



AZIENDA REGIONALE TERRITORIALE EDILIZIA

LA SPEZIA

Documento Programmatico sulla Sicurezza dei Sistemi Informativi (DPSS)

Versione	Data	Emesso da	Approvato da	Note
2.70	28-03-2011	Ufficio AA.GG. e Personale	Arch. Giancarlo RATTI Amministratore Unico	Decreto A.U. n. 83 in data 28/3/2011
	Firma			

1.1	Premessa.....	3
1.2	Riferimenti Normativi.....	3
1.3	Obbiettivi.....	3
1.4	Aggiornamento del documento	4
1.5	Trattamento dei dati (Regola 19.1)	4
1.6	Compiti, responsabilità, organizzazione e processi (Regola 19.2)..	5
1.5.1	Organizzazione	5
1.4.1	Operazioni nelle quali consistono i Trattamenti	6
1.4.2	Responsabilità e incarichi.....	6
1.4.3	Descrizione dei sistema informatico	8
1.7	Analisi del rischio (Regola 19.3)	9
1.8	Misure di sicurezza da adottare (Regola 19.4).....	12
1.8.1	Principi generali.....	12
1.8.2	Norme comportamentali e internet.....	13
1.8.3	Sicurezza fisica dei locali	13
1.8.3	Protezione da malware	14
1.8.4	Utilizzo dei supporti magnetici.....	14
1.8.5	Trasmissione dei dati	15
1.8.6	Autenticazione.....	15
1.8.7	Gestione delle credenziali	15
1.8.8	Network	15
1.9	Procedure di salvataggio e ripristino dei dati (Regola 19.5)	15
1.9.1	Linee guida per i salvataggi ed il ripristino dei dati.....	15
1.9.2	Piano dei salvataggi dei dati.....	16
1.9.3	Piano di ripristino dei dati	17
1.10	Formazione degli incaricati (Regola 19.6).....	17
1.10.1	Generalità.....	17
1.10.2	Piano di formazione	19
1.11	Trattamenti affidati all'esterno (Regola 19.7)	19
1.12	Cifratura e Speciali Misure di Protezione nel Settore Sanitario (Regola 19.8).....	20
Allegati:		
Allegato “A” - REGISTRO DEI SALVATAGGI		21
Allegato “B” - REGISTRO DEGLI INGRESSI SALA MACCHINE.....		22

1.1 Premessa

La normativa sulla sicurezza e sulla gestione dei dati sensibili richiede che tutti gli enti o aziende si debbano dotare di opportune strategie per garantire la corretta gestione dei dati sensibili e dei sistemi informativi più in generale. Il presente documento, descrivendo un insieme di procedimenti, consente di definire come strutturare e utilizzare l'intero sistema informativo nel rispetto della normativa in materia di privacy e gestione dei dati personali, giudiziari e sensibili.

1.2 Riferimenti Normativi

Legge n.547 del 1993 che modifica il codice penale introducendo i cosiddetti "computers crimes".

DPR n.318 del 1999 che dà attuazione alle previsioni in materia di sicurezza minima come prospettato nell'art.15 della Legge n.318 del 1999.

Decreto Legislativo 30 giugno 2003, n. 196 e successivi provvedimenti del garante in materia di Privacy , in particolare :

articoli da 28 a 30 (Soggetti che effettuano il trattamento);

articoli dal 31 al 36 (Misure di sicurezza);

articolo 180 (Disposizioni transitorie – Misure di sicurezza);

allegato B (Disciplinare tecnico in materia di misure minime di sicurezza).

Legge 24/03/2001 n. 127, recante delega al governo per l'emanazione di un T. U. in materia di trattamento dei dati personali.

1.3 Obiettivi

Il Documento garantisce che il trattamento dei dati si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Il trattamento dei dati personali è disciplinato in modo da assicurare un elevato livello di tutela dei diritti e delle libertà nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte del titolare del trattamento (art. 2 d.lgs. 196/2003).

Tali dati riguardano:

- clienti;
- fornitori;
- personale interno.

Le misure minime di sicurezza devono essere adottate in base al tipo di dato gestito (personali, giuridici e sensibili) , al tipo di archivio (elettronico o cartaceo) ed al tipo di elaboratore (connesso in rete e se la rete e' pubblica o meno). Il presente DPS costituisce lo strumento di riferimento per la gestione delle attività e la descrizione della struttura del sistema informativo. Il DPS e' disponibile sia in formato elettronico (file Word DPS **xx.xx.doc**, dove xx.xx e' la versione), sia in formato cartaceo. I due formati sono sempre conservati in modo da ricostruire la storia delle versioni.

Gli aspetti sviluppati sono i seguenti:

- descrizione dati personali, sensibili e giuridici;
- descrizione delle metodologie di accesso sicuro ai dati (misure minime di sicurezza adottate);
- individuazione dei responsabili e incaricati al trattamento dati;

- metodologia di aggiornamento del DPS;
- analisi del rischio;
- piano di formazione degli incaricati alla gestione dati;

Facciamo osservare che, aldilà del rispetto formale di quanto previsto nella normativa sopra citata, il DPS deve essere anche interpretato come uno strumento volto ad un più corretto e sicuro utilizzo dei supporti informatici; quindi deve essere anche sfruttato per l'acquisizione ed il rispetto delle metodologie di gestione "in sicurezza" degli impianti elettronici disponibili; il documento, comprende pertanto, anche alcune parti tese alla sensibilizzazione degli utenti su tale materia.

1.4 Aggiornamento del documento

L'aggiornamento del documento consente di disporre di un documento di riferimento sempre coerente con la situazione reale dell'architettura del sistema e con la normativa vigente.

L'aggiornamento del DPS e la ristampa dello stesso, sono eseguiti dall'ente che lo ha emesso. All'atto dell'aggiornamento del DPS deve essere riportata la nuova versione del documento e la data della nuova versione.

I vecchi DPS sono conservati sia in formato elettronico che cartaceo.

1.5 Trattamento dei dati (Regola 19.1)

Identificativo	Descrizione sintetica	Categorie di interessati	Natura dei dati (P,S,G)	Strumenti utilizzati	Altre strutture che concorrono al trattamento (anche esterne)
D1	Anagrafiche e identificativi, inerenti lo stato di salute e/o presenza di handicap , comunicati dagli stessi o acquisiti dall'Azienda qualora rilevanti ai fini dei procedimenti di spettanza dell'Azienda	Clienti (inquilini)	P,S	Cartacei ed elettronici	
D2	Dati atti alla gestione dei bandi stessi e a calcolare il punteggio, handicap fisici ed eventuale stato di carcerazione , rilevanti ai fini del calcolo del punteggio	Generici	P,S	Cartacei ed elettronici	

D3	Nominativo, indirizzo, codici fiscali, certificati anagrafici, dati contabili), necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi o richiesti ai fini fiscali e previdenziali o dati di natura bancaria, conseguenti al rapporto di lavoro, ovvero inerenti i rapporti con gli enti previdenziali ed assistenziali, o dati giudiziari del personale dipendente, o inerenti l'adesione ad organizzazioni sindacali	Personale interno	P,S,G	Cartacei ed elettronici	
D4	Denominazione, indirizzo, nominativi dipendenti ecc..., concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai fini fiscali o dati di natura bancaria, certificazione antimafia, certificazione del casellario giudiziale, per l'eventuale ammissibilità a bandi di gara;	Fornitori	P,S,G	Cartacei ed elettronici	

Il trattamento di tali dati è fatto quasi esclusivamente all'interno dell'azienda, dai dipendenti della medesima; fanno eccezione i dati degli inquilini che sono utilizzati dalle ditte fornitrici addette alla manutenzione degli alloggi tramite una procedura di attivazione degli interventi relativi mediante richiesta trasmessa via modem. Questi dati vengono trattati e conservati in fascicoli riposti in schedari e armadi dotati di chiusura, nonché trattati tramite computer in rete.

1.6 Compiti, responsabilità, organizzazione e processi (Regola 19.2)

1.5.1 Organizzazione

ARTE (Azienda Regionale Territoriale Edilizia) ha sede legale a La Spezia, in via XXIV Maggio 369 (di seguito anche detta l'Organizzazione).

ARTE è Ente pubblico di natura economica, strumentale della Regione Liguria, dotata di personalità giuridica, di autonomia imprenditoriale, patrimoniale, organizzativa e contabile. L'Azienda ha la finalità di provvedere alla realizzazione di programmi di intervento e di gestione del patrimonio di edilizia residenziale pubblica sovvenzionata, agevolata e convenzionata nonché, di esplicare tutte le funzioni ad essa spettanti quale soggetto istituzionale operante nell'ambito dell'attività di uso e trasformazione del territorio e quale operatore pubblico dell'edilizia. L'Azienda esercita altresì tutte le funzioni ad essa trasferite o delegate dalla Regione.

La definizione dei responsabili delle attività individua in maniera definita le responsabilità interne e i referenti specifici per la gestione del progetto DPS. L'individuazione di specifici responsabili consente di poter usufruire di un flusso controllato delle attività sul sistema. I responsabili (referenti) delle varie attività devono garantire la corretta esecuzione di determinate attività di gestione del sistema. Per ragioni di sicurezza e di avvicendamento del personale (per esempio in caso di ferie o malattia) è opportuno definire più di una persona per ogni tipo di incarico.

1.4.1 Operazioni nelle quali consistono i Trattamenti

Macroprocessi		operazioni	Input	Output
	A1 System Managment	acquisizione, estrazione, utilizzo, organizzazione, comunicazione, archiviazione, cancellazione di informazioni	da funzioni interne	A funzioni interne
	A2 Segreteria, personale, Protocollo, Centralino, Copia, Legale, Appalti e Ragioneria	acquisizione, organizzazione, utilizzo, estrazione, comunicazione, archiviazione	Da clienti (inquilini), da fornitori, da funzioni interne	A clienti, a fornitori, a funzioni interne
	A3 Gestione alloggi	acquisizione, organizzazione, utilizzo, estrazione, comunicazione, archiviazione	da clienti (inquilini)	A clienti

1.4.2 Responsabilità e incarichi

Titolare	Competenze	Recapito
Titolare del trattamento dei dati per l'Azienda	Rapporti con i fornitori di sistemi informativi Gestione e aggiornamento DPSS Responsabile della sicurezza dei dati interna	Arch. Giancarlo RATTI Amministratore Unico A.R.T.E La Spezia

RUOLO	Uffici	Nominativi
Responsabile Trattamento Dati	Segreteria, Personale, Protocollo, Centralino, Copia, Legale, Appalti e Ragioneria	Dott. Umberto BIANCHI
Incaricati al trattamento dei dati	Segreteria e personale – dati comuni e sensibili del personale dipendente	Sanvenero Gabriella Cardellini Rossella Landi Paolo
Incaricati al trattamento dei dati	Legale – dati comuni e giudiziari per tutti coloro per i quali viene a crearsi una relazione avente profili di natura legale	Latin Caterina
Incaricati al trattamento dei dati	Protocollo, centralino, copia – dati comuni e/o sensibili di inquilini, fornitori e dipendenti	Gianardi Valeria Mulonia Riccardo Castiglione Silvia Cardellini Rossella
Incaricati al trattamento dei dati	Appalti – dati comuni e giudiziari dei fornitori	Bianchi Umberto Sanvenero Gabriella Landi Paolo
Incaricati al trattamento dei dati	Ragioneria – dati comuni e/o sensibili di inquilini, rapporti bancari, fiscali, assicurativi e tributari dell’Azienda	Bruni Lorena Cardellini Rossella Carleo M. Gloria Castiglione Barbara Lugieri Renza Portunato Margherita Tini Clelia Triffoni Alessandra
Responsabile Trattamento Dati	Gestione Alloggi	Dott. Sangriso Francesco
Incaricati al trattamento Dei dati	Gestione Alloggi – dati giudiziari e sensibili degli inquilini	Peri Paola Cocchetti Frida Latin Caterina Landi Paolo Malaspina Corrado Serantoni Sandra Stefanelli Stefano
Incaricati al trattamento Dei dati	Gestione Alloggi – dati giudiziari e sensibili dei partecipanti al bando di assegnazione degli alloggi	Peri Paola Cocchetti Frida Latin Caterina Landi Paolo Malaspina Corrado Serantoni Sandra Stefanelli Stefano

Responsabile Trattamento dati	Manutenzione e Patrimonio	Ing. Stefano Pollina
Incaricati al trattamento dei dati	Dati comuni dei fornitori, dati comuni e sensibili degli inquilini	Biggi Domenico Giacomazzi Alessandro Grandinetti Fulvio Marcotto Gabriele Menicagli Simona Moscatelli Carlo Pollina Fabio Ventura Massimo
Responsabile Trattamento dati	Nuove Costruzioni	Ing. Stefano Pollina
Incaricati al trattamento dei dati	Dati comuni dei fornitori e dati sensibili degli inquilini	Trapani Luca Alfieri P.Luigi Arnaboldi Carla Ferri Carlo Golinelli Marco Ghinoy Francesca Pescara Michele Rossi Francesco Spagnoli Marzia

TRATTAMENTI ESTERNI INCARICATI ESTERNI	
PROCEDURA	AZIENDA
Gestione Contabilità	D.P.2000 s.r.l. – La Spezia
Gestione Inquinato	D.P.2000 s.r.l. – La Spezia
Gestione Manutenzione	D.P.2000 s.r.l. – La Spezia
Rendicontazione Inquilini	D.P.2000 s.r.l. – La Spezia
Paghe	INAZ Paghe – Milano
Rilevazione presenze	INAZ Paghe – Milano
Assistenza, manutenzione rete, server e PC	D.P.2000 s.r.l. – La Spezia
Trasferimento dati	Ente Poste Italiane Spa
Visualizzazione dati	Imprese addette alla manutenzione ordinaria (vedi contratti di servizio)

NB: Le aziende di cui sopra (incaricati esterni) sono sottoposte al vincolo di riservatezza, tale vincolo e' esplicitato ed accettato nei contratti di servizio firmati dall'azienda fornitrice.

1.4.3 Descrizione del sistema informatico

Il sistema informatico dell'Organizzazione e' così strutturato :

Rete locale Ethernet 10/100 Mbit sec con Switch centrale 100Mbit/Sec e tre rilanci (Inquilinato, Manutenzione, Uff.Progetti) in cui sono posti Hub/Switch a 10/100MbitSec. Cablaggio Utp Cat 5 con protocollo di trasmissione Tcp/Ip ed Ethernet. Classe della rete "C"
Accesso esterno tramite Proxy Server Internet su router ADSL, collegamento per internet tramite ADSL gestita da un router connesso ad un firewall hardware
Server Unix HPUNIX per gli applicativi di Contabilità, Inquilinato, Bandi, Rendiconti e Manutenzione
File Server per Office e CAD
Server Microsoft 2003 Server R2 per la gestione di Protocollo, DL241 e Inventario con database Oracle 9
Server Microsoft 2000 per la gestione della procedura Linea32 dell'azienda STR
N. 2 PC con S.O. Windows 7
N. 3 PC con S.O. Windows 2000 professional
N. 40 PC con S.O. Windows XP

1.7 Analisi del rischio (Regola 19.3)

La progettazione di un sistema informativo sicuro richiede anche una corretta valutazione ed una individuazione dei possibili rischi di malfunzionamento. L'analisi dei rischi si occupa di :

- acquisire consapevolezza e visibilità sul livello di esposizione ai rischi del proprio patrimonio informativo;
- avere una mappa preliminare delle possibili contromisure di sicurezza da realizzare.

La metodologia di calcolo del rischio e' fatta come prodotto di due parametri :

P – probabilita' dell'evento (da 1 a 5) – in questo caso migliori sono le misure di sicurezza adottate minore e' la probabilita' dell'evento

I – impatto o gravita' del danno arrecato dall'evento (da 1 a 5) – l'impatto o la gravita' e' direttamente proporzionale al danno arrecato dall'evento

La seguente tabelle riporta i valori di soglia :

RISCHIO	
1-6	Basso
7-11	Pericoloso
12-25	Molto pericoloso

Di seguito viene fatta una analisi dei rischi, una valutazione dell'impatto sulla produttivita' dell'Organizzazione. Inoltre vengono evidenziate, dove presenti le contromisure gia' adottate, oppure le contromisure consigliate.

Rischio	Misure adottate	Misure da adottare	P	I	R
Perdita e danneggiamento dati elettronici (salvataggi) - la perdita ed il danneggiamento dei dati elettronici comporta dal fermo dei vari servizi al fermo delle attivita' dell'Organizzazione; comporta poi i costi di recupero (spesso re-inserimento dei dati)	Politica dei salvataggi e del recupero dei dati	Mettere in alta affidabilità i sistemi	5	2	10
Perdita e danneggiamento dati cartacei - Tale evento, grave comporta la perdita di informazioni e quindi il danneggiamento delle attivita'	Armadi e schedari contenente documentazione dotati di chiusura a chiave e posti in luoghi non accessibili ai non addetti	Dotarsi di armadi e schedari anti-incendio e anti-allagamento, dotarsi di sistemi elettronici per l'archiviazione del cartaceo (sistemi documentali) in modo da eliminare la custodia del cartaceo	2	5	10
Rischi dovuti all'utilizzo della rete e della rete pubblica (internet) - L'utilizzo improprio e incontrollato di internet puo' comportare lo spionaggio e la diffusione di informazioni riservate e la perdita di efficienza e di immagine dell'Organizzazione	Rete segregata, presenza di firewall di frontiera, disposizioni al personale di accesso a internet corretto	Monitoraggio della rete Introdurre sistemi di IDS	3	3	9
Black Out elettrico - Il black out elettrico comporta il blocco parziale o totale delle attività basate su elaboratori elettronici.	Gruppo di continuità, impianto elettrico a norma e sezionato, nonostante	Dotarsi di gruppo elettrogeno di sicurezza autonomo	2	5	10
Danneggiamento sistemi operativi, applicativi e danneggiamento hardware sistemi centrali	Sistema di controllo degli accessi, contratti di assistenza, salvataggi,	Introduzione di concetti di alta affidabilità e business continuità (cluster, load balancer, mirror) per i server 'critici' (data base server, firewall, application server)	4	2	8
Rottura e/o danneggiamento client periferici - Tale evento comporta il fermo delle singole postazione di lavoro e quasi mai il fermo del servizio. Nel caso di mancanza di parole chiave puo' comportare lo spionaggio di informazioni (dati personali e sensibili) e la fuga di notizie	Parole chiave a vari livelli, dominio introduzione dello screen saver, rimozione dei servizi software giudicati non necessari alle specifiche attività del PC		2	1	2
Computer affetti da virus - E' necessario disporre di un sistema antivirus centralizzato e potente	Sistema di antivirus centralizzato e sistema di gestione delle patch		1	4	4
Inefficienza della rete dati informatica - Il blocco della rete informatica comporta il blocco delle attività dell'ente		Introdurre sistemi di monitoraggio della rete	3	2	6

Trasmissioni di dati verso l'esterno che possono comportare la diffusione di dati riservati o sensibili	Disposizione di utilizzare supporti certi e sull'utilizzo corretto di internet	Introdurre sistemi di controllo automatico	3	2	6
Accesso non autorizzato di personale alle macchine	Utilizzo di credenziali robuste e di metodologie tracciate degli accessi		2	4	8
Accesso di personale ai dati sensibili	Emesse disposizioni sulle corrette norme comportamentali di sicurezza		2	3	6
Accesso di personale ai locali che contengono strumentazione e apparati	Locali chiusi e accesso consentito solo al personale autorizzato. Presenza di portineria e vigilanza Tracciamento degli accessi	Potenziare le difese passive ed inserire un sistema anti-intrusione	2	4	8
Controllo licenze e dei contratti di servizio dei prodotti software e hardware - Al fine di evitare azioni giuridiche da parte dei fornitori e' necessario disporre di tutte le licenze dei prodotti installate hardware e software.	Licenze presenti		1	3	3
Errore nella gestione delle procedure da parte del personale addetto	Piani di formazione sulla sicurezza e sulla privacy		1	2	2
Frode	Evidenziate le ricadute giuridiche e penali al personale		1	3	3
Alluvione, frane terremoti ed eventi naturali catastrofici possono provocare fermo del servizio oppure disservizio.	Le aree ed i locali potrebbero essere interessati da eventi , allagamenti pur avendo l'azienda provveduto ad adottare le disposizioni di sicurezza stabilite dalla L. 626/94. Data la natura del territorio il rischio può comunque definirsi basso	Installare un sistema di disaster recovery	1	4	4
Incendio		Introdurre un sistema di rilevamento fumi installare un sistema di disaster recovery	3	5	15

1.8 Misure di sicurezza da adottare (Regola 19.4)

1.8.1 Principi generali

Al fine di garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali rilevanti ai fini della loro custodia ed accessibilità, devono essere adottate le seguenti misure:

- per l'accesso ai computer e alla rete, si richiede autenticazione, identificazione e autorizzazione ad ogni Incaricato;
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- verifica che le misure di prevenzione idonee a scongiurare il pericolo di incendi (impianto elettrico a norma, idranti, estintori, disponibilità degli spazi per l'ingresso dei mezzi dei Vigili del Fuoco, etc.) siano in buono stato e funzionanti;
- regolamentazione nell'accesso ai locali e alle attrezzature che conservano dati, archivi e documentazione;
- attuazione di misure di protezione attiva e passiva nei locali ove si trattano dati personali (sistemi allarme, porte di ferro, inferriate, protezione di accesso agli uffici amministrativi, archivio);
- i fascicoli prelevati dall'archivio permangono al di fuori del sito per il tempo strettamente necessario e successivamente vengono riposti al proprio posto;
- i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento devono essere conservati e custoditi con le necessarie precauzioni;
- periodico salvataggio dei dati dei sistemi informatici (PC) su unità rimovibili e verifica periodica del buon funzionamento dei sistemi di salvataggio;
- adozione di procedure per la custodia di copie di sicurezza e per il ripristino della disponibilità dei dati e dei sistemi in caso di distruzione o danneggiamento;
- installazione, in tutte le sedi, dell'apparato firewall e monitoraggio continuo del corretto funzionamento dello stesso e installazioni tempestive dei correttivi al fine di proteggere tutta la rete locale delle varie sedi e di impedire accessi non autorizzati.
- adozione di procedure di gestione delle credenziali di autenticazione. La password deve essere composta da almeno 8 caratteri, non deve contenere nomi comuni, nomi di persona, riferimenti agevolmente riconducibili all'incaricato. Inoltre la password deve essere modificata al primo utilizzo e successivamente modificata con cadenza semestrale.

Le apparecchiature devono essere opportunamente collocate o protette per ridurre rischi da minacce e alee ambientali. Devono essere create aree sicure allo scopo di proteggere le attrezzature con particolari esigenze di sicurezza. Le aree sicure devono essere protette da opportuni controlli d'ingresso per assicurare che l'accesso sia consentito ai soli autorizzati.

1.8.2 Norme comportamentali e internet

Sono disposte le seguenti norme comportamentali a tutti il personale per la gestione di internet e della propria dotazione (Personal computer ecc ecc) :

- si è vietata la navigazione su siti di hacking, cracking o sui siti illegali (pedofilia ecc ecc);
- si è vietato scaricare software da siti poco attendibili o non ufficiali;
- si è disposto di non aprire messaggi di posta elettronica e di non eseguire files allegati ai messaggi senza preventiva scansione antivirus;
- si è fatto divieto di installare programmi scaricati da siti non ufficiali o comunque di natura incerta e di non dar credito a un messaggio pubblicitario dalle caratteristiche sospette;
- si è disposto di tenere sempre attivata l'opzione del browser "richiedi conferma" per l'installazione e il download di oggetti;
- la casella di posta elettronica dell'Organizzazione è considerata strumento di lavoro e si è disposto che debba essere utilizzata esclusivamente per esigenze lavorative, così come gli accessi ad internet vanno effettuati per dette finalità;
- si è disposto che non siano lasciati incustoditi sulle scrivanie, o su altri ripiani, atti, documenti e fascicoli delle pratiche in luoghi accessibili a terzi non autorizzati;. i fascicoli vanno conservati negli appositi schedari;
- si è data disposizione che il materiale cartaceo non sia visibile o visionabile dal cliente o da terzi allorquando vengono autorizzati ad accedere all'interno dell'azienda o dei collaboratori ovvero alla postazione di lavoro degli incaricati;
- le comunicazioni a mezzo posta, o a mezzo telefax, dovranno essere tempestivamente protocollate smistate e consegnate ai destinatari. Quando è dato un ordine di stampa, il documento stampato dovrà essere prelevato e consegnato all'interessato.

1.8.3 Sicurezza fisica dei locali

I locali in cui vengono poste apparecchiature elettroniche particolarmente critiche per la gestione dei dati (locali tecnici di ARTE) quali computer server che contengono banche dati con dati sensibili, personal computer che contengono banche dati con dati sensibili e apparati di rete centrali devono rispettare norme di sicurezza di accesso e di struttura tali da garantire la sicurezza globale del sistema. Si prevedono le seguenti caratteristiche:

- accesso ai locali tramite chiave o sistema elettronico di accesso (badge);
- accesso ai locali consentito solamente agli amministratori di sistema o agli incaricati alla gestione dei dati sensibili;
- credenziali di accesso fisico (chiavi o badge) rilasciate alle sole persone autorizzate (tecnici interni ed esterni per interventi sul sistema, personale interno o esterno addetto ai salvataggi);
- sistema di condizionamento della temperatura;
- presenza di difesa passiva (inferiate e porte blindate); registrazione degli accessi in opportuno 'documento degli accessi ' (vedi allegato 'A').

1.8.3 Protezione da malware

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita degli stessi a causa di virus informatici, il Titolare o Responsabile del trattamento dei dati stabilisce, con il supporto dell'Amministratore di Sistema, quali protezioni software adottare in relazione all'evoluzione tecnologica dei sistemi disponibili sul mercato.

Il Titolare o Responsabile del trattamento stabilisce inoltre la periodicità (consigliata almeno giornaliera per i computer connessi in rete, mentre per i computer che non sono connessi in rete un periodo ragionevole può essere almeno mensile), con cui devono essere effettuati gli aggiornamenti dei sistemi antivirus utilizzati per i sistemi non dotati di collegamento in rete, al fine di ottenere un accettabile standard di sicurezza dei dati trattati.

E' opportuno che gli Incaricati che utilizzano i sistemi informatici annotino gli eventuali virus rilevati, e, se possibile, la fonte da cui sono pervenuti, al fine di isolare o comunque trattare con precauzione i possibili portatori di infezioni informatiche.

Nel caso in cui su uno o più sistemi si dovesse verificare perdita di informazioni o danni a causa di infezioni o contagio da virus, il Titolare o Responsabile del trattamento, unitamente all'Amministratore di Sistema, deve provvedere a:

- isolare il sistema;
- verificare se ci sono altri sistemi infettati con lo stesso virus informatico;
- identificare l'antivirus adatto e bonificare il sistema infetto;
- verificare il buon funzionamento dell'antivirus su tutti gli altri sistemi.

L'Organizzazione ha provveduto all'introduzione di un sistema AntiVirus che viene aggiornato in maniera automatica; per ogni singolo computer è prevista la funzione di aggiornamento automatico delle patch del sistema operativo Microsoft mediante lo strumento windows – update.

1.8.4 Utilizzo dei supporti magnetici

L'utilizzo ripetuto dei supporti magnetici (Dat, Floppy Disk, DLT, CD ecc ecc), in taluni casi, a causa del fatto che i programmi software di scrittura non cancellano completamente le precedenti registrazioni, può comportare che restino sui supporti magnetici informazioni riservate relative a dati sensibili. Al fine di evitare che i supporti magnetici vengano ispezionati e vengano estratti da essi eventuali dati sensibili che vi sono rimasti e' necessario cancellare tutte le tracce reperibili dei medesimi prima di divulgare i supporti magnetici.

Si prevede che prima del riutilizzo di particolari supporti magnetici si proceda secondo la seguente metodologia:

- nel caso di floppy disk eseguire l'operazione di formattazione *C:>format a:*
- nel caso di floppy disk unix eseguire l'operazione di formattazione *#format /dev/rfd<formato>*
- nel caso di DAT e/o DLT eseguire l'operazione di inizializzazione (a carico del gestore del sistema)

Sono esclusi da questa attività i supporti utilizzati per i salvataggi interni, poiché, comunque restano all'interno dell'Organizzazione.

1.8.5 Trasmissione dei dati

E' abilitato alla trasmissione dati tramite la rete Internet l'amministratore di sistema o suo delegato, che, contestualmente alla trasmissione dei dati, verifica la correttezza dei dati trasmessi.

E' abilitato alla trasmissione dati tramite supporti magnetici l'amministratore di sistema che, contestualmente alla trasmissione dei dati, verifica la leggibilità e la correttezza dei dati trasmessi.

L'utilizzo di internet è disponibile su vari livelli per più utenti (senza alcun vincolo nel sistema) ed i servizi disponibili sono :

- servizio ftp (transfer files);
- servizio di mail;
- servizi di navigazione e mailing diretti e/o tramite accesso controllato da Proxy Server.

L'attività di controllo del corretto utilizzo di internet è fatta dall'utente stesso che esegue l'operazione.

1.8.6 Autenticazione

Ciascun computer è dotato di una password a livello di bios e ciascun server di una password di amministratore. Inoltre si è disposto che tutti gli utilizzatori di strumenti elettronici non lascino incustodito, o accessibile, lo strumento elettronico stesso.

A tale riguardo, per evitare errori e dimenticanze, è stato inserito lo screensaver automatico dopo 5 minuti di non utilizzo, con ulteriore password per la prosecuzione del lavoro.

1.8.7 Gestione delle credenziali

Periodicamente è disposto di procedere alla revisione delle credenziali di accesso ai sistemi informatici (utente/password) e con il controllo dello stato delle medesime allo scopo di verificare che non ci siano credenziali non utilizzate.

Deve essere creato e gestito un documento contenente la lista utenti/password di livello amministratore che sia periodicamente aggiornato e custodito in modo sicuro.

1.8.8 Network

E' previsto di eseguire la verifica che il carico di rete sia all'interno dei valori consentiti. E' predisposto un test per il controllo periodico da parte dell'amministratore di sistema del carico di rete.

Gli accessi alla rete sono consentiti al solo personale autorizzato.

La rete deve essere segregata e protetta tramite opportuni firewall (hardware o software) nelle sue zone di frontiera.

1.9 Procedure di salvataggio e ripristino dei dati (Regola 19.5)

1.9.1 Linee guida per i salvataggi ed il ripristino dei dati

L'attività di salvataggio e ripristino dei dati di un sistema informativo è fondamentale per la messa in sicurezza del medesimo e la garanzia della stabilità delle informazioni. Pertanto tale attività deve essere pianificata e certificata in

modo rigoroso. L'attività' di salvataggio deve essere tale da consentire un veloce ripristino del sistema a fronte di un crash fisico delle macchine server.

Il risultato del salvataggio e' memorizzato in un opportuno file di log consultabile da parte del responsabile dei salvataggi. Ad ogni esecuzione del salvataggio il responsabile del controllo del salvataggio deve eseguire il controllo del buono esito dell'operazione e certificarlo.

Il salvataggio è eseguito utilizzando supporti magnetici sequenziali ed è attivato automaticamente dalla macchina in determinati orari (in tale caso il responsabile dei salvataggi deve solamente accertarsi di cambiare le cassette secondo la corretta sequenza) ed eseguire la verifica dei log files delle attività.

I supporti magnetici sono conservati in un luogo distinto (ufficio sig.ra Bruni) dal luogo dove sono installati i computer critici al fine da evitare in caso di disastro (incendio, crollo dei locali ecc ecc) di perdere assieme ai computer critici anche i salvataggi.

L'attività di salvataggio deve essere tracciata in un opportuno registro dei salvataggi in cui è annotato:

- autore del salvataggio, data e ora del lancio
- autore del controllo del salvataggio, data e ora del controllo
- tipo del salvataggio (statico, dinamico o altra)

L'allegato "B" fornisce il formato del registro per la scrittura dei salvataggi.

I supporti magnetici sequenziali su cui si effettuano i salvataggi devono essere predisposti ed utilizzati secondo la seguente regola di salvataggio:

- disponibilità di numero 6 supporti oppure numero 6 gruppi di supporti qualora siano necessari (uno per giorno della settimana) dedicati ai salvataggi dinamici. Ogni giorno ha un supporto rigorosamente assegnato che deve essere utilizzato per il salvataggio di quel giorno (Lun, Mar, Mer, Gio, Ven, Sab). Il responsabile dei salvataggi introduce il supporto giornaliero e registra l'attività nel registro dei salvataggi.
- disponibilità di un numero sufficiente di supporti dedicati a salvataggi particolari

1.9.2 Piano dei salvataggi dei dati

Il Titolare, o il Responsabile del trattamento con il supporto dell'Amministratore di Sistema, stabilisce la periodicità con cui debbono essere effettuate le copie di sicurezza delle banche dei dati trattati. In particolare per ogni banca dati devono essere definite le seguenti specifiche:

- il tipo di supporto da utilizzare per le copie di back-up;
- il numero di copie di back-up effettuate ogni volta;
- se i supporti utilizzati per le copie di back-up sono riutilizzati e in questo caso con quale periodicità;
- se per effettuare le copie di back-up si utilizzano procedure automatizzate e programmate;
- trasposizione dei dati informatici su unità rimovibili;
- la durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati;

Banca dati / data base / archivio dati	Criteria e procedure per il salvataggio e il ripristino dei dati	Pianificazione delle prove di ripristino
Contabilità, manutenzione e gestione alloggi	Backup notturno giornaliero che crea e salva i dati su cassetta DDS tramite istruzione tar	Semestrale
Protocollo, paghe e documenti shared	Backup tramite ntbackup attivato in notturno e con procedimento di salvataggio su nastro. Il controllo dell'esito della procedura di salvataggio è possibile tramite l'icona sul DeskTop del server	Semestrale
Dati su PC	Il salvataggio dei dati presenti sui personal computer è demandato ai singoli dipendenti che possono optare su una apposita cartella personale su file server oppure di copiarli su CD	A carico dell'utente

1.9.3 Piano di ripristino dei dati

Nell'ipotesi di distruzione o danneggiamento dei dati o degli strumenti elettronici, si è predisposto apposito piano di ripristino degli stessi, impartendosi comunque sin d'ora le seguenti istruzioni:

- avvertire il titolare del trattamento dei dati e l'incaricato che ha in custodia il nastro di backup nonché i CD contenenti i vari software dell'azienda installati sugli strumenti elettronici;
 - rivolgersi immediatamente e chiedere l'intervento del tecnico manutentore del sistema informativo sollecitandone al più presto l'assistenza;
 - reinstallare i programmi danneggiati o distrutti, sempre che non sia necessario sostituire l'intero hardware, provvedere a reinstallare tutti i dati contenuti nei nastri di back up;
 - provvedere all'aggiornamento dei sistemi operativi una volta reinstallati;
- verrà dato incarico al tecnico manutentore di suggerire ogni altra misura;

In ogni caso, viene data esplicita istruzione che il ripristino dei dati e dei sistemi sia effettuato entro e non oltre 7 giorni;

1.10 Formazione degli incaricati (Regola 19.6)

1.10.1 Generalità

Aspetto fondamentale nella gestione dei dati sensibili e' la preparazione e la capacita' degli addetti (utenti e amministratori) in tale attività. A tale scopo e'

necessario che le singole figure previste nel DPS abbiano sia conoscenza di Informatica di Base che conoscenze specifiche al problema.

Gli addetti alla gestione dei dati sensibili sono formati alle seguenti attività:

- entrata controllata nel sistema
- informatica di base e utilizzo del Computer (office, applicativi particolari)
- formattazione o reinizializzazione dei supporti magnetici
- responsabilità giuridiche per la gestione dei dati sensibili
- utilizzo di internet

Gli addetti alla amministrazione del sistema sono formati alle seguenti attività:

- esecuzione e controllo dei salvataggi
- esecuzione del ripristino
- entrata controllata nel sistema
- informatica di base e utilizzo del Computer (office, applicativi particolari)
- verifica della sicurezza degli accessi
- aggiornamento del DPS
- verifica dei supporti magnetici per la trasmissione dati
- utilizzo di Internet
- verifica della corretta applicazione delle norme di sicurezza
- responsabilità giuridiche nella gestione dei dati

Gli utenti generici sono formati alle seguenti attività:

- informatica di base e utilizzo del Computer (office, applicativi particolari)
- utilizzo di Internet

A tutti gli Amministratori di Sistema e di dati e' fornito il presente DPS di cui prendono visione e lettura al fine di essere sensibilizzati alla problematica della gestione dei dati sensibili e relative responsabilità e di individuare nel DPSS la parte di proprio specifico interesse e competenza.

La formazione degli incaricati viene effettuata al momento dell'assunzione, all'installazione di nuovi strumenti per il trattamento dei dati e comunque con frequenza annuale. Essa tende a sensibilizzare gli incaricati sulle tematiche di sicurezza, facendo comprendere i rischi e le responsabilità (con specificazione delle sanzioni connesse penali e disciplinari) che riguardano il trattamento dei dati personali. Destinatari della formazione sono i dipendenti e collaboratori. Inoltre, la formazione tende alla compiuta spiegazione del concetto di quale sia la natura ed il contenuto dei dati personali, sensibili e giudiziari, con l'invito a segnalare eventuali disfunzioni dei sistemi operativi e, per ogni dubbio, di richiedere al titolare. La formazione è fatta tramite consulenze di ditte esterne o a-learning.

1.10.2 Piano di formazione

Obiettivi: istruire e sensibilizzare le risorse umane incaricate, secondo i diversi ruoli e responsabilità, nei confronti: <ul style="list-style-type: none"> • dell'importanza della sicurezza informativa e dei principi e pratiche di sicurezza • dei rischi connessi al trattamento di dati personali; • delle misure di protezione da adottare per mitigare i rischi; • delle misure di prevenzione e detenzione disponibili, secondo l'evoluzione tecnica; • delle implicazioni legali e disciplinari. 			
Azioni:			
Tutti i Neoassunti	Nel training	Corso di base su privacy	Consulenti esterni o a-learning
Incaricati nei casi di cambio di mansioni	QN	Istruzioni sui processi sotto l'aspetto della protezione dei dati personali	Consulenti esterni o a-learning

1.11 Trattamenti affidati all'esterno (Regola 19.7)

Nel caso di attività affidate a terzi che comportano il trattamento di dati, è necessario che la società a cui viene affidato il trattamento rilasci specifiche dichiarazioni o documenti, oppure assuma alcuni impegni, anche su base contrattuale, con particolare riferimento, ad esempio, a:

- trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto;
- adempimento degli obblighi previsti dal codice per la protezione dei dati personali;
- rispetto delle istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o integrazione delle procedure già in essere;
- 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.

Nel caso in cui il trattamento dei dati venga affidato a soggetti esterni, che li trattino con strumenti elettronici, per avere la garanzia che essi adottino le misure minime di sicurezza si esigerà dagli stessi una dichiarazione di avere redatto il documento programmatico sulla sicurezza, nel quale attestino di aver adottato le misure minime previste dal disciplinare.

Alle ditte che provvedano ad effettuare prestazioni che comportano accesso di estranei all'azienda, viene dato incarico scritto con richiesta di specificazione dei nominativi delle persone che accedono ed espresso invito a limitarsi alle sole attività pertinenti alla prestazione per cui accedono.

Tutte le misure di sicurezza indicate, salvo quelle da attuarsi, devono intendersi in essere, e vengono sottoposte a verifica dal titolare nel corso dell'anno.

Non sono rilevati, al momento della stesura di questo documento, trattamenti di dati esterni.

1.12 Cifratura e Speciali Misure di Protezione nel Settore Sanitario (Regola 19.8)

Non applicabili in quanto l'Organizzazione non rientra tra i soggetti di cui al p. 24 all. B) (organismi sanitari e esercenti professioni sanitarie). Tuttavia l'Organizzazione utilizza tecniche di cifratura allo scopo di proteggere la riservatezza di determinate informazioni ritenute meritevoli di speciale protezione.

