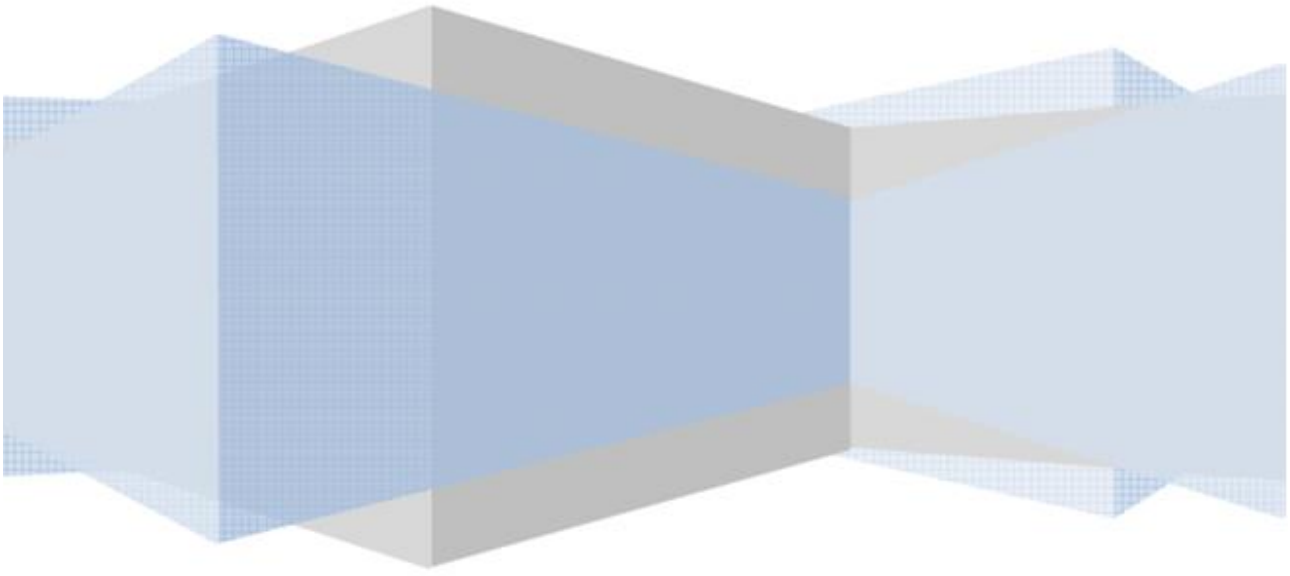
Città Metropolitana
di Genova

PIANO PER LA SICUREZZA INFORMATICA

ANNO 2015



Sommario

1. Introduzione

Il presente documento si propone di descrivere gli accorgimenti organizzativi e tecnici che la Città Metropolitana di Genova mette in atto per applicare correttamente le misure di sicurezza previste dalla normativa.

2. Finalità.

Scopo di questo documento è di garantire la protezione del patrimonio informativo da rilevazioni, modifiche o cancellazioni non autorizzate per cause accidentali o intenzionali e ridurne gli effetti causati dall'eventuale occorrenza.
Le misure di sicurezza organizzative, fisiche e logiche adottate e da adottare affinché siano rispettati gli obblighi, in materia di sicurezza, devono essere conformi al Codice in materia di protezione dei dati personali approvato con Dlgs. 30 giugno 2003 n.° 196, al fine di assicurare la riservatezza e la salvaguardia dei dati personali trattati dall' Ente.

3. L'architettura dell'infrastruttura informatica di rete

Con Delibera della Giunta Provinciale N.175 del 17 giugno 2008 la Provincia di Genova ha autorizzato la sottoscrizione della Convenzione tra Regione Liguria e Provincia di Genova per l'attuazione del progetto istituzionale "Liguria in rete" e con Delibera della Giunta Provinciale N.55 del 22 aprile 2014 ha approvato il rinnovo della stessa per ulteriori 5 anni.
In data 3/09/2008 Regione Liguria e Provincia di Genova hanno sottoscritto la Convenzione "Liguria in Rete" e in data 13/06/2014 hanno sottoscritto il rinnovo della stessa per collaborare nell'interscambio d'esperienze e di apporti conoscitivi anche sotto il profilo organizzativo, applicativo e tecnico per la realizzazione dei comuni obiettivi di innovazione del ruolo della Pubblica Amministrazione nel quadro del processo di organizzazione e decentramento amministrativo.
Ai fini dell'attuazione di tale Convenzione Regione Liguria e Provincia di Genova si sono impegnate a che le rispettive Strutture organizzative competenti sull'informatizzazione, anche in forma congiunta con le Strutture regionali competenti per specifico ambito tematico, mantengano in modo continuativo rapporti con l'obiettivo di:

- individuare le iniziative e i progetti da realizzare;
- identificare progetti comuni di sviluppo della Società dell'Informazione e di e-government da inserire nei propri Piani;
- sottoporre i progetti e le iniziative di cui sopra all'approvazione delle rispettive Amministrazioni;
- monitorare le fasi di attuazione;
- rendere disponibili ad altre amministrazioni pubbliche quanto realizzato congiuntamente nella logica del riuso.

All’Art. 5 di tale Convenzione, Regione Liguria e Provincia di Genova , hanno altresì convenuto di adottare appositi Piani Attuativi per definire i dettagli di specifiche attività che di comune accordo si vorranno intraprendere.
Successivamente nella seduta del 16 settembre 2008 la Giunta Provinciale ha condiviso l’affidamento in housing delle attrezzature più critiche presenti nelle proprie sale servers, in quanto la gestione delle diverse sale server dell’Amministrazione risultava particolarmente onerosa sia in termini di infrastrutture che di risorse umane e strumentali.
Infine con Deliberazione della Giunta Provinciale N.120 Protocollo Generale 63939/2009 la Provincia di Genova ha approvato il Piano Annuale di Attuazione 2009, in attuazione degli obiettivi previsti dalla Convenzione “Liguria in rete”, nel quale all’Azione 4 era previsto il trasferimento dei sistemi dell’Amministrazione provinciale presso la Server Farm della Regione Liguria.
Nei successivi Piani Annuali di Attuazione del 2010, 2011, 2012, 2013 e 2014 la Giunta Provinciale ha sempre confermato il mantenimento dei propri sistemi presso la Server Farm della Regione Liguria.

1.1. Sito Primario

In conseguenza di quanto sopra i sistemi della Città Metropolitana di Genova sono collocati nella Server Farm della Regione Liguria, gestita dalla società in house della Regione stessa “Liguria Digitale Scpa”, in grado di fornire adeguati livelli prestazionali, di sicurezza e opportune condizioni ambientali sia alle infrastrutture informatiche sia a quelle di rete.

1.2.Caratteristiche dei Locali

- 800 mq di spazio già suddivisi in otto locali;
- accesso carrabile al piano, che rende agevole la movimentazione di materiali pesanti e/o voluminosi ;
- area destinata a Computer Room appositamente partizionata in sale tecniche separate e distinte, con propri accessi indipendenti controllati;
- sala di controllo, dove sono concentrate le console in accesso remoto verso ciascun server, oltre ai pannelli di controllo degli strumenti di gestione delle reti e dei sistemi;
- condizionamento attivabile e regolabile in modo indipendente in ciascuna sala;
- centrale di condizionamento ridondata in doppio;
- quadro elettrico di distribuzione autonomo in ciascuna sala;
- isolamento da ambienti confinanti a livello: acustico, elettrico, telefonico;
- le uscite di sicurezza dotate di sensori di allarme centralizzati su un sistema di monitoraggio;

- pavimento tecnico sopraelevato con canalizzazione distribuita a griglia (sotto pavimento) in ciascuna sala, che permette di facilitare la stesura dei cavi e mantenere ordinato il cablaggio;
- facilità di provisioning WAN-MAN, grazie alla disponibilità di una sala trasmissiva comune (arrivo delle fibre ottiche dai carrier), attrezzata con struttura di fila a standard Telecom e con permutatore verso le sale tecniche. Tale soluzione consente di riconfigurare o potenziare i collegamenti di rete in modo agevole e con impatti minimi o nulli sulla continuità di servizio;
- ampi spazi per il magazzino "materiali di consumo" e "parti di ricambio.

1.3.Principali servizi impiantistici ed infrastrutturali

a) *Rilevazione fumi e spegnimento incendi*. Tutti gli ambienti della sede sono dotati di rilevatori antifumo e antincendio con attivazione dei relativi impianti di spegnimento automatico degli incendi a saturazione di ambiente con estinguente chimico gassoso. L'impianto di spegnimento è stato progettato nel pieno rispetto della normativa UNI 9795 che garantisce la segmentazione dell'impianto e di conseguenza la perdita delle sole zone oggetto di eventuale incidente o calamità naturale ed il continuo funzionamento del resto dell'impianto.

b) *Anti allagamento*. Sono previste delle sonde di rilevazione presenza liquidi nel sottopavimento in prossimità dei raccordi, delle valvole e delle derivazioni principali dell'impianto di distribuzione dell'acqua. Eventuali fuori uscite di acqua sono opportunamente allontanate mediante convogliamento e scarico verso l'esterno.

c) *Anti intrusione*. E' attivo un sistema di anti intrusione integrato con il sistema di Telecamere a circuito chiuso. I sensori del sistema allocati all'interno dell'edificio sono attivati e disattivati da segnali provenienti dal sistema di controllo accessi.

d) *Telecamere a circuito chiuso*. Le telecamere sono posizionate per il controllo del perimetro dell'edificio, degli ingressi, delle porte interbloccate e di eventuali altre zone critiche. Il sistema TVCC è predisposto per attivazione tramite "motion detection".

e) *Condizionamento*. Le condizioni di temperatura delle singole computer room sono regolate tramite termostati situati nelle suddette computer room.

f) *Continuità ed Emergenza.* Sono presenti tre gruppi di continuità (UPS) centralizzati da 200 KVA ciascuno, operanti in parallelo. Gli UPS assicurano la continuità a tutti i dispositivi informatici. Tali gruppi sono tenuti sotto monitoraggio 7x24. In caso di prolungata assenza di alimentazione elettrica vengono automaticamente attivati due gruppi elettrogeni, in grado di garantire un' ampia autonomia di servizio

g) *Alimentazione a 48 V*. Le due sale TLC sono equipaggiate con alimentazione a 48 V per gli apparati di telecomunicazione.

h) *Controllo degli accessi fisici all'IDC*. Il personale che accede in nome e per conto dei Clienti è soggetto a procedure di registrazione degli accessi e identificazione del

personale stesso. L'accesso alle sale sistemi è controllato elettronicamente tramite badge.

i) *Connettività*. La connettività esterna per la raggiungibilità delle apparecchiature via rete pubblica (banda internet) o rete dedicata privata (rame o fibra ottica) è concentrata in apposita sala TLC. Attualmente presso i locali vi sono attestazioni di rete a Fibra Ottica dei principali fornitori di TLC .

l) *Sistema di gestione e remotizzazione allarmi*. Gli eventuali allarmi rilevati sono registrati ed inoltrati anche a distanza. In ogni locale vengono effettuati due tipi di controlli:
   - automatici
   - manuali.

I controlli automatici sono effettuati tramite SW o apparecchiature e prevedono controlli di temperatura, erogazione corrente elettrica sugli UPS, funzionamento gruppi elettrogeni, funzionamento chiller, accessi, allagamento ed incendio, intrusione perimetrale.
I controlli manuali sono effettuati a periodi fissi e prevedono:

- controllo delle temperature e di eventuali problemi all'infrastruttura eseguiti da Servizio di Vigilanza con periodicità giornaliera
- controllo funzionamento infrastruttura del locale eseguito giornalmente dal personale del Data Center
- controllo quadri elettrici secondo le normative sulla sicurezza (4 volte all'anno)
- controllo condizionamento con pulizia e regolazioni ove necessario (4 volte all'anno)
- controllo impianto allarmi e pulizia sensori ove necessario (2 volte all'anno)
- controllo impianto spegnimento (2 volte all'anno)
- controllo Gruppi di continuità (2 volte all'anno)
- controllo Gruppi elettrogeni (controllo settimanale)

Tutta l'infrastruttura e gli impianti in essa funzionanti sono sotto costante controllo automatico 7x24.
Gli apparati e i server sono alloggiati in appositi locali e interconnessi con reti Lan di tipo Ethernet 10/100/1000 Mbps o Fibre channel.
Dal punto di vista networking sono disponibili:

- Accesso alla rete dei principali carrier
- Accesso ad Internet ed alla rete SPC tramite Autonomous System (BGP)
- Sistemi di sicurezza perimetrale (firewall, Ids/Ips e concentratori VPN dedicati su infrastruttura centralizzata in High Availability)

- Gestione di un sistema L4/7 switching per alta disponibilità e bilanciamento del carico

1.4.La gestione dei servizi

I servizi sono gestiti in parte su server fisici, in parte su server virtualizzati ed in parte sulla SAN.

- I server fisici comprendono servizi web, storage non primario ed infine 4 server VMWARE necessari alla virtualizzazione, Server FAX (gestione ricezione e invio fax automatizzato).
- I server virtualizzati, compresi nei 4 server citati in precedenza, comprendono gestione DB e front-end di gestione procedure interne

I server fisici sono in numero di 8, mentre i server virtualizzati sono in numero di 10.
Nella server Farm regionale è stato messo a disposizione della Città Metropolitana di Genova un ambiente virtualizzato (SAN - Storage Area Network), al fine di permettere il funzionamento dei seguenti servizi:

- SQL Server (SQL Server Microsoft)
- Gestione foresta domini AD (windows 2003/2008)
- Storage (windows storage)
- Spooler di stampa (windows server con gestione delle code)
- Gestione servizi al cittadino (portali internet: sito istituzionale, trasparenza, etc.)

Il servizio di virtualizzazione è fornito su una struttura VMWare VSphere ESX 5.x, su sistema blade HP C class, con gestione dell'alta disponibilità.
L'area Storage è costituita da un'infrastruttura SAN HP EVA8000 su cui sono riservati 6 TB lordi suddivisi tra dischi FATA e FC (questi ultimi limitatamente all'utilizzo fino ad un massimo di 100GB per l'utilizzo del DB Server) con collegamento dual-path.
La configurazione di rete prevede la suddivisione in "inside" e DMZ, con protezione perimetrale.

1.5.La gestione dei Server Fax

La ricezione e l'invio dei fax da parte dei dipendenti della Città Metropolitana di Genova viene gestita tramite un'infrastruttura client-server che si basa sul software Achab RelayFax (vers. 6.x).
Il server RelayFax si integra con il mail server esistente, nel nostro caso Microsoft Exchange, e consente la gestione dei messaggi fax in entrata e uscita tramite il sistema di posta elettronica stesso.
RelayFax converte i fax in messaggi di posta elettronica, cioè in email.
Dalla postazione che trasmette il fax, viene inviata un'email che viene "parcheggiata" in una delle caselle POP dedicate sul mail server che ad intervalli regolari e configurabili,

recupera i messaggi dalle caselle postali, li converte in formato inviabile via fax (TIFF) e li trasmette.
La ricezione avviene in maniera analoga: i fax ricevuti da RelayFax tramite il fax-modem, collegato al centralino mediante 8 linee telefoniche, vengono convertiti in immagini o in file PDF. Tali immagini o PDF vengono allegati a messaggi di posta elettronica e inviati alle caselle postali degli utenti del mail server. RelayFax può essere configurato anche per selezionare il numero dell'ISP e connettersi a server di posta esterni, che possono tenere "in deposito" i messaggi che si vogliono inviare come fax.
Questo sistema permette una sofisticata gestione dei fax in ingresso e in uscita: con delle regole personalizzabili è possibile instradare automaticamente i fax in ingresso verso alcune persone o dipartimenti, per esempio in base al numero del mittente o in base al numero chiamato.

1.6. La gestione dei backup

La struttura prevista per l'erogazione del servizio di backup è stata concepita in modo da offrire elevati livelli di affidabilità e gestibilità. Si tratta di una architettura centralizzata, basata sulla tecnologia EMC Legato specializzata nella gestione dei processi di salvataggio e ripristino dei dati residenti sui sistemi informatici.
La soluzione architetturale prevede una modalità di salvataggio disc-to-disc, mediante utilizzo di tecnologia Storage Data Domain (o equivalente), al fine di velocizzare il processo di backup (ed eventualmente di restore per dati recenti), con un trasferimento su nastro in differita per le archiviazioni secondo i piani di "retention" definiti.
La piattaforma di backup risiede in apposito locale ad accesso controllato ed adibito alla specifica funzione.
L'utilizzo dello Storage Data Domain permette, rispetto all'utilizzo delle normali Librerie per i backup, di poter eseguire backup e restore contemporaneamente, di effettuare i cloni pur continuando a fare i backup, di ottimizzare lo spazio utilizzato dai dati salvati.
L'uso dei cloni permette di avere una doppia copia dei dati. Tale copia può essere messa in cassaforte presso la Sede della Società in house Liguria Digitale Scpa, che gestisce la Server Farm regionale, o essere depositata presso il Cliente (previo accordo).
Normalmente tutti i backup eseguiti durante i 3 cicli giornalieri sono replicati in tempo reale su opportuno Storage Data Domain ubicato in sede diversa dalla Server Farm.
A livello di erogazione di servizio, questa struttura è parte integrante di quella generale di gestione dei backup da parte della Società in house Liguria Digitale Scpa e permette una ridondanza in grado di assicurare una elevata disponibilità del servizio.
Le politiche di backup prevedono quanto segue:

- I dati salvati hanno validità (retention) di 3 settimane. Le archiviazioni mensili hanno validità 1 anno.

- I cicli sono 3. Ognuno è composto da un salvataggio full effettuato durante il fine settimana e 6 incrementali ad esso logicamente collegati che vengono effettuati la sera dei giorni precedenti il successivo salvataggio full. Alla quarta settimana i dati presenti sullo Storage Data Domain vengono rimossi seguendo la politica di retention del punto precedente.
- Tutti i backup eseguiti durante i 3 cicli sono replicati in tempo reale su opportuno Storage Data Domain ubicato in sede diversa dalla Server Farm.

1.7.Sito Secondario

Nel Piano Annuale di Attuazione 2014 (approvato con Deliberazione della Giunta Provinciale N.150 Protocollo Generale 106430/2014) la Città Metropolitana di Genova ha manifestato l'intenzione di adottare, quale soluzione tecnologica per la continuità operativa e il Disaster Recovery, quella prevista nello studio di fattibilità tecnica presentato dalla Regione Liguria all'Agenzia per l'Italia Digitale con nota dell'08/02/2013 e da quest'ultima acquisito con proprio protocollo N.1067.
Nello stesso piano la Regione Liguria ha manifestato il proprio assenso a considerare nel dimensionamento complessivo del proprio sito di Disaster Recovery, gli apparati, i dispositivi e le risorse della Provincia di Genova attualmente ospitati presso la sala server regionale.

4. Analisi delle minacce e delle vulnerabilità dell'infrastruttura informatica di rete

ANALISI DEI RISCHI					
Descrizione rischi (1) (Elenco possibili rischi a cui sono esposti i dati)		Impatto sulla sicurezza dei dati			
		impatto sui beni (2)	Probabilità della minaccia/vulnerabilità (3)	Misura del rischio (impatto x probabilità) (4)	Classifica del rischio
Comportamenti degli operatori	Sottrazione di credenziali di autenticazione (Accesso non consentito ai dati Sottrazione, cancellazione, manomissione, diffusione dei dati)	5	3 per i client 1 per i servers	15 per i client 5 per i servers	altissimo per i client medio per i servers
	Carenza di consapevolezza, disattenzione, incuria (Cancellazione,manomissione e diffusione dei dati)	4	3 per i client 1 per i servers	12 per i client 4 per i servers	altissimo per i client medio per i servers

ANALISI DEI RISCHI					
	Descrizione rischi (1) (Elenco possibili rischi a cui sono esposti i dati)	Impatto sulla sicurezza dei dati			
		impatto sui beni (2)	Probabilità della minaccia/vulnerabilità (3)	Misura del rischio (impatto x probabilità) (4)	Classifica del rischio
	Comportamenti sleali o fraudolenti (Sottrazione, cancellazione, manomissione, diffusione dei dati)	4	1	4	medio
	Errore materiale (Cancellazione,manomissione e diffusione dei dati)	4	2 per i client 1 per i servers	8 per i client 4 per i servers	alto per i client medio per i servers
Eventi relativi agli strumenti	Malfunzionamenti, indisponibilità o degrado degli strumenti dovuti a comportamenti sleali o fraudolenti (sabotaggio) (Sottrazione, cancellazione, manomissione, diffusione dei dati)	4	2 per i client 1 per i servers	8 per i client 4 per i servers	alto per i client medio per i servers
	Malfunzionamenti, indisponibilità o degrado degli strumenti dovuti a guasti dei sistemi complementari (impianto elettrico, climatizzazione,….) dovuti a degrado/usura dello strumento (Cancellazione dei dati)	2	2 per i client 1 per i servers	4 per i client 2 per i servers	medio per i client basso per i servers
	Azione di virus informatici o di programmi suscettibili di recare danno (Sottrazione, cancellazione, manomissione, diffusione dei dati)	4	1	4	basso

ANALISI DEI RISCHI					
	Descrizione rischi (1) (Elenco possibili rischi a cui sono esposti i dati)	Impatto sulla sicurezza dei dati			
		impatto sui beni (2)	Probabilità della minaccia/vulnerabilità (3)	Misura del rischio (impatto x probabilità) (4)	Classifica del rischio
	Accessi esterni non autorizzati con sottrazione di dati (Sottrazione, cancellazione, manomissione, diffusione dei dati)	4	1	4	basso
	Intercettazione di informazioni in rete (Sottrazione, diffusione dei dati)	4	4	16	altissimo
Eventi relativi al contesto	Malfunzionamenti, indisponibilità o degrado degli strumenti dovuti a eventi distruttivi naturali o artificiali (…..) (Cancellazione dei dati)	2	1	2	basso
	Accesso non autorizzato ai locali/reparti ad accesso ristretto (Sottrazione, cancellazione, diffusione dei dati)	4	2 per i client 1 per i servers	8 per i client 4 per i servers	alto per i client medio per i servers
	Sottrazione di strumenti contenenti dati (Sottrazione, cancellazione, diffusione dei dati)	4	2 per i client 1 per i servers	12 per i client 4 per i servers	alto per i client medio per i servers
	Malfunzionamenti, indisponibilità o degrado degli strumenti dovuti a guasti dei sistemi complementari (impianto elettrico, climatizzazione,….) (Cancellazione dei dati)	2	3 per i client 1 per i servers	6 per i client 2 per i servers	medio per i client basso per i servers
	Errori umani nella gestione della sicurezza fisica (Cancellazione dei dati)	2	2 per i client 1 per i servers	4 per i client 2 per i servers	medio per i client basso per i servers

5. Misure adottate per la protezione e la sicurezza dell'infrastruttura informatica di rete

Al fine di adottare misure idonee per la protezione e la sicurezza dell'infrastruttura informatica di rete, il Servizio Sistemi Informativi adotta i seguenti accorgimenti tecnologici:

- *Firewall*, ovvero un dispositivo hardware posto a protezione dei punti di interconnessione tra l'infrastruttura informatica di rete della Città Metropolitana di Genova e le reti pubbliche esterne (ad es. Internet);
- *Antivirus,* ovvero un software dotato di un motore di scansione che ricerca all'interno dei file, della *RAM (Random Access Memory)* e del flusso di rete la presenza di determinate sequenze di byte che costituiscono l'impronta digitale identificativa di un virus. Considerata la frequenza con la quale i nuovi virus vengono messi in circolazione, l'aggiornamento periodico del file delle definizioni viene fatto più volte al giorno. Inoltre l'antivirus adottato è il grado di identificare, anche se in modo probabilistico, nuove tipologie di virus.
- *Sistemi di autenticazione per l'accesso all'infrastruttura da client*: i client sono dotati di sistema di autenticazione per l'accesso all'infrastruttura di rete con parole chiave composte da almeno 8 caratteri, non contenenti riferimenti agevolmente riconducibili all'incaricato e sostituite ogni 3 mesi a cura dall' incaricato.
- *Sistemi di autenticazione per l'accesso ai servizi dell'infrastruttura da client:* utilizzo di password personali per l'accesso ai singoli servizi
- *Sistemi di autenticazione per l'accesso diretto ai servers:* i servers e gli elaboratori di classe dipartimentale sono dotati di sistema di autenticazione con parole chiave in possesso ai soli incaricati del Servizio Sistemi Informativi;
- *Accessi ristretti alle sale server* e accesso controllato ai locali del Servizio Sistemi Informativi;
- *Sistemi complementari presenti nelle 2 sale server:*

Sala server	Sistema di condizionamento	Gruppo di continuità	Sistema antincendio
Sala server ubicata presso la società Liguria Digitale	X	X	X
Uffici distaccati (SE.DI.)	X	X	NO

6. Misure adottate per la disponibilità dei dati e la continuità del servizio

Al fine di adottare misure idonee per il ripristino per la perdita di dati causata da malfunzionamenti hardware, cancellazioni e/o modifiche accidentali degli stessi, il Servizio Sistemi Informativi adotta per i servers e gli elaboratori di classe dipartimentale i seguenti accorgimenti tecnologici:

- *Repliche/mirror dei dati* mediante l'utilizzo di sistemi *RAID (Redundant array of inexpensive disks)*. La funzionalità offerta da tali dispositivi è quella di garantire la disponibilità e l'integrità dei dati anche nel caso di guasto di uno dei dischi che compongono il sistema;
- Back-up*, ovvero salvataggio dei dati memorizzati sui servers su supporti magnetici (nastri). Conservazione dei supporti magnetici in cassaforte ignifuga in locali diversi da quelli nei quali sono posizionati i servers.*

A seguito degli accorgimenti tecnologici sopra descritti, il Servizio Sistemi Informativi garantisce un ripristino dei dati entro un tempo massimo di sette giorni.

7. Distribuzione dei compiti

Al personale di ciascuna direzione il dirigente assegna, con proprio provvedimento od ordine di servizio, compiti specifici attinenti il trattamento dei dati e della documentazione (ambito di trattamento consentito) e li aggiorna annualmente. Ai dipendenti nominati incaricati del trattamento dei dati personali sono impartite le disposizioni riguardanti:

- le modalità di conservazione della documentazione;
- le modalità di memorizzazione dei documenti in formato elettronico contenenti dati personali, specificando quale unico supporto di memorizzazione i dischi di rete (M:\ e altri dischi di rete) ovvero il divieto di utilizzo del disco locale e/o di supporti removibili, compresi i personal computer portatili, per la memorizzazione dei dati in questione;
- la riservatezza dei dati e delle notizie di cui vengono a conoscenza e la non accessibilità a soggetti non autorizzati dello strumento elettronico durante la sessione di trattamento dei dati;
- modalità di predisposizione di atti/provvedimenti amministrativi, destinati alla pubblicazione all'Albo Pretorio, nell' osservanza del principio di pertinenza e non eccedenza nell'utilizzo dei dati personali (nonché il principio di indispensabilità se i dati sono sensibili o giudiziari).
- metodi di archiviazione della documentazione in maniera da tutelare e preservare la privacy degli utenti.
- le metodologie di consegna dei documenti agli utenti/cittadini al fine di preservarli dalla diffusione a terzi di notizie riservate.

Il nuovo personale assunto di ciascuna direzione viene istruito dal responsabile del

trattamento sui comportamenti da adottare all' interno degli uffici secondo quanto sopra esposto.

Il dirigente, inoltre, individua con provvedimento od ordine di servizio, il dipendente addetto alla custodia delle passwords. Con lo stesso provvedimento il dirigente responsabile del trattamento individua la procedura di disponibilità nella quale vengono indicati i casi e le modalità con cui si potrà aprire la busta contenente le password.

Il Dirigente del Servizio Sistemi Informativi, valutata l'esperienza, la capacità e l'affidabilità, è individuato quale "Amministratore di sistema" ai fini della gestione e manutenzione delle strutture informatiche dell'Ente. L'"Amministratore di Sistema" dovrà provvedere a:

- rispettare durante le attività svolte le misure di sicurezza previste dalla legge e specificate nel Documento programmatico sulla sicurezza;
- garantire la massima riservatezza nel trattamento dei dati;
- individuare per iscritto il/i soggetto/i incaricato/i della custodia delle parole chiave per l'accesso al sistema informativo e vigilare sulla sua attività;
- impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici, conforme a quanto previsto dai punti da 1 a 10 del Disciplinare tecnico, allegato B) al D. Lgs. n. 196/2003;
- impostare e gestire un sistema di autorizzazione per gli incaricati dei trattamenti di dati personali effettuati con strumenti elettronici, conforme a quanto previsto dai punti da 12 a 14 del Disciplinare tecnico, allegato B) al D. Lgs. n. 196/2003;
- verificare costantemente che l'Ente abbia adottato le misure minime di sicurezza per il trattamento dei dati personali con strumenti elettronici, previste dall'art. 34 del D. Lgs. n. 196/2003, e dal Disciplinare tecnico, allegato B) al decreto legislativo medesimo, provvedendo senza indugio agli adeguamenti eventualmente necessari;
- suggerire, per quanto riguarda l'aspetto informatico, l'adozione e l'aggiornamento delle più ampie misure di sicurezza atte a realizzare quanto previsto dall'art. 31 del D. Lgs. n. 196/2003, che dispone che i dati personali oggetto di trattamento devono essere 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;
- curare l'adozione e l'aggiornamento delle eventuali misure "idonee" di cui al punto precedente;
- attivare e aggiornare con cadenza almeno semestrale idonei strumenti elettronici atti a proteggere i dati trattati attraverso gli elaboratori del sistema informativo contro il rischio di intrusione e contro l'azione dei virus informatici;
- aggiornare periodicamente, con frequenza almeno annuale (*e* semestrale *in caso*

di trattamento di dati sensibili o giudiziari), i programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti;

- impartire a tutti gli incaricati istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale;
- adottare procedure per la custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi;
- collaborare alla predisposizione ed aggiornamento, entro il 31 marzo di ogni anno, del documento programmatico sulla sicurezza previsto dal punto 19 del Disciplinare tecnico, allegato B) al D. Lgs. n. 196/2003;
- predisporre un piano di controlli periodici, da eseguirsi con cadenza almeno annuale, dell'efficacia delle misure di sicurezza adottate in azienda;
- adottare sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici da parte dell' "Amministratore di sistema" e/o suoi incaricati, con password avente privilegi di amministratore di sistema ;
- riferire periodicamente, ed in ogni caso con cadenza annuale, al Titolare sullo svolgimento dei Suoi compiti, dandogli inoltre piena collaborazione nello svolgimento delle verifiche periodiche circa il rispetto delle disposizioni di legge e l'adeguatezza delle misure di sicurezza adottate.

8. La conservazione a norma

Con Delibera del Commissario Straordinario N.63 del 20/05/2014 la Provincia di Genova, oggi Città Metropolitana di Genova, ha approvato l'affidamento della conservazione dei documenti informatici dell'Ente, nel rispetto delle norme di legge e delle delibere del CNIPA, all'Istituto per i Beni Artistici, Culturali e Naturali (IBACN) della Regione Emilia-Romagna. In data 29/07/2015 l'Ente ha sottoscritto l'accordo di collaborazione per lo svolgimento della funzione di conservazione dei documenti informatici all'interno del quale l'IBACN, tramite il Servizio Polo Archivistico Regionale dell'Emilia-Romagna (di seguito denominato ParER), si impegna alla conservazione dei documenti trasferiti e ne assume la funzione di responsabile della conservazione ai sensi della normativa vigente, garantendo il rispetto dei requisiti previsti dalle norme in vigore nel tempo per i sistemi di conservazione. Resta a carico della Città Metropolitana la titolarità e la proprietà dei documenti depositati.

9. Altre misure di protezione dei dati personali

La tutela dai rischi esterni ed interni di distruzione, perdita accidentale o accessi abusivi avviene nel seguente modo:

- il custode delle password conserva le password in busta chiusa e controfirmata dall' incaricato che le ha consegnate.
- l' ingresso degli immobili sede degli uffici è protetto sia da porte blindate sia da porte comuni e le finestre dei piani più bassi sono dotate di grate metalliche;

- sistema di rilevazione fumi installato negli archivi, nei depositi, nei magazzini, all' interno del Servizio Sistemi Informativi, e dell' Archivio Generale;
- sistema di rilevazione gas installato all' interno del laboratorio di analisi;
- estintori installati almeno in ogni piano degli edifici dell' Ente;
- l' accesso agli uffici dell' Archivio Generale oltre l' orario di apertura avviene con la registrazione su apposito supporto cartaceo/informatico dei soggetti che vi accedono tramite la loro identificazione anagrafica e il riporto degli estremi di un documento di identità.
- Accesso controllato ai locali del Servizio Sistemi Informatici.

10. Interventi formativi

Per il personale neoassunto incaricato del trattamento dei dati sono previsti interventi formativi, da realizzarsi entro il corrente anno, riguardanti:

- i principi generali in materia di privacy;
- le novità introdotte dal dlgs. 196/2003 rispetto alla normativa previgente;
- le corrette modalità di trattamento dei dati;
- modalità di accesso ai dati personali;
- i rischi che incombono sui dati personali trattati;
- i comportamenti idonei e le misure adottare per prevenire eventi dannosi.

E' stato, inoltre, messo a disposizione sulla rete Intranet dell'Ente, e quindi consultabile da tutti i dipendenti, un "manuale" in cui vengono illustrati i principi e le regole più rilevanti in materia di trattamento di dati personali. Il "manuale" , oltre ad essere finalizzato alla formazione del personale, costituisce un costante punto di riferimento per i dipendenti per la verifica della correttezza delle modalità con cui avvengono i trattamenti di competenza.