TOTALE	**€ 280. 702,00**		**€ 27.504,00**

6.3 Misure da adottare

In riferimento agli elementi di criticità vengono indicate le misure da adottare e i tempi previsti per la loro messa in opera .

Gli obiettivi di sicurezza che ci si pone sono coerenti con quanto previsto dall'art. 31 del D.Lgl. 196/2003 e cioè:
"1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta."

In particolare occorre dare attuazione a quanto previsto dall'allegato B del D.L. 196/2003, dando attuazione a misure di sicurezza ulteriori – rispetto a quelle previste dal D.L. 196/2003 – che l'azienda ritenga opportune e necessarie nell'ottica del perseguimento degli obiettivi istituzionalmente attribuiti, riducendo a livelli ritenuti accettabili i principali rischi di sicurezza a cui il sistema informativo aziendale è sottoposto.
Questo deve essere ottenuto, compatibilmente con i vincoli di sicurezza sopra enunciati, mantenendo il massimo livello di usabilità del sistema.

Per arrivare a questo risultato, che per sua natura si configura come un processo sempre in itinere e non come un passo completato *una tantum*, si definisce una *Politica di sicurezza e gestione del rischio*, alla quale si dà massima diffusione presso i responsabili delle strutture organizzative dell'Azienda. Lo scopo del presente documento è anche quello di costituire la base per programmare l'applicazione continua e l'aggiornamento delle politiche di sicurezza definite.

La gestione dei sistemi informativi è quasi completamente centralizzata e la maggior parte dei server è concentrata nella struttura di Iglesias via Gorizia.

Ciò costituisce un elemento di ottimizzazione delle attività sistemistiche, a condizione di curare l'aspetto della sicurezza e della continuità operativa dei servizi critici.

È in corso di avviamento il sistema informativo sanitario regionale SISaR per il quale parte degli applicativi e database, con i relativi server, sono centralizzati a livello regionale presso il CRESSAN mentre altri sono stati installati presso il CED di Via Gorizia.

A tal proposito la dotazione del Centro consente di garantire l'erogazione dei servizi in condizione di normale attività. Esistono però dei fattori di criticità sul lato della sicurezza che, all'accadere di determinati eventi indesiderati, possono compromettere la continuità operativa e la stessa integrità dei sistemi.

A seguito dell'analisi del rischio sono stati individuati degli interventi prioritari che dovranno essere pianificati al fine di adeguare gli impianti alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta (art. 31 D. Lgs. 196/2003). Tali interventi sono stati inseriti nella programmazione triennale 2007-2009 e sono in fase di realizzazione.

A titolo esemplificativo e non esaustivo si citano i seguenti punti:

- Continuità elettrica: la continuità è garantita dalla presenza di due unità UPS consentono di conservare operatività per un periodo di circa 1-2 ore in caso di interruzione nella erogazione della corrente elettrica; per interruzioni superiori si sta procedendo alla installazione di un gruppo elettrogeno.
- Protezione fisica degli ambienti: gli ambienti sono protetti con porte blindate ed impianto di allarme antintrusione, cosicché è possibile garantire la sicurezza fisica degli apparati anche negli orari in cui i locali non sono presidiati direttamente. Non è invece attivo un sistema antincendio anche se sono presenti gli estintori. E' quindi necessario predisporre un sistema di rilevazione fumi e impianto antincendio con gas inerte a saturazione totale, centralina di allarme antincendio ed antifurto con invio automatico di alert al personale preposto (tramite sms, email e chiamata telefonica).
- Impianti di raffreddamento: sono presenti due split che, complessivamente, sono sufficienti a garantire il mantenimento della temperatura di esercizio. Il guasto di uno dei due apparati può però provocare un innalzamento eccessivo della temperatura, che non viene rilevato da nessun procedimento automatico di controllo. Occorre perciò valutare la predisposizione di automatismi di rilevazione della temperatura e di allarmi progressivi (pre-allarme e allarme) al superamento dei valori di soglia impostati.
- Consolidamento server: Installazione di due server su cui virtualizzare tutti i server applicativi attualmente in utilizzo. Consolidamento del server dati (DataBase Server) in configurazione cluster. Realizzazione di una nuova SAN (Storage Area Network);
- Backup e ripristino: è presente un sistema di storage (SAN Storage Area Network), che non può però contenere dischi rigidi sufficientemente veloci per consentire l'utilizzo efficiente della memoria da parte dei server applicativi (sono utilizzabili solo dischi di tipo SATA). La SAN può quindi essere utilizzata solo come area di backup temporaneo. Le altre unità di backup sono principalmente unità a nastro o masterizzatori. Manca però un piano di salvataggio e i backup avvengono principalmente su un unico nastro, in modo incrementale. Un guasto del dispositivo o un danneggiamento del nastro possono perciò compromettere gravemente i salvataggi. Manca infine un piano di "disaster recovery", che consenta l'adozione di procedure di ripristino a seguito di un guasto gravissimo ("disastro"), in modo da prevedere la riattivazione dei servizi in tempi certi commisurati al danno prodottosi. Le procedure di ripristino comportano principalmente il coinvolgimento delle Ditte fornitrici delle apparecchiature hardware e software, cosicché un qualsiasi problema comporta costi elevati sia in termini di spesa che di tempo necessario al ripristino.
  Per la protezione dei dati utente: mancano dispositivi di backup o aree di salvataggio dati dedicate agli operatori dell'Azienda; inoltre quasi tutti i PC client non dispongono di apparati idonei ad effettuare copie di backup (masterizzatori di CD, DVD). L'attivazione di un dominio di rete, in fase di completamento, può rendere l'operazione di salvataggio periodico dei dati più sicuro, prevedendo eventualmente delle aree riservate in cui salvare i dati più importanti. È inoltre necessario dotare ogni PC di almeno una unità di salvataggio diversa dal lettore di floppy.
- Linee dati: con la centralizzazione dei servizi è diventata critica la necessità di continuità nella trasmissione dei dati tra i nodi della rete aziendale. Infatti un'interruzione del servizio da parte del gestore Telecom, per quanto improbabile, produrrebbe per molte

unità uno stop delle attività (ad esempio per i laboratori di analisi). È stata pressoché conclusa la transizione verso il Sistema Pubblico di Connettività, con livelli di garanzia elevati di disponibilità dei servizi di trasporto.

6.3.1 Misure fisiche di protezione dei sistemi

Al fine di garantire l'integrità dei dati contenuti nei data server del centro di Iglesias e la continuità operativa dei servizi, è indispensabile adottare le seguenti misure:

- Installazione di un gruppo elettrogeno opportunamente dimensionato per la sala server del Data Center di Iglesias; predisposizione del quadro elettrico relativo;
- Installazione di un impianto antincendio di tipo a gas estinguente, con centralina di segnalazione, sensori rilevatori di fumo, sensori di temperatura e dispositivi di allarme; dotazione di estintori idonei per l'utilizzo in locali con apparecchiature elettriche ed elettroniche;

6.3.2 Misure per la continuità operativa

Al fine di garantire la disponibilità dei sistemi, dei dati e dei servizi con operatività 24/24, 7/7, come richiesto dagli obblighi di legge e di servizio per diversi reparti dell'Azienda, occorre improntare la configurazione architetturale del sistema in modo da proteggere adeguatamente i dati e garantire l'erogazione dei servizi anche in caso di guasto o danneggiamento dei dispositivi hardware o delle installazioni software.
Tra le soluzioni che l'evoluzione tecnologica mette a disposizione, quella che si giudica obiettivamente più confacente alle esigenze dell'Azienda, anche in considerazione delle necessità di protezione e continuità operativa rilevate e della massiccia centralizzazione delle funzioni e dei dati, è quella che prevede il consolidamento e la duplicazione delle unità di elaborazione (server applicativi) e la concentrazione del DBMS oracle su un cluster di server dedicati che afferiscono ad una storage area network efficiente e sicura, in modo da consentire il raggiungimento di un adeguato livello di *robustezza* e *ridondanza*, la semplificazione della gestione degli applicativi e l'ottimizzazione dell'attività di manutenzione e/o di ripristino dei sistemi a seguito di fault. A tale architettura occorre affiancare un server che gestisca, in modo automatico, tutte le procedure di backup, limitando al minimo le possibilità di errore e riducendo le spese ed i tempi di ripristino.

Occorre inoltre aumentare la ridondanza per i punti critici del sistema, che si individuano nelle seguenti componenti:

a) apparati attivi di rete e firewall
b) rete privata aziendale

Per ciò che attiene al primo punto occorre operare sui seguenti elementi:

- firewall Fortigate, è stato recentemente raddoppiato e clusterizzato
- switch e collegamenti in fibra con la SAN, che vanno duplicati

Per quanto riguarda la rete privata aziendale occorre creare una rete di backup che consenta di sostenere i collegamenti delle unità operative sparse sul territorio, ospedali, distretti, poliambulatori, uffici amministrativi, anche nel caso di un'interruzione del servizio di connessione offerto dalla

Telecom Italia. È stato attivato il nuovo contratto SPC, che consente di avere maggiore affidabilità nei collegamenti di rete.

6.4 Attività di verifica e controllo

La necessità di valutare l'efficacia delle misure di sicurezza messe in atto e verificare se vi siano attacchi o violazioni alle norme di riservatezza, limitando i danni conseguenti, richiede l'adozione di un opportuno insieme di misure di monitoraggio.
In particolare ogni responsabile di struttura, con il supporto del Servizio Sistemi Informativi, provvederà a programmare le verifiche, con frequenza almeno mensile, dell'efficacia delle misure adottate relativamente a:

- accesso fisico a locali dove si svolge il trattamento
- procedure di archiviazione e custodia dati trattati
- efficacia e utilizzo delle misure di sicurezza nell'uso degli strumenti elettronici
- integrità dei dati e delle loro copie di backup
- distruzione dei supporti magnetici non più riutilizzabili
- livello di informazione degli interessati

Sarà cura del Servizio Sistemi Informativi redigere un documento nel quale si descrivano:

- gli eventuali altri aspetti di sicurezza da monitorare;
- le soglie oltre le quali si deve innescare un controllo maggiormente approfondito o una specifica contromisura;
- periodicità e modalità con le quali operare il controllo con particolare riguardo ai sistemi informatici.

Il Servizio Sistemi Informativi dovrà redigere specifiche procedure che regolamentino l'operato degli incaricati del controllo, nelle quali si imponga di mantenere evidenza dei controlli effettuati.
Si stabilisce inoltre che possa essere condotta da esperti del settore – eventualmente esterni all'azienda – una sessione di auditing volta a verificare la robustezza delle misure messe in atto per la tutela del confine aziendale e dei servizi messi in disponibilità ad utenti esterni al confine aziendale. Di tali verifiche sarà conservata evidenza.

6.5 Cifratura dei dati o separazione dei dati identificativi

I software utilizzati all'interno dell'Azienda, pur permettendo la separazione dei dati sensibili da quelli personali comuni (anagrafica), non consentono la cifratura dei dati sensibili. Si potrà valutare, in relazione al grado di rischio accertato per i flussi di dati che interessano i singoli applicativi, la possibilità di aggiornare i software affinché cifrino i dati sensibili.

7 PROCEDURE DI BACKUP E RECOVERY

In questa sezione sono descritti i criteri e le procedure adottati per il ripristino dei dati in caso di loro danneggiamento o di inaffidabilità della base dati. L'importanza di queste attività deriva dall'eccezionalità delle situazioni in cui il ripristino ha luogo: è essenziale che, quando sono necessarie, le copie dei dati siano disponibili e che le procedure di reinstallazione siano efficaci.

7.1 Procedure di salvataggio

Le procedure di salvataggio dei server vengono eseguite giornalmente. Le cassette di backup vengono conservate in una cassaforte ignifuga e il loro contenuto verificato periodicamente. Il controllo del log di salvataggio viene eseguito a cura del Servizio Sistemi Informativi.

7.2 Procedure di ripristino

Le procedure di ripristino che riguardino copie dei database vengono effettuate direttamente dal Servizio Sistemi Informativi, eventualmente con il supporto remoto delle Ditte fornitrici degli applicativi.

Il ripristino dei sistemi e degli applicativi a seguito di guasto catastrofico è effettuato a cura delle Ditte fornitrici.

7.3 Prove di ripristino

Considerato che diversi sistemi in uso nell'Azienda sono operativi 24/24 e 7/7, risulta estremamente complicato pianificare prove di ripristino e test di efficacia delle procedure di salvataggio/ripristino dei dati adottate senza sospendere l'erogazione dei servizi.

8 PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI

In questa sezione sono riportate le informazioni necessarie per individuare il quadro sintetico degli interventi formativi che si prevede di svolgere.

8.1 Formazione programmata

Tutti i dipendenti che svolgono qualsivoglia trattamento di dati personali debbono seguire un corso di formazione e/o aggiornamento sul trattamento dei dati personali in conformità con le regole della vigente normativa in materia (Codice sul trattamento dei dati personali D.L.vo 196/2003).

Ai fini di della formazione dei dipendenti sul trattamento di dati personali, l'Azienda predispone corsi gestiti da proprio personale qualificato che ha maturato esperienza nel settore, oppure può avvalersi dell'opera di soggetti esterni.

I corsi di formazione dovranno avere una durata di almeno quattro ore; le ore dedicate sono considerate quale servizio e aggiornamento obbligatorio.

I corsi vengono calendarizzati dalla Direzione per moduli, compatibilmente con le esigenze dei Servizi/UU.OO.

Il corso deve prevedere:

A) Una fase di formazione attraverso una lezione in aula che affronti - anche con l'eventuale ausilio di dispense, di strumenti informatici e/o audiovisivi - l'analisi dei rischi che incombono sui dati e delle specifiche misure per prevenirli con riferimento alle specifiche mansioni svolte dai dipendenti, l'esame degli elementi principali della normativa in materia di protezione dei dati personali, l'analisi di casi pratici, cenni sulle modalità con cui aggiornarsi sulle misure minime di sicurezza adottate dalla Azienda.

B) Una fase di verifica delle conoscenze acquisite dai partecipanti sul corretto trattamento dei dati personali e sugli elementi fondamentali della normativa vigente in materia, anche attraverso elaborati scritti o la compilazione di test a risposta multipla.

Al termine del corso di formazione l'Azienda rilascia ad ogni partecipante un attestato di partecipazione contenente una sintetica valutazione di quanto emerso nella fase di verifica del corso. Copia dell'attestazione è conservata dall'Ufficio del Personale nel fascicolo di ciascun dipendente.

Ove venisse riscontrata una carenza di formazione nel singolo dipendente, l'Azienda dovrà disporre un ulteriore evento formativo, da realizzarsi entro il termine di sei mesi in base alle direttive sopra indicate.

8.2 Formazione iniziale

In caso di assunzione di nuovi dipendenti o dell'inserimento di personale con contratto di lavoro interinale o di collaborazione/consulenza, ovvero in caso di cambiamento di mansioni, l'Ufficio

del Personale segnalerà i nominativi alla Direzione perchè vengano predisposti gli appositi corsi di formazione, anche individuali, da realizzarsi in base alle direttive sopra indicate.

8.3 Formazione continua

L'Azienda, in base alle risultanze dei corsi, può individuare nelle varie Strutture il personale che possa assolvere alla funzione di punto di riferimento per le eventuali ulteriori esigenze di formazione sulla materia del trattamento dei dati personali in tale ambito.

8.4 Piano di formazione

L'informazione e la formazione sull'applicazione delle regole di sicurezza e sul corretto utilizzo dei sistemi costituisce un importante elemento di prevenzione e di riduzione del rischio.

Infatti si stima che la maggior parte delle violazioni o perdite di dati si hanno a causa di comportamenti errati, disattenzione, incuria o errore umano.

Quello che segue costituisce un programma di interventi di tipo modulare:

Modulo 1 (4 ore) : Sicurezza e tutela dei dati personali (per operatori sanitari ed amministrativi)	
Obiettivi	Obiettivo del modulo è quello di introdurre il tema della sicurezza e del corretto trattamento dei dati personali, in relazione alle politiche di sicurezza definite nell'Azienda e alla tipologia di trattamenti effettuati.
Contenuti	Normativa sulla sicurezza; Il Documento Programmatico per la Sicurezza e le politiche di sicurezza adottate nell'Azienda; regole di corretto utilizzo degli strumenti informatici e misure di contenimento del rischio.

Modulo 2 (18 ore): Sicurezza e tutela dei dati personali (per tecnici)	
Obiettivi	Obiettivo del percorso è quello di approfondire le tematiche della sicurezza informatica dei dati e delle comunicazioni per la prevenzione e gestione di eventuali attacchi esterni.
Contenuti	Introduzione alla sicurezza ed alla terminologia della sicurezza informatica; tecniche e strumenti per la protezione dei dati a livello fisico e logico; tipi di attacco; tipi di programmi di attacco; tecniche di attacco alle reti; incidenti; virus; politiche di sicurezza; Backup e ripristino di sistemi; DPS e privacy.

Modulo 3 (2 ore): Politiche di gestione, custodia ed archiviazione dei dati (per Responsabili)	
Obiettivi	Introdurre le problematiche relative agli aspetti organizzativi e di controllo per ridurre il rischio e garantire un corretto trattamento dei dati da parte delle strutture.
Contenuti	Normativa sulla sicurezza; Il Documento Programmatico per la Sicurezza e le politiche di sicurezza adottate nell'Azienda; aspetti organizzativi per la gestione della sicurezza; procedure di continuità ed emergenza; misure di sicurezza relative alla salvaguardia delle informazioni detenute su supporto cartaceo.

Modulo 4 (4 ore): Il trattamento dei dati con strumenti informatici (per operatori sanitari ed amministrativi)	
Obiettivi	Avere padronanza degli strumenti utilizzati nel trattamento dei dati personali, con particolare riguardo agli applicativi e alle strumentazioni in dotazione nell'Azienda
Contenuti	Utilizzo degli strumenti informatici e degli applicativi in uso nell'Azienda nel trattamento dei dati personali connessi con i compiti affidati, con particolare riferimento alle misure per la prevenzione di errori, alla correttezza delle operazioni svolte, alle procedure da mettere in atto per garantire la riservatezza dei dati.

Modulo 5 (18 ore): Amministrazione di basi di dati (per Database Administrators)	
Obiettivi	Introdurre i concetti fondamentali di gestione dei dati con strumenti informatici
Contenuti	Basi di dati e sistemi di gestione di basi di dati. I modelli dei dati. Livelli di astrazione nei DBMS. Linguaggi per data base. Interfacce per DBMS. Utenti della base di dati. Controllo della base di dati: integrità, affidabilità, sicurezza. Misure di protezione dei dati: autenticazione ed autorizzazione informatica. Classificazione dei DBMS. I moduli di un DBMS.

La programmazione degli interventi prevede l'esecuzione di fasi formative per i tecnici del Servizio Sistemi Informativi, attraverso i moduli 2 e 5 le cui tematiche potranno essere coperte da più corsi separati che congiuntamente coprano il fabbisogno formativo complessivo. I moduli 1 e 3 saranno realizzati attraverso l'impiego dei tecnici del Servizio Sistemi Informativi, che effettueranno direttamente i corsi programmati. Il modulo 4 sarà invece realizzato dalle Ditte fornitrici degli applicativi utilizzati nell'Azienda.

Gli schemi seguenti riassumono la programmazione degli interventi per l'anno 2009.

anno 2009	**Destinatari**	**N. sessioni**	**N. ore complessivo**	**N. persone formate**
Modulo 1	Operatori/Infermieri	25	100	500
Modulo 2	Tecnici	4	72	4
Modulo 3	Responsabili	3	6	50
Modulo 4	Operatori/Infermieri	20	80	400
Modulo 5	Tecnici	4	72	4
TOTALE		**56**	**330**	**958**

9 APPENDICE 1: ISTRUZIONI PER IL TRATTAMENTO DEI DATI CON STRUMENTI INFORMATICI

9.1 Introduzione

Questo documento fornisce agli incaricati del trattamento una panoramica sulle responsabilità loro spettanti, rispetto alla gestione ed allo sviluppo della sicurezza dell'informazione, nel caso di trattamenti effettuati con strumenti informatici.

Nell'ambito informatico, il termine "sicurezza" si riferisce a tre aspetti distinti:

Riservatezza: Prevenzione contro l'accesso non autorizzato alle informazioni;

Integrità: Le informazioni non devono alterabili da incidenti o abusi;

Disponibilità: Il sistema deve essere protetto da interruzioni impreviste.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche gli opportuni meccanismi organizzativi; misure soltanto tecniche, per quanto possano essere sofisticate, non saranno efficienti se non usate propriamente.

In particolare, le precauzioni di tipo tecnico possono proteggere le informazioni durante il loro transito attraverso i sistemi, o anche quando queste rimangono inutilizzate su un disco di un computer; nel momento in cui esse raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle norme.

Nella gestione dei dati personali e dei dati sensibili è bene immaginare di trattare sostanze pericolose (ad esempio esplosivi), ed usare tutti gli accorgimenti che si adotterebbero per gestire in sicurezza tali sostanze.

In effetti la norma assimila il trattamento dei dati personali al maneggio di materiali pericolosi e impone al responsabile del trattamento l'obbligo di dimostrare di aver adottato tutti gli accorgimenti, tecnici, organizzativi e di comportamento, per ridurre il rischio sotto una soglia accettabile.

9.2 Linee guida per la sicurezza

1. UTILIZZATE LE CHIAVI!

Il primo livello di protezione di qualunque sistema o dato è quello fisico; è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario non banale per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania; pertanto, chiudete a chiave il vostro ufficio alla fine della giornata e chiudete i documenti a chiave nei cassetti ogni volta che potete.

2. CONSERVATE DISCHETTI, CD, PENNE USB ED ALTRI SUPPORTI RIMOVIBILI IN UN LUOGO SICURO

Per i supporti rimovibili si applicano gli stessi criteri che per i documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. A meno che non siate sicuri che contengano solo informazioni non sensibili o personali, riponeteli sotto chiave non appena avete finito di usarli. Nell'utilizzo di supporti rimovibili occorre considerare che i floppy disk costituiscono supporti poco affidabili, in quanto si smagnetizzano o rovinano facilmente, ed il loro uso dovrebbe quindi essere destinato solo al trasferimento temporaneo di files e non per archiviazione.

3. UTILIZZATE LE PASSWORD

Vi sono svariate categorie di password, ognuna con il proprio ruolo preciso:

- La password di accesso al computer impedisce l'utilizzo improprio della vostra postazione, quando per un motivo o per l'altro non vi trovate in ufficio;
- La password di accesso alla rete impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse della rete;
- La password dei programmi specifici (ad es. OASIS) permette di restringere l'accesso ai dati e alle procedure del programma al solo personale autorizzato;
- La password del salvaschermo (screensaver), infine, impedisce che una vostra assenza momentanea permetta a una persona non autorizzata di visualizzare il vostro lavoro e i vostri files.

Imparate a utilizzare questi quattro tipi fondamentali di password, e mantenete distinta almeno quella del primo tipo, che può dover essere resa nota, almeno temporaneamente, ai tecnici incaricati dell'assistenza o ai colleghi in caso di vostra assenza.

4. ATTENZIONE ALLE STAMPE DI DOCUMENTI RISERVATI

Non lasciate accedere alle stampe persone non autorizzate; se la stampante non si trova sulla vostra scrivania recatevi quanto prima a ritirare le stampe. Distruggete personalmente le stampe quando non servono più.

5. NON LASCIATE TRACCIA DEI DATI RISERVATI

Quando rimuovete un file, i dati non vengono effettivamente cancellati ma soltanto marcati come non utilizzati, e sono facilmente recuperabili. Neanche la formattazione assicura l'eliminazione dei dati; solo l'utilizzo di un programma apposito garantisce che sul dischetto o hard disk non resti traccia dei dati precedenti. Nel dubbio, se I dati da cancellare sono contenuti su un disco rimovibile, è sempre meglio usare un dischetto nuovo e distruggere quello vecchio.

6. PRESTATE ATTENZIONE ALL'UTILIZZO DEI PC PORTATILI

I PC portatili sono un facile bersaglio per i ladri. Se avete necessità di gestire dati riservati su un portatile usate una password sicura per l'accesso al sistema e fate un backup periodico del contenuto del disco.

7. NON FATEVI SPIARE QUANDO STATE DIGITANDO LE PASSWORD

Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate la vostra password, questa potrebbe essere letta guardando i tasti che state battendo.

8. CUSTODITE LE PASSWORD IN UN LUOGO SICURO

Non scrivete la vostra password, meno che mai vicino alla vostra postazione di lavoro. L'unico affidabile dispositivo di registrazione è la vostra memoria. Se avete necessità di conservare traccia delle password per iscritto, non lasciate in giro i fogli utilizzati.

9. NON FATE USARE IL VOSTRO COMPUTER A PERSONALE ESTERNO A MENO DI NON ESSERE SICURI DELLA LORO IDENTITÁ

Personale esterno può avere bisogno di installare del nuovo software/hardware nel vostro computer. Assicuratevi dell'identità della persona e delle autorizzazioni ad operare sul vostro PC.

10. NON UTILIZZATE APPARECCHI NON AUTORIZZATI

L'utilizzo di modem su postazioni di lavoro collegati alla rete di edificio offre una porta d'accesso dall'esterno non solo al vostro computer, ma a tutta la rete, ed è quindi vietata. Per questa ragione è fatto divieto l'utilizzo di apparecchi non autorizzati per l'accesso ad Internet o ad altre reti.

11. NON INSTALLATE PROGRAMMI NON AUTORIZZATI

Solo i programmi istituzionali o acquistati dall'Azienda con regolare licenza sono autorizzati. Se il vostro lavoro richiede l'utilizzo di programmi specifici, consultatevi con il Servizio Sistemi Informativi.

12. APPLICATE CON CURA LE LINEE GUIDA PER LA PREVENZIONE DA INFEZIONI DI VIRUS

La prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus; tra l'altro, potreste incorrere in una perdita irreparabile di dati.

13. EFFETTUATE BACKUP (COPIE DI SICUREZZA) DEI DATI

Dato che il rischio di guasto delle apparecchiature non può essere mai ridotto a zero, l'unico modo per garantire la salvaguardia dei dati è quello di effettuare copie periodiche dei dati contenuti nei dischi del PC, usando supporti sicuri, ad esempio CD o DVD. Conservate le copie di sicurezza in luoghi sicuri e protetti.

9.3 Linee guida per la prevenzione dei virus

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

COME SI TRASMETTE UN VIRUS:

1. Attraverso programmi provenienti da fonti non ufficiali;
2. Attraverso le macro dei programmi di automazione d'ufficio (word, excel);
3. Attraverso allegati o link (collegamenti) in messaggi di posta elettronica.

COME *NON* SI TRASMETTE UN VIRUS:

1. Attraverso file di dati NON in grado di contenere macro (file di testo, pdf, ecc.);
2. Attraverso mail NON contenenti allegati.

QUANDO IL RISCHIO DA VIRUS SI FA SERIO:

1. Quando si installano programmi;
2. Quando si copiano dati da dischetti;
3. Quando si scaricano dati o programmi da Internet;
4. Quando si aprono allegati non sicuri giunti per email o si clicca su link presenti nel messaggio.

QUALI EFFETTI HA UN VIRUS?

1. Effetti sonori e messaggi sconosciuti appaiono sul video;
2. Nei menù appaiono funzioni extra finora non disponibili;
3. Lo spazio disco residuo si riduce inspiegabilmente;
4. Il computer diventa lento nelle elaborazioni;
5. Si perdono dati dal disco rigido
6. Il browser si collega da solo a siti sconosciuti
7. Vengono trasmessi dati riservati per email a propria insaputa

COME PREVENIRE I VIRUS:

1. USATE SOLTANTO PROGRAMMI PROVENIENTI DA FONTI FIDATE

Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione con antivirus prima di essere installato. Non utilizzate programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus.

2. ASSICURATEVI DI NON FAR PARTIRE ACCIDENTALMENTE IL VOSTRO COMPUTER DA DISCHETTO

Infatti se il dischetto fosse infettato, il virus si trasferirebbe nella memoria RAM e potrebbe espandersi ad altri files.

3. PROTEGGETE I VOSTRI FLOPPY DA SCRITTURA QUANDO POSSIBILE

In questo modo eviterete le scritture accidentali, magari tentate da un virus che tenta di propagarsi. I virus non possono in ogni caso aggirare la protezione meccanica.

4. ASSICURATEVI CHE IL VOSTRO SOFTWARE ANTIVIRUS SIA ATTIVO

La tempestività nell'azione di bonifica è essenziale per limitare i danni che un virus può causare; inoltre è vitale che il programma antivirus conosca gli ultimi aggiornamenti sulle "impronte digitali" dei nuovi virus. Il sistema antivirus presente in azienda viene aggiornato automaticamente; occorre però verificare che il software sia attivo sul proprio PC.

COME *NON* PREVENIRE I VIRUS:

1. NON DIFFONDETE MESSAGGI DI PROVENIENZA DUBBIA

Se ricevete messaggi che avvisano di un nuovo virus pericolosissimo, ignoratelo: le email di questo tipo sono detti con terminologia anglosassone *hoax* (termine spesso tradotto in italiano con "bufala"), l'equivalente delle "leggende metropolitane" della rete. Questo è vero anche se il messaggio proviene dal vostro migliore amico, dal vostro responsabile o da un tecnico informatico. È vero anche e soprattutto se si fa riferimento a "una notizia proveniente dalla Microsoft" oppure dall'IBM (sono gli *hoax* più diffusi).

2. NON PARTECIPATE A "CATENE DI S. ANTONIO" E SIMILI

Analogamente, tutti i messaggi che vi invitano a "diffondere la notizia quanto più possibile" sono *hoax*. Anche se parlano della fame nel mondo, della situazione delle donne negli stati arabi, di una bambina in fin di vita, se promettono guadagni miracolosi o grande fortuna; sono tutti *hoax* aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche. Queste attività sono vietate dagli standard di Internet e contribuire alla loro diffusione può portare alla terminazione del proprio accesso.

9.4 Linee guida per la scelta delle password

Il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è, quindi, parte essenziale della sicurezza informatica.

COSA NON FARE

1. NON dite a nessuno la vostra password. Ricordate che lo scopo principale per cui usate una password è assicurare che nessun altro possa utilizzare le vostre risorse o possa farlo a vostro nome.
2. NON scrivete la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer.
3. Quando immettete la password NON fate sbirciare a nessuno quello che state battendo sulla tastiera.
4. NON scegliete password che si possano trovare in un dizionario. Su alcuni sistemi è possibile "provare" tutte le password contenute in un dizionario per vedere quale sia quella giusta.
5. NON crediate che usare parole straniere renderà più difficile il lavoro di scoperta, infatti chi vuole scoprire una password è dotato di molti dizionari delle più svariate lingue.
6. NON usate il vostro nome utente. È la password più semplice da indovinare.

7. NON usate password che possano in qualche modo essere legate a voi come, ad esempio, il vostro nome, quello di vostra moglie/marito, dei figli, del cane, date di nascita, numeri di telefono etc.

COSA FARE

1. Cambiare la password a intervalli regolari, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari l'obbligo è di modificare la parola chiave almeno ogni tre mesi.
2. Usare password lunghe almeno otto caratteri con un misto di lettere, numeri e segni di interpunzione.
3. Utilizzate password distinte per sistemi con diverso grado di sensibilità. In alcuni casi la password viaggiano in chiaro sulla rete e possono essere quindi intercettate, per cui, oltre a cambiarla spesso, è importante che sia diversa per quella usata da sistemi "sicuri". Il tipo di password in assoluto più sicura è quella associata a un supporto di identificazione come un dischetto o una carta a microprocessore; la password utilizzata su un sistema di questo tipo non deve essere usata in nessun altro sistema.

COME SCEGLIERE UNA PASSWORD

Le migliori password sono quelle facili da ricordare ma, allo stesso tempo, difficili da indovinare, come quelle che si possono ottenere comprimendo frasi lunghe. La frase "C'era una volta una gatta che aveva una macchia nera sul muso" può ad esempio fornire, tra le tante possibilità, "CrlVlt1Gtt". Oppure la frase "Password del sistema OASIS per i laboratori di analisi" può essere tradotta in "PdSoPiLdA".

Le regole da seguire sono semplici ma importanti:

non scegliere password troppo brevi: usa almeno 8 caratteri

non usare password troppo intuibili, come targa dell'auto, numero di telefono, nomi di familiari, date di nascita

usa qualche cosa di memorizzabile, che non ti obblighi a scriverla per non scordarla

se possibile cambiarla con una certa frequenza, almeno ogni sei mesi (tre mesi se si trattano dati sensibili)