COMUNE DI CATTOLICA
Allegato F

Piano di sicurezza

Scopo e ambito di applicazione

Il presente documento definisce le strategie e i metodi adottati dal Comune di Cattolica per la salvaguardia delle informazioni e dei dati trattati dall'Ente in materia di protocollo e gestione documentale.

Il 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. 196/2003".

Struttura logistica dell'Ente

Sedi

Il Comune di Cattolica è dislocato su 10 sedi presso le quali vengono trattati dati:

1	Sede Comunale - Residenza Municipale	Piazzale Roosevelt, 5
2	Sede distaccata ex scuole medie Filippini	Piazzale Roosevelt, 7
3	Istituzione culturale della regina	Piazza della Repubblica, 30
4	Museo della regina	Via Pascoli, 21
5	Teatro della regina	Piazza della Repubblica, n.
6	Laboratorio Attività espressive	
7	Farmacia Comunale N. 1	Via Delprete, 7
8	Farmacia Comunale San Benedetto	Via Cabral, 27
9	Scuola Materna	Via Carpignola
10	Asilo Anilo	Via Primule

Figure interessate

Si elencano di seguito le figure interessate dal trattamento dei dati ai sensi del Decreto Legislativo 196/2003.

Titolare del Trattamento dei Dati

E' la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
Nel caso di un Comune, il titolare dei trattamenti è il Sindaco quale rappresentante legale.

Responsabile della Sicurezza Informatica

E' la figura nominata dal Titolare dei trattamenti con le funzioni di coordinamento e supervisione della sicurezza informatica all'interno dell'Ente;

ha il compito di

- sovrintendere alle operazioni inerenti la sicurezza informatica;
- definire le misure di sicurezza informatica da adottare e predisporre l'informativa per l'amministratore di sistema e per i responsabili del trattamento dei dati
- collaborare con i responsabili del trattamento dei dati per definire il piano di formazione
- provvedere all'aggiornamento del DPS secondo le scadenze di legge
- predisporre le lettere di nomina dei responsabili al trattamento da sottoporre alla firma del titolare dei trattamenti dei dati
- informare il titolare del trattamento sulle mancate corrispondenze con le norme di sicurezza e su eventuali incidenti.

Responsabile del trattamento dei dati

E' la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

Il Responsabile del Trattamento dei dati riveste per definizione il ruolo di Incaricato al Trattamento.

Incaricato al trattamento

E' la persone fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile;

Interessato dal Trattamento

è la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

Amministratore di sistema

Il provvedimento del Garante per la protezione dei dati personali del 27/11/2008 ha puntualizzato la figura di amministratore di sistema e la distinzione tra Amministratore di rete e Amministratore di data Base.

Con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del provvedimento del Garante per la protezione dei dati Personali del 27/11/2008 vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

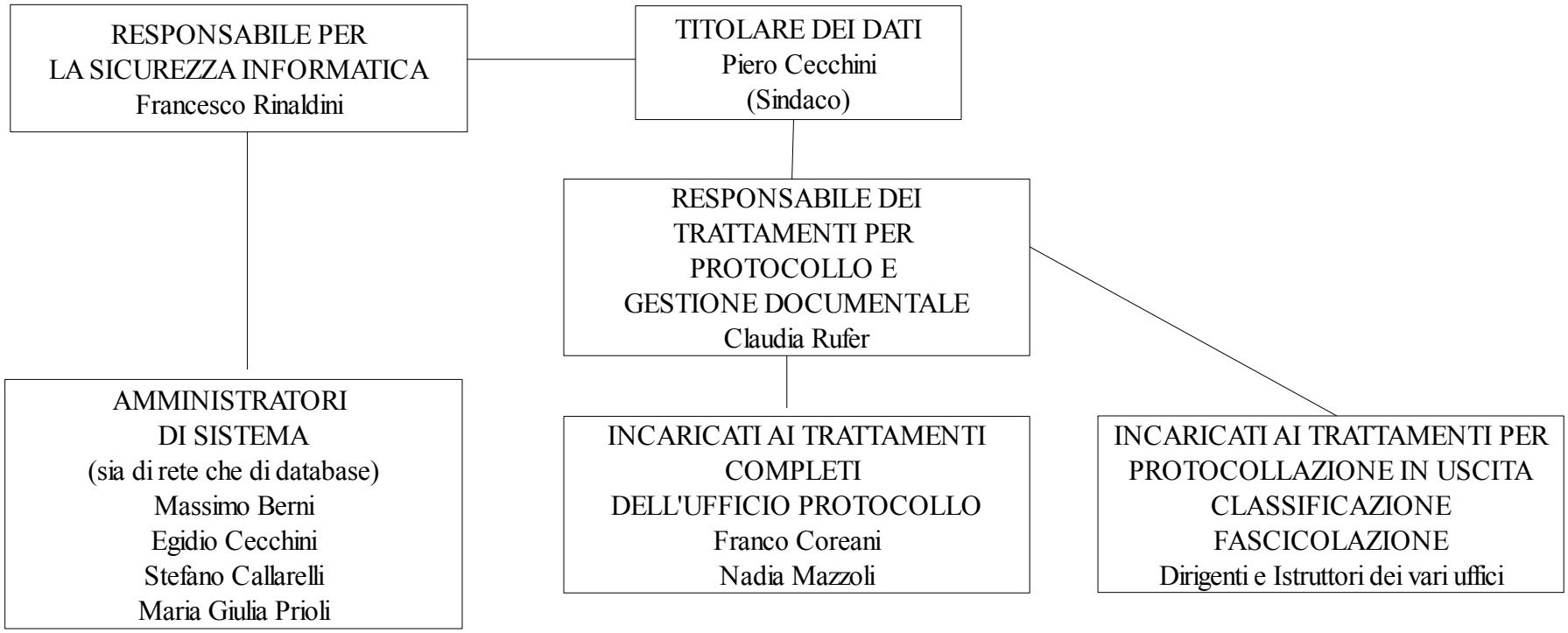
Amministratore di Rete

E' l'Amministratore di Sistema che si occupa della sicurezza dei sistemi operativi, della rete intranet e della connessione alla rete internet.

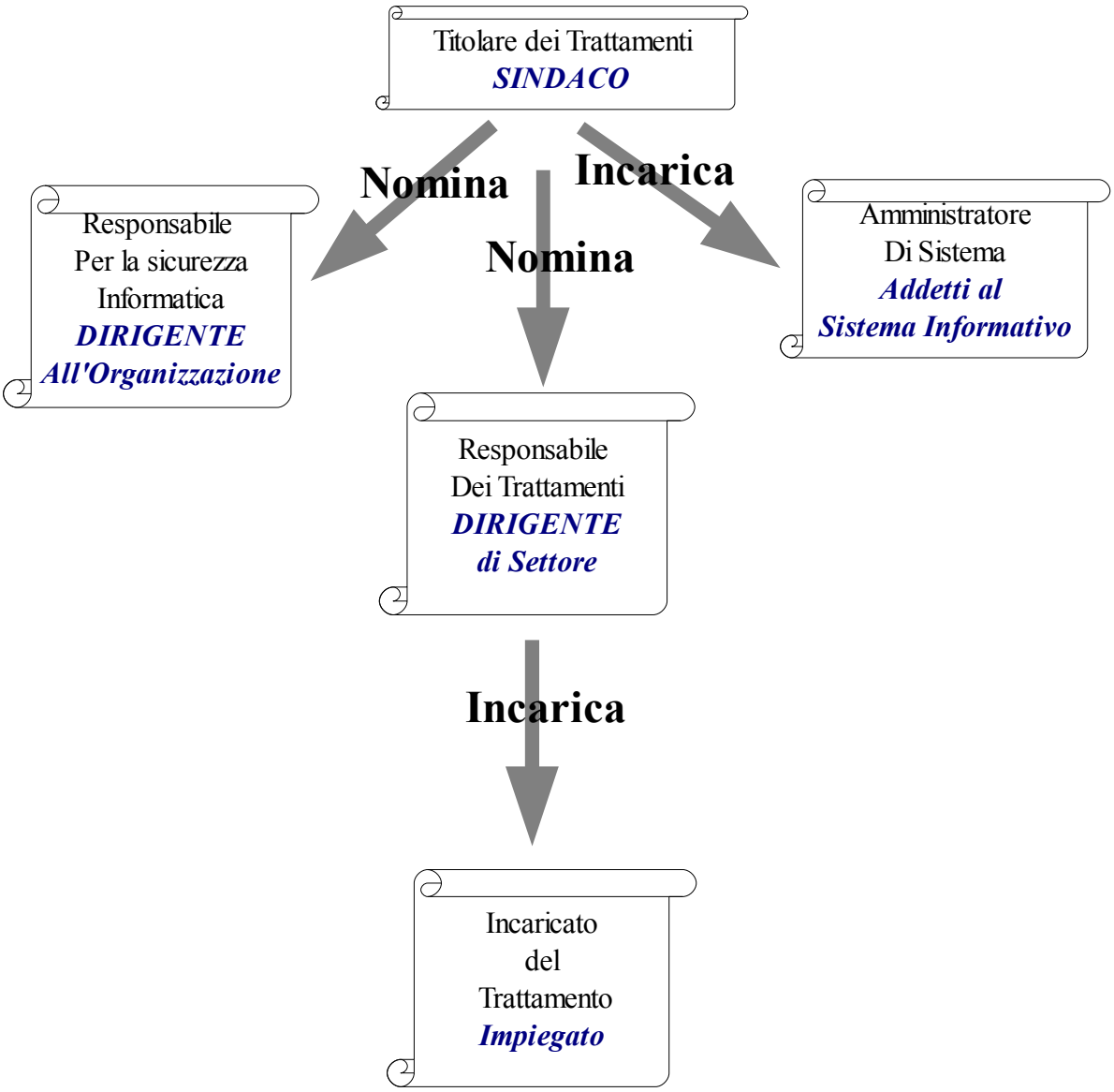
Amministratore di Database

E' l'Amministratore di Sistema che si occupa della sicurezza dei sistemi di gestione dei database (DBMS), della salvaguardia integrità dei dati in essi contenuti e dei programmi applicativi che accedono ai dati contenuti nei database stessi.

1 - Struttura organizzativa



Criterio per l'assegnazione dei ruoli di sicurezza nel Comune di Cattolica



Altre definizioni

Trattamento

Qualunque operazione o complesso di operazioni, effettuate anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modifica, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione, di dati, anche se non registrati in una banca dati.

Dati Personali

Qualunque informazione relativa a persona fisica,persona giuridica,ente od associazione, identificati o identificabili , anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

Dati identificativi

I dati personali che permettono l'identificazione diretta dell'interessato;

Dati sensibili

I dati idonei a rivelare l'origine etnica, la convinzione religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione ai partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale nonché i dati personali idonei a rilevare lo stato di salute e la vita sessuale.

Dati Giudiziari

I dati personali idonei a rilevare provvedimenti di cui all'articolo 3 comma 1, lettere da a) a o) e da r) a u) del DPR 14 novembre 2002, n 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

Minaccia

Un evento potenzialmente in grado di determinare danno a tutte o parte delle risorse.

Vulnerabilità

La misura in cui una minaccia può concretizzarsi in un sistema

Tabelle descrittive di informazioni codificate

Natura dei dati trattati

I	Dati **I**dentificativi
P	Dati **P**ersonali
S	Dati **S**ensibili
G	Dati **G**iudiziari

Strumenti utilizzati per il trattamento

Sigla	Descrizione postazione
PC	**P**ersonal **C**omputer
TC	**T**erminale **C**itrix Metaframe
TX	Terminale Linux
M	**M**anuale

Modalità di connessione della postazione di lavoro al server contenente la base di dati

NO	PC Stand alone non connesso	WAN	Rete geografica
LAN	Rete Locale (LAN)	I	Internet

Individuazione dei server utilizzato per il sistema di protocollo e gestione documentale

Identificativo di rete del Server	Descrizione	hardware	Sistema Operativo
SICRAWEBAPPSERVER	Application server del Software SICRAWEB utilizzato per il protocollo e la gestione documentale	Macchina virtuale VMWare su hardware HP	CENTOS
SICRAWEBDBSERVER	Database server basato su PostgreSQL 9.1	Macchina virtuale VMWare su hardware HP	CENTOS
SICRAWEBREP	Repository del sistema di gestione documentale	Macchina virtuale VMWare su hardware HP	WINDOWS SERVER

Strutture preposte ai trattamenti, Responsabili, Incaricati e Amministratori di Sistema

In questa sezione vengono individuate le strutture interessate al trattamento dei dati relativi a protocollo e gestione documentale, alla gestione della loro sicurezza e la figura responsabile. Per ogni struttura viene indicato il tipo di trattamento e il suo responsabile.

La tabella che segue elenca i nominativi dei responsabili, degli incaricati ai trattamenti e dei relativi amministratori di sistema.

Settore di Rif.	*Struttura di riferimento*	*Id tr.*	*Trattamento*	*Tipo di trattamento*	*Responsabile del Trattamento*	*Incaricati al trattamento*	*Amministratore di Rete*	*Amministratore di database*
4	Protocollo / Archivio	1	Protocollazione centralizzata in entrata e uscita	Aggiornamento	Rufer Claudia	Mazzoli Nadia Coreani Franco Lombardo Giovanna	Berni Massimo Callarelli Stefano Cecchini Egidio Prioli Maria Giulia	Cecchini Egidio Prioli Maria Giulia
4	Protocollo/ Archivio	4	Gestione Casella PEC Istituzioanle	Aggiornamento	Rufer Claudia	Coreani Franco Mazzoli Nadia Cecchini Egidio Berni Massimo	Provider Esterno Legalmail	Provider Esterno Legalmail
tutti	Tutte la strutture	5	Protocollazione documenti in uscita	Aggiornamento	Rufer Claudia	Tutti i dipendenti limitatamente all'Ufficio di appartenenza.	Berni Massimo Callarelli Stefano	Cecchini Egidio Prioli Maria Giulia
tutti	Tutte la strutture	6	Smistamento registrazioni di protocollo in entrata	Aggiornamento	Rufer Claudia	Smistatori di settore designati dal Dirigente	Berni Massimo Callarelli Stefano	Cecchini Egidio Prioli Maria Giulia
tutti	Tutte le strutture	7	Consultazione protocollo	Consultazione	Rufer Claudia	Tutti i dipendenti limitatamente all'Ufficio di appartenenza.	Berni Massimo Callarelli Stefano	Cecchini Egidio Prioli Maria Giulia
4	Protocollo / Archivio	8	Conservazione digitale dei documenti	Conservazione	Come previsto dall'art. 44-ter del D. LGS 82/2005 e ss.mm.ii, per una corretta conservazione dei documenti informatici, è stipulata, con delibera della Giunta Comunale n. 125 del 23/09/2015, la convenzione con il Polo Archivistico Regione Emilia-Romagna (PAR-ER), istituto che garantisce l'archiviazione dei documenti, con			

Settore di Rif.	Struttura di riferimento	Id tr.	Trattamento	Tipo di trattamento	Responsabile del Trattamento	Incaricati al trattamento	Amministratore di Rete	Amministratore di database
					durata fino al 2033. L'ente affida la conservazione dei propri documenti informatici, nel rispetto delle norme di legge e delle delibere CNIPA, all'Istituto per i Beni Artistici, Culturali e Naturali della Regione Emilia-Romagna, individuandolo come responsabile della conservazione dei documenti trasferiti in base alla convenzione stipulata.			

Analisi delle minacce e criteri di protezione

I dettagli relativi alle misure di sicurezza, proprio per la loro natura, sono riservati e non possono essere illustrati in un documento pubblico. In sintesi il criterio utilizzato per adottare le misure di sicurezza è il seguente:

- Analisi delle minacce (sono individuate 36 tipologie di minaccia)
- Valutazione del rischio, fase in cui vengono individuate le eventuali debolezze del sistema informativo.
- Azione in essere/da effettuare. Lo sviluppo dei provvedimenti di sicurezza è continuo al pari dell'evoluzione delle minacce. Gli interventi presi per fronteggiare i rischi sono a 360 gradi e riguardano, in linea di massima:
  - Qualità e sicurezza dell'ambiente di lavoro dei server
  - Sicurezza degli accessi ai server e sistemi di allarme
  - Garanzia di continuità anche in caso di black out
  - Garanzia di continuità in caso di guasti hardware (componenti ridondanti, virtualizzazioni ecc.)
  - Difesa attiva e passiva da attacchi alla sicurezza
  - Protezione da eventi naturali avversi
  - Formazione del personale addetto ai lavori e informazione su nuove minacce (e-mail, news ecc.)
  - Assistenza contunua agli utenti da parte del servizio sistemi informatici

Piano operativo di salvataggio dei dati fuori linea

Il presente paragrafo descrive in dettaglio l'intero piano di azione per la gestione della sicurezza

Salvataggi fuori linea – Pianificazione per ogni base di dati

Id. Base dati	Denominazione	Struttura incaricata	Supporto di salvataggio	Periodicità	Numero di copie minimo mantenute	Tipo di copia
SICRAWEBAPPSERVER	Application server SICRAWEB	Sistema Informativo ComunaleAmbiente Vmware	Ambiente Vmware	Giornaliera	5 copie (dal lunedì al venerdì) + archivio separato diverso per 4 settimane	Totale
SICRAWEBREP	Repository documentale di SICRAWEB	Sistema Informativo ComunaleAmbiente Vmware	Ambiente Vmware	Giornaliera	5 copie (dal lunedì al venerdì) + archivio separato diverso per 4 settimane	Totale
SICRAWEBDB	Database di SICRAWEB	Sistema Informativo ComunaleAmbiente Vmware	Ambiente Vmware	Giornaliera	5 copie (dal lunedì al venerdì) + archivio separato diverso per 4 settimane	Totale

Nel presente paragrafo vengono illustrati i criteri di protezione attivi sui supporti di massa, per i server sui quali è previsto un sistema di dischi o di alimentazione ridondante.

Protezione dei server

Server HW Id. di Rete	Ambiente con aria condizionata	Doppio processione fault tolerant	Protezione sui Dischi	Sostituzione a Caldo	Tempo masimo di fermo macchina in caso di guasto	Alimentazione ridondante	Ventilazione potenziata
SICRAWEBAPPSERVER	SI	SI	RAID 5	si	48 ore	SI	SI
SICRAWEBDB	SI	SI	RAID 5	SI	48 ore	SI	SI
SICRAWEBREP	SI	SI	RAID 5	si	48 ore	SI	SI

Protezione delle postazioni di lavoro client

Le postazioni di lavoro client sono quasi completamente in ambiente citrix, pertanto tutti i file salvati dagli utenti risiedono su di un server soggetto a copia di siscurezza. Ciò solleva l'utente stesso dal compito di provvedere alle copia di sicurezza dei propri documenti..

Fanno eccezione le poche postazioni rimaste in ambiente personal computer per le quali ogni utente deve provvedere in prima persona ad effettuare le copie di sicurezza in un'area centralizzata sottoposta a backup oppure chiedere un piano specifico di protezione al rispettivo Responsabile dei Trattamenti.

Regole generali di comportamento in caso di incidente di sicurezza

Le regole che seguono devono essere seguite in tutti i casi in cui si accerti o si sospetti un incidente di sicurezza.

<table>
<tr><th>Attività</th><th>Incidente di sicurezza</th><th>Comportamento</th></tr>
<tr><td rowspan="5">Collegamento alla postazione di lavoro o ad uno specifico programma applicativo</td><td>Immettendo user id e password non viene effettuato il login e non viene visualizzato uno dei seguenti messaggi:
Userid password errati
Userid disattivato
Password scaduta</td><td rowspan="8">Avvertire immediatamente un Amministratore di Sistema

in assenza di esso, annotarsi le caratteristiche dell'incidente e tentare di spegnere la postazione di lavoro annotandosi tutte le operazioni effettuate. Appena possibile riferire il tutto ad un Amministratore di Sistema.</td></tr>
<tr><td>Immettendo ripetutamente userid e password corretti viene rifiutato il login</td></tr>
<tr><td>Il login viene effettuato anche senza immettere userid e/o password</td></tr>
<tr><td>Il sistema è eccessivamente lento rispetto alla norma
Il sistema presenta rallentamenti improvvisi e temporanei</td></tr>
<tr><td rowspan="2">Svolgimento del normale lavoro al terminale</td></tr>
<tr><td>Il sistema è eccessivamente lento rispetto alla norma
Il sistema presenta rallentamenti improvvisi e temporanei</td></tr>
<tr><td>Scollegamento dal programma applicativo</td><td>E' impossibile chiudere il programma applicativo</td></tr>
<tr><td>Scollegamento dalla postazione di lavoro</td><td>E' impossibile scollegarsi o spegnere il sistema</td></tr>
<tr><td>Svolgimento del normale lavoro al terminale</td><td>Si verifica un incidente fisico che possa arrecare danni alle persone e alle cose (es principio di incendio, ecc.)</td><td>rispettare le seguenti priorità:
1. evitare danni diretti alle persone;
2. proteggere l'informazione sensibile o proprietaria;</td></tr>
</table>

		3. evitare danni economici; 4. limitare i danni all'immagine dell'organizzazione. Garantita l'incolumità fisica alle persone procedere a: 1. isolare l'area contenente il sistema oggetto dell'incidente; 2. isolare il sistema compromesso dalla rete distaccando il cavo di collegamento; 3. spegnere nel modo più corretto possibile il sistema oggetto dell'incidente Una volta spento il sistema oggetto dell'incidente non deve più essere riacceso; 4. documentare tutte le operazioni.

Piano operativo di ripristino dei dati

Il ripristino dei dati è necessario nei seguenti casi:

- rottura di più dischi contemporaneamente sui server provvisti di protezione RAID o Mirroring,
- rottura di un disco sui server sprovvisti di protezione.
- Guasto permanente sui dischi contenenti il sistema operativo

Per i tempi di fermo macchina massimi sui server dotati di protezione, fare riferimento alla tabella seguente.

Criteri di ripristino dei dati

Server HW (Id. di Rete) **Dispositivo di rete**	**Guasto permanente del Sistema Operativo o Rottura di dischi (multipla sui sistemi protetti)**		
	Intervento ***Struttura incaricata***	**Operatore esterno**	**Tempo max.**
SICRAWEBAPPSERVER	Ripristino della macchina virtuale *Incaricato: Sistema Informatico Comunale*	Maggioli – HP se attiva l'assistenza	96 ore
SICRAWEBDBSERVER	Ripristino della macchina virtuale *Incaricato: Sistema Informatico Comunale*	Maggioli – HP se attiva l'assistenza	96 ore
SICRAWEBREP	Ripristino della macchina virtuale *Incaricato: Sistema Informatico Comunale*	Maggioli – HP se attiva l'assistenza	96 ore

Regole per l'accesso ai sistemi

Regole generali

N.	Regola
1	Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina.
2	Il posto di lavoro costituito da personal computer viene consegnato completo di quanto necessario per svolgere le proprie funzioni, pertanto è vietato modificarne la configurazione.
3	Il software installato sui personal computer è quello richiesto dalle specifiche attività lavorative dell'operatore. E' pertanto proibito installare qualsiasi programma da parte dell'utente o di altri operatori, escluso l'amministratore del sistema.
4	L'utente ha l'obbligo di accertarsi che gli applicativi utilizzati sulla sua postazione di lavoro siano muniti di regolare licenza.
5	Ogni utente è responsabile dei dati memorizzati nel proprio personal computer. Per questo motivo è tenuto ad effettuare la copia di questi dati.
6	E' vietato ogni tipo di abuso. In particolare è vietato: - usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da quanto previsto dal presente documento; - utilizzare la rete per scopi incompatibili con l'attività istituzionale; - utilizzare un profilo utente a cui non si è autorizzati; - cedere a terzi codici personali (USER ID e PASSWORD) di accesso al sistema; - conservare la password in modo scritto in luoghi visibili o comunque non protetti sotto chiave - conseguire l'accesso non autorizzato a risorse di rete interne o esterne; - violare la riservatezza di altri utenti o di terzi; - agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti; - agire deliberatamente con attività che distraggano risorse (persone, capacità, elaboratori); - effettuare o permettere ad altri, trasferimenti non autorizzati di informazioni (software, basi dati, ecc.); - installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (p.e. virus, cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing - p2p); - installare o eseguire deliberatamente programmi software non autorizzati e non compatibili con le attività istituzionali; - cancellare, disinstallare, copiare, o asportare deliberatamente programmi software per scopi personali; - installare deliberatamente componenti hardware non compatibili con le attività istituzionali; - rimuovere, danneggiare deliberatamente o asportare componenti hardware. - utilizzare le risorse hardware e software e i servizi disponibili per scopi personali; - utilizzare la posta elettronica con le credenziali di accesso di altri utenti;

N.	Regola
	- utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi. - utilizzare l'accesso ad Internet per scopi personali; - accedere direttamente ad Internet con modem collegato al proprio Personal Computer; - connettersi ad altre reti senza autorizzazione; - monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere copiare o cancellare file e software di altri utenti, senza averne l'autorizzazione esplicita; - usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete; - inserire o cambiare la password del bios; - abbandonare il posto di lavoro lasciandolo incustodito o accessibile.
7	L'Incaricato al Trattamento è obbligato a modificare immediatamente la sua parola d'ordine, nel momento in cui sospetti che qualcuno ne sia venuto a conoscenza.
8	Nel caso in cui l'Incaricato al Trattamento dimentichi la propria password deve contattare l'Amministratore di Sistema che provvederà a riattivare il profilo con una nuova password (che dovrà essere modificata dal Dipendente al primo accesso). Non si deve tentare ripetutamente di inserire una password errata.

Regole per l'accesso alla rete e al sistema operativo

N.	Regola
1	Ogni postazione di lavoro è collegata alla rete in modo univoco: ogni porta della rete è abilitata al collegamento di una e una sola postazione ben identificata attraverso l'identificativo della propria scheda di rete (mac address).
2	L'accesso alla postazione di lavoro è certificato in modo centrale dal server e le configurazioni delle stazioni di lavoro (desktop, privilegi, menu) sono assegnati in modo dinamico al momento del collegamento
3	Ogni utente possiede le credenziali per collegarsi alla postazione di cui è titolare, salvo i casi in cui il titolare di un'altra postazione conceda in forma scritta l'accesso alla propria unità.
4	L'accesso è certificato tramite identificativo utente e password assegnati inizialmente dal Responsabile di Rete con obbligo di modifica della password al primo accesso. Nessun amministratore (di rete o di sistema informativo) conosce la password di un utente.
5	La password ha una validità massima di 3 mesi. L'utente viene preavvertito dell'imminente scadenza, ad ogni connessione al sistema, a partire da 15 giorni dalla data di scadenza stessa
6	La password di sistema ha una lunghezza minima di 12 caratteri composta da lettere, numerie,cartteri speciali e non deve essere uguale a nessuna delle 24 precedentemente utilizzate
7	Per gli Amministratori (Consiglieri e Assessori) e per il Sindaco le credenziali di accesso alla rete vengono assegnate d'ufficio al momento dell'entrata in carica e revocate d'ufficio al momento del termine di mandato.
8	Per i dipendenti non di ruolo le credenziali scadono automaticamente al termine del periodo di assunzione indicato nella lettera di incarico.
9	Su ogni postazione sono disabilitate tutte le periferiche rimovibili (floppy, lettori CD) e tutte le porte USB

N.	Regola
10	L'accesso al registro di configurazione di ogni postazione è consentito esclusivamente all'amministratore di rete
11	Le autorizzazioni particolari relative alla posta elettronica e per l'accesso ai siti internet non compresi nella lista di siti istituzionali aperti a tutti i dipendenti, devono essere richieste, dal responsabile dei trattamenti, all'Amministratore di Rete specificando le finalità della richiesta.
12	Al fine di evitare l'accesso da parte di estranei, trascorso un intervallo di 60 minuti di inattività, la postazione di lavoro si pone automaticamente in stato di stand by. Per accedere nuovamente alla postazione l'utente collegato deve reinserire la password.
13	Se a seguito di assenza prolungata dal lavoro di un Incaricato al Trattamento, si rende necessario accedere alla sua postazione, il Responsabile del Trattamento dei dati autorizzerà, attraverso lettera di incarico, un nuovo Incaricato o direttamente un Amministratore di Sistema.
14	L'Amministratore di Sistema non è autorizzato a svolgere funzioni applicative di terzi col proprio profilo di amministratore. Può solamente a installare e configurare la postazione stessa e il suo software.

Regole per l'accesso ai programmi applicativi e ai dati del Sistema Informativo

N.	Regola
1	L'accesso al sistema informativo è certificato attraverso identificativo utente e password. La lunghezza minima della password è di 7 caratteri e il controllo dell'accesso varia a seconda del programma applicativo utilizzato, comunque è sempre conforme alle misure minime previste dalla normativa vigente.
2	L'accesso ai dati dei vari database aziendali avviene solamente attraverso i programmi applicativi. Sono disabilitati dalle postazioni client tutti gli altri metodi d'accesso quali interfacce SQL strumenti di amministrazione di database e client interattivi specifici.
3	E' assente dalle postazioni client ogni driver ODBC in grado di accedere ai database del sistema informativo.
4	Qualunque informazione presente sul sistema informativo, non ottenibile con i programmi applicativi, deve essere richiesta su modulo firmato, al responsabile del trattamento. I relativi funzionari responsabili provvederanno ad ottenere la varie autorizzazioni dai dirigenti titolari dei dati e fornire entro 36 ore lavorative la risposta.
9	Qualunque informazione presente sul sistema informativo (eccetto i casi di certificazione o di trasmissione di atti regolamentati dalla legge) può essere trasmessa all'esterno dell'Ente solo dietro autorizzazione scritta del responsabile dei trattamenti competente per il trattamento dei dati.
10	Se a seguito di assenza di un Incaricato al Trattamento, si rende necessario accedere ad una funzione applicativa di sua competenza esclusiva, il Responsabile del Trattamento dei dati interessato deve autorizzare l'amministratore di database ad inserire la sostituzione sul programma applicativo.