PIANO DI SICUREZZA INFORMATICA

UNIONE RENO GALLIERA

ADOTTATO CON DETERMINA CED N. 55 DEL 30.09.2015

UNIONE
RENO GALLIERA

ARGELATO | BENTIVOGLIO | CASTELLO D'ARGILE | CASTEL MAGGIORE | GALLIERA | PIEVE DI CENTO | SAN GIORGIO DI PIANO | SAN PIETRO IN CASALE

SEDE CENTRALE
Via Fariselli 4
40016 San Giorgio di Piano
tel.: 051 8904711
fax: 051 8904790
partita IVA e CF 02855851206
unione.renogalliera@cert.provincia.bo.it

SERVIZI ALLA PERSONA
Via Pescerelli 47
40018 San Pietro in Casale
tel.: 051 8904711
fax: 051 4689602
serviziallapersona@pec.renogalliera.it

SISTEMI INFORMATIVI
Via Argelati 4
40050 Argelato
tel.: 051 8904777
fax: 051 7417283
informatica@renogalliera.it

POLIZIA MUNICIPALE
Via Fariselli 4
40016 San Giorgio di Piano
tel.: 051 8904750
fax: 051 8904794
numero verde 800 800 606
pm@renogalliera.it

Sommario

Premessa: la gestione della sicurezza informatica 4
Identificazione del servizio da erogare 7
Descrizione infrastrutture tecnologica 8
Descrizione dei sistemi informativi 11
Analisi dei rischi (regola 19.3 dell'Allegato B al Codice) 12
Azioni intraprese 16
Modalità di accesso ai sistemi e ai dati 16
Misure fisiche, tecnologiche 17
Privacy e gestione dei trattamenti 19
Descrizione analitica degli strumenti utilizzati 19
Le operazioni di salvataggio dei dati: regola 19.5 dell'Allegato B al Codice 19
I controlli anti-intrusione dall'esterno 20
Azioni intraprese per il fault tolerance: regola 19.5 dell'Allegato B al Codice 21
Procedure da seguire in caso di fault 25
Azioni da intraprendere per il disaster recovery 26
Azione preventive da eseguire nella sede principale 27
Procedure da seguire in caso di disaster 27
Conclusioni 28
Riferimenti 29

SEDE CENTRALE
Via Fariselli 4
40016 San Giorgio di Piano
tel.: 051 8904711
fax: 051 8904790
partita IVA e CF 02855851206
unione.renogalliera@cert.provincia.bo.it

SERVIZI ALLA PERSONA
Via Pescerelli 47
40018 San Pietro in Casale
tel.: 051 8904711
fax: 051 4689602
serviziallapersona@pec.renogalliera.it

SISTEMI INFORMATIVI
Via Argelati 4
40050 Argelato
tel.: 051 8904777
fax: 051 7417283
informatica@renogalliera.it

POLIZIA MUNICIPALE
Via Fariselli 4
40016 San Giorgio di Piano
tel.: 051 8904750
fax: 051 8904794
numero verde 800 800 606
pm@renogalliera.it

Premessa: la gestione della sicurezza informatica

Con l'entrata in vigore del "*Codice in materia di protezione dei dati personali*" il legislatore ha sancito che il diritto alla riservatezza, all'identità personale e alla protezione dei dati riferiti a persone fisiche o giuridiche sono da annoverarsi tra i diritti fondamentali. Di conseguenza qualsiasi *trattamento* di dati personali deve svolgersi nel rispetto della dignità del soggetto interessato sottoposto al trattamento.

Da quanto esposto sopra deriva la necessità di rafforzare, in un quadro di evoluzione tecnologica, le misure di sicurezza contro i rischi di distruzione o perdita, anche accidentale, dei dati personali, di accesso non autorizzato o di uso improprio dei dati stessi.

A tal fine alle precauzioni già previste se ne aggiungono altre come: password di non meno di otto caratteri, autenticazione informatica, sistemi di cifratura, procedure per il ripristino dei dati, ecc., nonché la tenuta di un aggiornato documento programmatico sulla sicurezza. Per quanto oggi la normativa non prevede l'approvazione annuale di questo documento è buona prassi verificare e mantenere aggiornate le misure che si adottano.

Nonostante sia utopistico credere che possa esistere la sicurezza assoluta, questo non esime qualsiasi titolare, responsabile o incaricato del trattamento dei dati personali a predisporre un piano di sicurezza dell'ente. Occorre però individuare, in via preliminare, quali sono i requisiti minimi di sicurezza di un sistema informativo basato su strumenti elettronici o su strumenti cartacei per poterli applicare al sistema stesso nella totalità o in parte.
L'obiettivo è quindi quello di stabilire il livello di sicurezza da raggiungere in relazione al valore del bene intangibile da proteggere (informazione) ed al rischio sostenibile, senza ridurre la possibilità di fruizione dello stesso.

Un sistema informativo deve, quindi, avere un sistema di protezione contro i seguenti rischi:

- accesso indebito alle risorse;
- azioni dolose;
- errori operativi;
- manomissioni o furti;

- fault di servizi;
- eventi dannosi o disastrosi

offrendo al contempo garanzia di:

- autenticità e integrità delle registrazioni elettroniche

ed assicurando:

- facilità di auditing

Per **accesso indebito alle risorse** s'intende che dati, programmi e strumenti di comunicazione devono essere protetti da accessi non autorizzati, in ottemperanza al d.lgs. n. 196/2003.

Per **protezione da azioni dolose** s'intende che devono esistere procedure e strumenti per proteggere le risorse del S.I. da azioni particolari come modifica o copia di informazioni, messaggi, file, programmi da parte di persone non autorizzate, uso non autorizzato dei privilegi di sistema, dirottamento o duplicazione di informazioni o programmi da parte di persone non autorizzate, bombe logiche, cavalli di Troia, virus.

Per **protezione dagli errori operativi** s'intende che il S.I. deve essere progettato in modo che errori operativi non arrechino danni alle risorse hardware e software, che le operazioni critiche siano attivabili solo da personale autorizzato e che devono essere previsti strumenti per ripristinare lo stato corretto del sistema nel caso vengano rilevati errori operativi.

Per **protezione da manomissioni o furti** s'intende che i server dell'ente, nonché i documenti cartacei, devono essere custoditi in locali protetti in cui l'accesso è permesso solo agli incaricati per lo svolgimento di compiti ad essi assegnati.

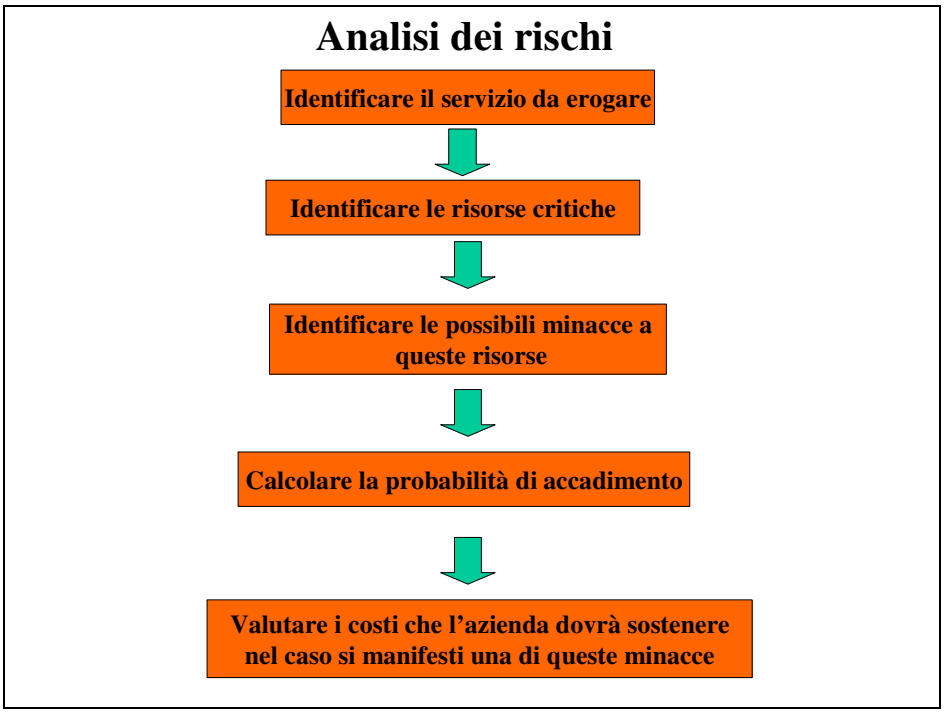
Per **protezione contro il fault o la caduta di alcuni servizi**, s'intende che è opportuno che esista una procedura in grado di far ripartire un servizio più o meno critico, più o meno importante, servizio caduto in seguito ad un guasto hardware e/o software, con i tempi ed i modi definiti dal "manuale della sicurezza".

Infine per **protezione contro eventi dannosi o disastrosi** s'intende che è necessario che il sistema informativo preveda contromisure per tutelarlo da eventi dannosi (assenza di alimentazione elettrica o condizionamento) o disastrosi (incendi ecc.).

La **garanzia** che deve essere offerta dal sistema informativo è relativa all'**autenticità dei dati**, ovvero deve essere disponibile un meccanismo per associare ad una unità di registrazione l'identificativo dell'utente che l'ha generata nella forma in cui essa è memorizzata, con una prova incontestabile, e all'**integrità del dato stesso**. Per integrità dei dati gestiti e registrati a livello applicativo; si afferma che il compito del S.I. è quello di garantire l'integrità logica (*coerenza e consistenza*) e fisica (*esistenza di copie o di salvataggi*) di tali dati.

Per quanto riguarda i **requisiti di auditing** essi riguardano quelle caratteristiche del sistema informativo che possono facilitare le attività ispettive necessarie per assicurare il mantenimento del livello di sicurezza.
Il presente documento viene redatto tenendo conto dell'architettura centralizzata del servizio informatico associato dell'Unione Reno Galliera a cui l'Amministrazione ha conferito con apposita convenzione la gestione delle funzioni informatiche.
Il primo passo da fare per decidere la politica da seguire nel garantire la sicurezza di un sistema è l'analisi del rischio. L'obiettivo di tale analisi è quello di identificare le minacce alle risorse critiche del sistema per valutare le perdite derivanti dal verificarsi di tali minacce e potere eventualmente giustificare i costi da sostenere per la gestione della sicurezza.

Il processo è quindi il seguente:



L'analisi dei rischi, oggetto del presente lavoro, non tratta in dettaglio le probabilità di accadimento dei rischi stessi, né i costi, legati al mancato uso dei sistemi, in quanto si da per scontato che tali eventi si verifichino e che i costi ad essi associati siano ingenti.

Identificazione del servizio da erogare

I Comuni della Reno Galliera hanno conferito all'Unione la gestione associata dei sistemi informatici e telematici in piena armonia con la normativa nazionale e regionale in materia di gestioni associate.

Tale conferimento prevede lo svolgimento delle seguenti attività:

- la progettazione gestione centralizzata dell'infrastruttura tecnologica
- la progettazione e gestione della rete dati
- l'assistenza informatica
- l'installazione e configurazione delle postazioni di lavoro
- la gestione unitaria dei contratti informatici
- l'omogeneizzazione dei software di back office
- l'erogazione di servizi on line
- la sottoscrizione di accordi con altri enti in ambito ICT

- la gestione del sistema informativo territoriale
- il supporto alle Amministrazioni sulle problematiche relative al digital divide
- l'attivazione e la gestione degli hot spot wi fi sul territorio

Descrizione infrastrutture tecnologica

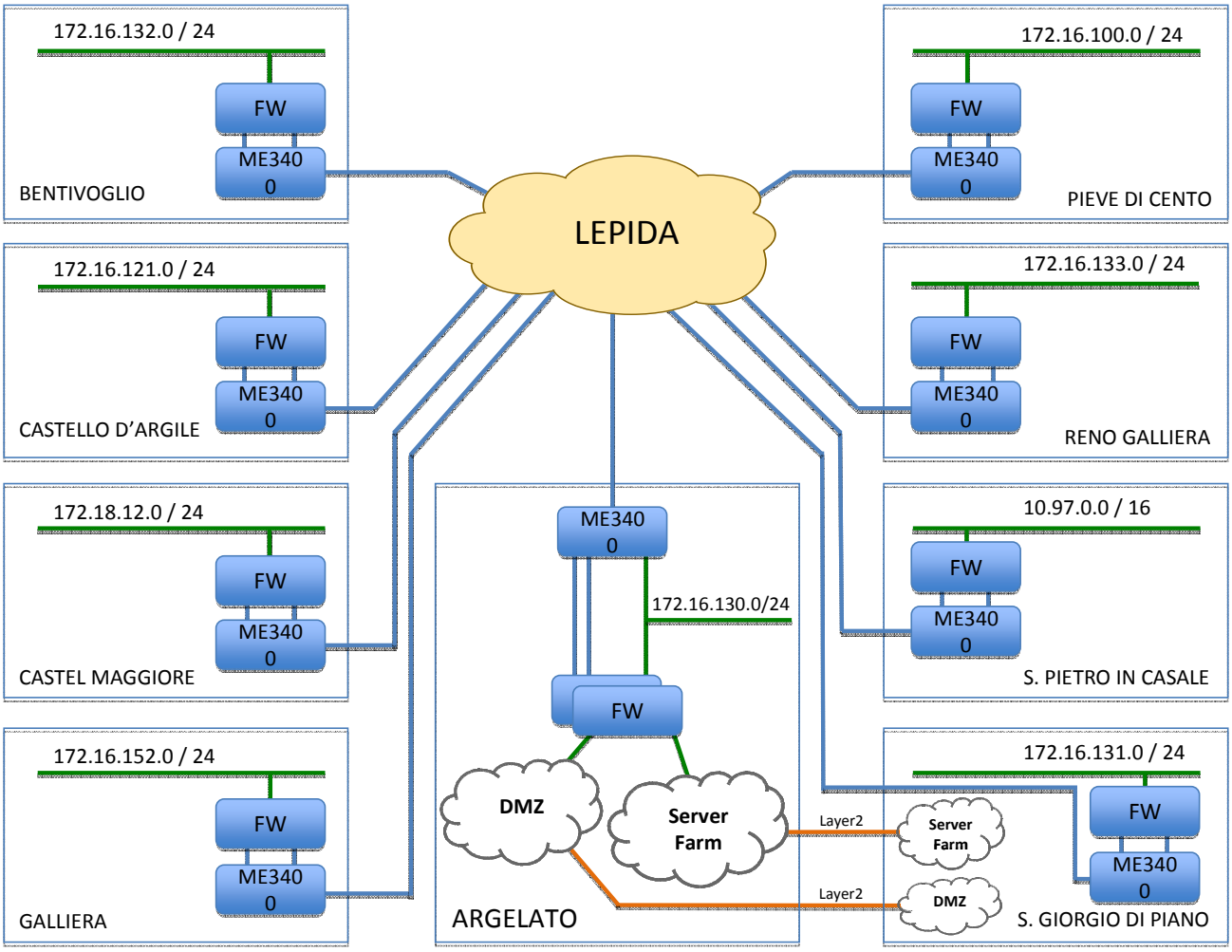
Il Data Center dell'Unione Reno Galliera è sito presso la sede municipale del Comune di Argelato con una sede di Disaster Recovery presso la sede dell'Unione Reno Galliera a San Giorgio di Piano.

Tutti i comuni sono collegati alla rete in banda larga regionale Lepida che dispone di un servizio di assistenza help desk attivo 24 ore per 365 giorni all'anno.

Il data center è basato su un'architettura totalmente virtualizzata tramite la tecnologia XEN.

Le applicazioni non sono installate sulle postazioni di lavoro, ma distribuite tramite le tecnologie a terminale grafico Citrix.

Il sistema utilizza 12 server fisici (divisi tra la sede centrale e quella di disaster recovery) e circa 60 server virtuali.



Elenco dei server fisici

Nome	O.S.	Posizione dell'elemento	Modello	Numero di serie (S	Commenti
gvmw-rgdomain2	Windows 2012 R2 Standard (64 bit)	RG > Sede Servizio Informatico (Sala	Fujitsu Primergy RX300 S4	YKAF024406	Domain Controller 2
gvmw-rgdomain3	Windows 2012 R2 Standard (64 bit)	RG > Sede Unione (A) (Sala Server DI	Fujitsu Primergy RX300 S4	YKAF026034	Domain Controller 3
RGSRV013	Windows 2003 Standard (32 bit)	RG > Sede Servizio Informatico (Sala	Fujitsu Primergy RX300 S4	YKAF026448	Appoggio
rgsrvbk1	Windows 2012 Standard Storage (64 bit)	RG > Sede Unione (A) (Sala Server DI	Fujitsu Primergy RX300 S7	YLAR006076	Backup
RGVID041	Windows 2012 R2 Standard (64 bit)	RG > Sede Unione (A) (Sala Server DI	Fujitsu Primergy RX300 S8	YLNT013487	Master Server Videosorveglianza PM
RGVID043	Windows 2012 R2 Standard (64 bit)	RG > Sede Unione (A) (Sala Server DI	Fujitsu Primergy RX300 S8	YLNT013489	Server Videosorveglianza PM
RGVID045	Windows 2012 R2 Standard (64 bit)	RG > Sede Unione (A) (Sala Server DI	Fujitsu Primergy RX300 S8	YLNT013488	Server Videosorveglianza PM
XEN030	Linux "XenServer" (64 bit)	RG > Sede Unione (A) (Sala Server DI	Fujitsu Primergy RX300 S6	YL6T028585	Pool Master XenServer Sede DR
XEN031	Linux "XenServer" (64 bit)	RG > Sede Unione (A) (Sala Server DI	Fujitsu Primergy RX300 S6	YL6T028588	Pool XenServer Sede DR
XEN032	Linux "XenServer" (64 bit)	RG > Sede Unione (A) (Sala Server DI	Fujitsu Primergy RX300 S6	YL6T028587	Pool XenServer Sede DR
XEN033	Linux "XenServer" (64 bit)	RG > Sede Unione (A) (Sala Server DI	Fujitsu Primergy RX300 S6	YL6T028571	Pool XenServer Sede DR
XEN130	Linux "XenServer" (64 bit)	RG > Sede Servizio Informatico (Sala	Fujitsu Primergy RX200 S8	YLNS006990	Pool Master XenServer Sede Principale
XEN131	Linux "XenServer" (64 bit)	RG > Sede Servizio Informatico (Sala	Fujitsu Primergy RX200 S8	YLNS006988	Pool XenServer Sede Principale
XEN132	Linux "XenServer" (64 bit)	RG > Sede Servizio Informatico (Sala	Fujitsu Primergy RX200 S8	YLNS006989	Pool XenServer Sede Principale
XEN133	Linux "XenServer" (64 bit)	RG > Sede Servizio Informatico (Sala	Fujitsu Primergy RX200 S8	YLNS006991	Pool XenServer Sede Principale

UNIONE RENO GALLIERA

Elenco server virtuali

Nome	Commenti	O.S.
acisincrocat	Sincrocat per ACI	Linux CentOS (64 bit)
acivesta	ACI / Vesta	Linux CentOS (64 bit)
ADSDBAR	DB Oracle ADS AR	Linux Red Hat (64 bit)
ADSDBBE	DB Oracle ADS BE	Linux Red Hat (64 bit)
ADSDBPC	DB Oracle ADS PC	Linux Red Hat (64 bit)
ADSDBSG	DB Oracle ADS SG	Linux Red Hat (64 bit)
ADSDBSP	DB Oracle ADS SP	Linux Red Hat (64 bit)
Akropolis	Oralce Server per Demografici Galliera (licenza Oracle	Windows 2012 R2 Standard (64 bit)
asset	Asset - GLPI gestione ticket e inventario	Windows 2003 R2 (32 bit)
citrixlic	License Server vecchia farm	Linux CentOS (64 bit)
CTX03	Vecchia farm citrix - no provisioning	Windows 2003 R2 (32 bit)
DMZ-AccertaPdaAnacne	8 apache tomcat per gli Anacner degli 8 comuni (e relat	Linux CentOS (64 bit)
DMZ-FTP	FTP	Windows 8 (64 bit)
DMZ-NetScaler	NetScaler per accesso web (interno ed esterno) nuova	FreeBSD (64 bit)
DMZ-revproxy	SSL	Linux CentOS (64 bit)
DMZ-ws2003sms	Servizio Web per SMS CA e SG	Windows 2003 R2 (32 bit)
docway	storage docway non interfacciato con doc-er	Linux CentOS 6 (64 bit)
docwaytest	storage doc-er; NB: produzione - interfacciato con doc-e	Linux CentOS 6 (64 bit)
flower	front end doc-er (consente accesso doc-er)	Linux CentOS 6 (64 bit)
gvmw-ctxweb	Vecchia farm citrix - Macchina web	Windows 2003
GVMW-RGDOMAIN	Domain Controller	Windows 2012 R2 Standard (64 bit)
gvmwapp	Tomcat ADS (Anagrafe AR, BE, PC, SG, SP)	Windows 2003 R2 (32 bit)
hobbit	Hobbit - Monitoraggio server - indirizzo internet monitor.	Linux Debian 5 (64 bit)
MSSQL079	Microsoft SQL express 2012 per Affrancatrice AR, Opta	Windows 2012 R2 Standard (64 bit)
OgO5	Server Posta Elettronica (Mail)	Linux CentOS (64 bit)
oraclesoftech	Database server GarsiaWe, Sosia ASP, Sosia CM e SF	Linux CentOS 5 (64 bit)
Plone	Sito Web Plone di SP - Plone 3	Linux CentOS (64 bit)
plone-ca	Plone Castello d'Argile - Sito non ancora in esercizio- Pl	Linux CentOS 6 (64 bit)
plone-pc	Plone Pieve di Cento - sito web comune Pieve - Plone 4	Linux CentOS 6 (64 bit)
plone-rg	Plone Reno Galliera - Sito Web Istituzionale - plone 4	Linux CentOS 6 (64 bit)
PROV2012	Provisioning nuova farm Citrix e relativo DB Microsoft S	Windows 2012 R2 Standard (64 bit)
PROV2012B	Provisioning nuova farm Citrix (senza DB)	Windows 2012 R2 Standard (64 bit)
proxy	Proxy squid danguardian	Linux CentOS (64 bit)
Pubblicita	DB Informix IMB (Per Kibernetes)	Linux CentOS (64 bit)
RGCED054	Macchina per aggiornamenti	Windows XP (32 bit)
RGCED088	Gestore Fotocopiatrici SG e PC	Windows XP (32 bit)
RGCED089	Gestore Infomonitor RG e PM	Windows XP (32 bit)
RGCED090	Gestore visualizzazione tabulati telefonici per PM (Polizi	Windows XP (32 bit)
RGCTX001	Nuova farm citrix	Windows 2012 R2 Standard (64 bit)
RGCTX002	Nuova farm citrix	Windows 2012 R2 Standard (64 bit)
RGCTX003	Nuova farm citrix	Windows 2012 R2 Standard (64 bit)
RGCTX004	Nuova farmi citrix	Windows 2012 R2 Standard (64 bit)
RGCTX005	Nuova farm citrix	Windows 2012 R2 Standard (64 bit)
RGCTX006	Nuova farm citrix	Windows 2012 R2 Standard (64 bit)
RGCTXXXX	Nuova farm citrix (template provisioning)	Windows 2012 R2 Standard (64 bit)
RGDDC107	Citrix Studio (Gestione nuova server farm citrix) e relativ	Windows 2012 R2 Standard (64 bit)
rgsophos	server antivirus sophos con SQL	Windows 2012 R2 Standard (64 bit)
RGSRV012	DB Firebird per CBA (ASP)	Windows 2003 R2 (32 bit)
RGSRV082	MS-SQL SuapNet, Mercati, Rilevanet (Ambito)	Windows 2003 R2 (32 bit)
RGSRV083	MS-SQL per ATWS (Ambito), Optac (PM), Verbatel	Windows 2003 R2 (32 bit)
RGSRV084	MySql Federa Google (Iscrizioni SG)	Windows 2003 R2 (32 bit)
RGSRV085	MS-SQL ACI, Nettime, SIT, ND24, Federa per SIT	Windows 2008 R2 Standard (64 bit)
RGSRV121	MS-SQL Vistared (PM) Microrex Volpolini	Windows 7 (64 bit)
RGSRVDOC	Autostore: Documentale con OCR per fotocopiatrici PC	Windows 2012 R2 Standard (64 bit)
serpico	Vecchia anagrafe Datamanagement	Windows 2003 R2 (32 bit)
serverweb	IIS per:	Windows 2003 R2 (32 bit)
SoftechApp	Application server Garsia WE	Linux CentOS 6 (64 bit)
SQLdatagraph	Database Server MS-SQL 2008 R2 per applicazioni Dat	Windows 2008 R2 Standard (64 bit)
Tributi	Database PostgreSQL 8.3.7 Kibernetes	Linux CentOS 6 (64 bit)
webposta	Accesso secondario alla posta Zimbra	Linux CentOS (64 bit)
webserver	IIS	Windows 2012 R2 Standard (64 bit)

Descrizione dei sistemi informativi

La notevole complessità amministrativa dei comuni ha come conseguenza un'elevata articolazione dei sistemi informativi comunali.

A partire dal 2011 è stato attivato un processo di omogeneizzazione dei software comunali, ancora in corso. Di seguito vengono riportati i sistemi informativi comunali e la loro modalità di gestione e dispiegamento.

Sistema Informativo	**Fornitore**	**Modalità di dispiegamento**
Protocollo	Datagraph	Client server tramite Citrix
Contabilità	Datagraph	Client server tramite Citrix
Atti Amministrativi	Datagraph	Client server tramite Citrix
Demografici	Fornitori diversi (ADS, Datagraph, Data Management, Comune di Bologna)	Modalità diverse (web, client server tramite citrix, terminale 3270)
Edilizia Privata e SUAP	Ambito	Client server tramite Citrix
Tributi	Fornitori diversi (ADS, Datagraph, Advanced System, Comune di Bologna)	Modalità diverse (web, client server tramite citrix)
Gestione del personale (paghe) – Servizio Associato in Unione	Datagraph	Client server tramite Citrix
Gestione del personale (presenze) – Servizio Associato in Unione	Softer Bologna	Webmail
Servizi alla persona	Datagraph	Client server tramite Citrix
Siti web	Fornitori diversi (Progetti d'impresa, Red Turtle, Ambito)	Web
Posta elettronica	Studio Storti con il sistema Zimbra	Cloud

Nel corso del 2015 si è provveduto all'adozione di un piano di informatizzazione delle procedure ai sensi dell'art. 24 comma 3bis DL 90/2014 (L. 114/2014). Tale piano è stato approvato con Determina CED N. 13 del 14/02/2015

Analisi dei rischi (regola 19.3 dell'Allegato B al Codice)

In linea con l'art. 35, Capo I, Titolo V del d.lgs. n. 196/2003 che "*impone di 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"* si procede analizzando i rischi a cui sono soggetti i dati informatici ed i dati cartacei trattati dagli incaricati dell'ente.

Per ciò che concerne le azioni intraprese per fronteggiare tali rischi si rimanda al successivo capitolo Azione Intraprese e strumenti utilizzati.

Analisi dei rischi dei dati elettronici

I rischi ai quali possono essere soggetti i dati residenti sugli elaboratori presenti nell'ente, già precedentemente inventariati, sono i seguenti:

- Accesso indebito alle risorse sia da parte di personale interno non autorizzato, che da parte di "pirati" esterni.
- Rischi connessi alla trasmissione dei dati.
- Perdita dei dati e quindi perdita della loro integrità fisica.
- Errori operativi volti a minare l'integrità logica dei dati.
- Azioni dolose.
- Manomissioni o furti.
- Eventi dannosi o disastrosi.

Presentazione sintetica dei rischi a cui sono soggetti i dati elettronici trattati dall'Unione Reno Galliera.

Rischio	Dettaglio	Gravità stimata	Probabilità di accadimento
Accesso indebito alle risorse da parte di utenti interni all'ente	• Accesso alle banche dati non autorizzato. • Copie non autorizzate dei dati per il trasporto all'esterno dell'ente	○ Alta ○ Alta	○ Bassa ○ Media
Comportamenti degli operatori	• Furto di credenziali di autenticazione • carenza di consapevolezza, disattenzione o incuria • comportamenti sleali o fraudolenti • errore materiale	○ Alta ○ Alta ○ Alta ○ Media	○ Bassa ○ Bassa ○ Bassa ○ Bassa
Eventi relativi agli strumenti	• azione di *virus* informatici o di codici malefici • spamming o altre tecniche di sabotaggio • malfunzionamento, indisponibilità o degrado degli strumenti	○ Alta ○ Alta ○ Media	○ Media ○ Media ○ Media

Rischio	Dettaglio	Gravità stimata	Probabilità di accadimento
Eventi relativi al contesto	• accessi non autorizzati a locali/reparti ad accesso ristretto • Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ...)	○ Media ○ Alta	○ Bassa ○ Media
Sicurezza nelle trasmissioni dei dati	• Tentativi di carpire i dati che vengono inviati all'ente da parte di pirati esterni. • Tentativi di carpire i dati che vengono spediti dall'Unione Reno Galliera da parte di pirati esterni. • Rischio di invio dati a destinatari sbagliati. • Tentativi di intrusione nella rete interna dell'ente. dall'esterno, da Internet, da sedi di comuni collegati via linee telefoniche all'ente e da parte di pirati esterni.	○ Alta ○ Alta ○ Bassa ○ Alta	○ Media ○ Media ○ Bassa ○ Media

Rischio	Dettaglio	Gravità stimata	Probabilità di accadimento
Rischi circa l'integrità fisica dei dati	• Cancellazione involontaria/accidentale dei dati. • Servizi di back-up non andati a buon fine.	○ Bassa ○ Bassa	○ Bassa ○ Bassa
Rischi circa l'integrità logica dei dati	• Incongruenze fra i dati. • Le applicazioni software in uso che creano disallineamenti.	○ Bassa ○ Bassa	○ Bassa ○ Bassa
Rischi manomissioni o furti o azioni dolose	• Manomissioni del CED. • Furti di dati sia dagli elaboratori, che degli elaboratori stessi.	○ Alta ○ Alta	○ Bassa ○ Bassa
Eventi dannosi o disastrosi	• Incendio. • Terremoti, alluvioni ed ogni altro evento non prevedibile.	○ Alta ○ Impredicibile	○ Media ○ Alta

Azioni intraprese

Modalità di accesso ai sistemi e ai dati

Rischio	Azione
Criteri e procedure per evitare l'accesso indebito alle risorse da parte di utenti interni all'ente	• Ogni utente ha un codice identificativo ed una password che lo abilitano ad entrare nel sistema di rete limitatamente ai dati necessari per lo svolgimento delle proprie mansioni. La password è a scadenza secondo i requisiti normativi • L'abilitazione per entrare in rete permette per la quasi totalità delle applicazioni; i casi in cui c'è un sistema di credenziali distinto sono residuali
Criteri e procedure per disciplinare il comportamenti degli operatori	• Formazione periodica di tutti gli incaricati e diffusione del disciplinare di utilizzo dei sistemi informativi approvato con delibera Giunta dell'Unione 19 del 29/06/2010 • Controlli periodici circa l'operato degli utenti • Controlli degli accessi, sia fisici che informatici • Content filtering tramite server proxy
Criteri e procedure per assicurare l'integrità logica dei dati	• Le applicazioni software in uso coprono l'ente da tale rischio

Rischio	Azione
Elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni	• Ogni volta che si presenta la necessità vengono tenute delle sessioni di aggiornamento, anche nell'ambito della formazione all'utilizzo dei nuovi strumenti informatici, volte ad assicurare tale conoscenza e l'aggiornamento della stessa

Misure fisiche, tecnologiche

Rischio	Azione
Criteri e procedure per disciplinare gli eventi relativi al contesto	• Tutti i locali sono ad accesso controllato • I sistemi di condizionamento del CED sono a tolleranza di guasto, sono disponibili in coppia ed in caso di guasto è pronta ad intervenire la società che ne ha in gestione la manutenzione • Nel locale della sala server è disponibile un sistema antincendio con sensori di rilevazione e spegnimento automatico a sali di potassio attivato nel febbraio 2015
Criteri e procedure per assicurare <u>l'integrità fisica</u> dei dati	• I back-up sono normalmente archiviati in su disco nella sede di disaster recovery presso l'Unione. • È installato un sistema antivirus. Il prodotto adottato è dato dalla suite

Rischio	Azione
	della Sophos
Criteri e procedure per assicurare la sicurezza nelle trasmissioni dei dati	• L'accesso alla rete pubblica degli utenti è regolamentato da strumenti tecnici (firewall) che consentono l'accesso al servizio solo agli incaricati che ne hanno necessità e registrano le attività fatte • I suddetti sistemi proteggono la rete locale da accessi indebiti alle risorse da parte di "pirati" esterni • La comunicazione con alcuni fornitori ed utenti avviene tramite router specifico via VPN, associati ai relativi username e password
Criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché individuazione delle procedure per controllare l'accesso delle persone autorizzate ai locali medesimi: ciò al fine di evitare al massimo manomissioni o furti o azioni dolose	• I server di rete sono localizzati in un ambiente – CED ad accesso controllato, la cui chiave è nelle mani esclusive dei membri del Servizio Informatico e delle altre persone autorizzate
Criteri tecnici ed organizzativi per limitare al massimo gli effetti di eventi dannosi o disastrosi	• Il piano di disaster recovery è definito ed è stato comunicato all'AGID nel 2012; la sede di Disaster Recovery è presso l'Unione Reno Galliera dove c'è una infrastruttura di server simile a quella del

Rischio	Azione
	Data Center principale
Controlli periodici	• Il responsabile e l'amministratore di sistema effettuano controlli periodici annuali circa l'applicazione delle regole suddette
Criteri e procedure per disciplinare gli eventi relativi agli strumenti	• Aggiornamento e potenziamento periodico dei sistemi antivirus installati

Privacy e gestione dei trattamenti

Ogni ente dell'Unione, ha previsto con atti interni propri all'individuazione del titolare dei trattamenti dei dati nonché all'individuazione dei responsabili e alla nomina degli incaricati.

Descrizione analitica degli strumenti utilizzati

Le operazioni di salvataggio dei dati: regola 19.5 dell'Allegato B al Codice

Si presenta, di seguito, il piano di sicurezza specifico per le operazioni di salvataggio dei dati, che nell'ambito del D.p.s. è sicuramente il documento che riveste la maggiore importanza.

Il sistema di back-up dei dati dei server è separato per ogni server e centralizzato nelle responsabilità: è basato su diversi software di back-up che pilotano disco di rete.

Il back-up è quotidiano full. Vengono conservati 30 giorni precedenti.

Tramite il sistema di storage, durante la giornata lavorativa vengono effettuate delle immagini periodiche del file system.

Il backup viene effettuato su dischi di rete nella sede di disaster recovery.

Non viene previsto alcun sistema di back-up dei client in quanto si è già specificato che tutti i dati sono e devono risiedere su server.

Di seguito elencheremo le operazioni previste, che fungono da manuale di istruzioni per gli incaricati addetti, ed il responsabile della esecuzione di tali operazioni:

1. Eseguire giornalmente il back-up dei dati
2. Archiviare i supporti del back-up sotto chiave
3. Controllare che le versioni del software di back-up siano allineate alle ultime versioni disponibili → Luca Tolomelli
4. Eseguire trimestralmente una prova di restore parziale dei dati
5. Eseguire annualmente una prova di restore dei dati ai fini di disaster su di un server jolly
6. Provvedere a centralizzare in luogo definito, CD ROM dei sistemi operativi e dei software di sistema, in modo da averli sempre a disposizione in caso di bisogno
7. Provvedere a centralizzare in luogo definito e sicuro, copie dei back-up, in modo da averli sempre a disposizione in caso di bisogno

I controlli anti-intrusione dall'esterno

Presentiamo di seguito il piano di sicurezza relativo ai controlli anti-intrusione: anche in questo caso elencheremo le operazioni previste, che fungono da manuale di istruzioni per gli incaricati addetti.

1. tenere aperto il monitor relativo ai tentativi di intrusione che il firewall offre

2. eseguire settimanalmente il controllo del log relativo ai tentativi di intrusione
3. avvisare l'amministratore di sistema dei dati di eventuali attacchi
4. attivare azioni correttive
5. chiedere consulenza al fornitore dell'assistenza sistemistica su altre precauzioni da adottare

Azioni intraprese per il fault tolerance: regola 19.5 dell'Allegato B al Codice

Le soluzioni adottate per attivare un meccanismo di fault tolerance per ciascuno dei device in elenco sono strettamente legate al fattore criticità ed al tipo di device di fronte al quale ci troviamo. Come si evince dall'elenco ci troviamo di fronte ai seguenti a sistemi che possiamo così catalogare:

- Server Windows 200X - Server Linux - Database Server
- Switch
- Router e Firewall
- Collegamenti WAN per telecomunicazioni
- Sistema di storage
- Sistema di alimentazione elettrica
- Sistema antincendio

E' opportuno evidenziare che i fault vengono monitorati grazie al sistema Hobbit che permette di individuare le interruzioni del servizio su:

- server fisici e virtuali
- apparati di rete
- connessioni LAN e WAN

Analizziamo ora le azioni adottate per ciascun elemento

Server Windows 200X – Server Linux – Database server

Una prima considerazione va fatta sulla macchina fisica. I servizi su questi server sono critici, ma esistono già dei sistemi di fault tolerance sui dischi (Raid 1); e sulle memorie RAM. Come per tutti i server, la macchina è coperta da 3 anni di garanzia e dopo il terzo anno è prevista la sostituzione della macchina stessa. Le operazioni sopra riportate sono eseguite dal responsabile della rete interna. In caso di assenza del responsabile di rete l'operazione può essere fatta da uno qualunque dei membri del Servizio Informatico.

Le macchine virtuali sono facilmente "spostabili" su altri server fisici, con una operazione a cura degli operatori del CED.

Switch

Attualmente nell'Unione Reno Galliera risultano installati diversi switch sui quali si basano tutta l'architettura di rete delle sedi interessate dal progetto ed hanno chiaramente un fattore elevato di criticità.

In caso di fault gli switch possono essere sostituiti, temporaneamente e con l'obiettivo di far ripartire un servizio, anche se ridotto, da un vecchio modello, disponibile a magazzino. La rete ripartirà comunque anche se con velocità ridotte. Le operazioni sopra riportate sono eseguite dal responsabile della rete interna. In caso di assenza del responsabile di rete l'operazione può essere fatta da uno qualunque dei membri del Servizio Informatico.

Firewall e Router

I router costituiscono la portante delle comunicazioni dell'ente verso il mondo esterno. I router sono apparecchiature sulle quali non è sempre possibile prevedere un back-up a caldo e d'altronde non è possibile pensare di tenere una macchina di questo tipo di scorta in magazzino. Le precauzioni intraprese sono due:

1. Il router che connette l'ente ad Internet tramite la rete a Larga Banda LEPIDA è in gestione e manutenzione dalla società Lepida.

2. Per le connessioni HDSL il router è a noleggio ed è assistito da Telecomitalia, la quale assicura dei livelli di SLA Service Level Agreement in grado di assicurare tempi di intervento dell'ordine delle 8 ore dalla segnalazione di guasto o del problema.

Le connessioni in fibra ottica sono gestite tramite switch e apparecchiature relative (media converter, ecc.).

Il firewall è ridondato ovvero ci sono due sistemi Sonicwall 4060 in modalità attivo – passivo: quando il firewall primario va in fault interviene il secondario che ha le stesse configurazioni del primario. Il sistema è assistito direttamente in gestione e manutenzione alla System Service.

Collegamenti WAN per telecomunicazioni

Tutti i collegamenti LAN principali sono in fibra ottica a 1000 Mb/s grazie alla rete regionale Lepida che fornisce assistenza 24x7 e su cui si appoggia anche la telefonia in modalità VOIP. Presso la sede del CED è attivo un collegamento di backup HDSL.

Sistema di Storage

Sul sistema di storage sono memorizzati i pool delle macchine XEN, il file server e i database server.

Il sistema di Storage (SAN NetApp Fas 2220) gode della garanzia triennale del produttore ed è supportato da un punto di vista sistemistica dalla ditta 3Cime Technology.

Il sistema è a doppia testa ridondata (per gestire eventuali fault di controller, CPU, sistema operativo, ecc).

In caso di fault di dischi la situazione è la seguente:

- in caso di rottura di un disco il sistema continua a funzionare e viene attivata in automatico una richiesta di sostituzione al fornitore;
- in caso di rottura di due dischi (sullo stesso array) il sistema continua a funzionare per 2 ore e poi si mette in protezione non potendo garantire integrità dei dati;
- in caso di rottura di 3 dischi sullo stesso array il sistema cessa di funzionare ed è necessario il ripristino dei backup;
- in caso di rottura di due dischi su array diversi il sistema continua a funzionare (come nel caso di un fault di un singolo disco);

Alimentazione elettrica

Tutti i server dispongono di doppia alimentazione e ogni alimentazione si appoggia ad un gruppo di continuità diverso. I gruppi di continuità sono alimentati da linee elettriche distinte.

In caso di sovratensioni gli UPS vanno in protezione per evitare danneggiamenti al sistema ed è necessario provvedere a riattivarlo.

Sistema antincendio

Il sistema antincendio dispone di sensori per la rilevazione dei fumi attraverso i quali c'è l'attivazione del sistema automatico di spegnimento che si basa su una tecnologia a sali di potassio. All'esterno della sala sono disponibili una serie di pulsanti e interruttori che permettono l'attivazione o il blocco manuale del sistema.

Il sistema è attivo da febbraio 2015, controllato e verificato 2 volte all'anno.

Procedure da seguire in caso di fault

La procedura da seguire, che cercheremo di definire passo a passo, è strettamente legata alle soluzioni tecniche adottate. Vero è che quasi tutti i sistemi di fault tolerance individuati si attivano in modo automatico. Ci sono però delle azioni da eseguire comunque.

Server

Il sistema virtualizzato (prevalentemente anche se non totalmente) pemette nella stragrande maggioranza dei casi di affrontare eventuali fault fisici senza interruzioni del servizio. Vediamo nel dettaglio le operazioni da compiere.

1. Rilevazione del fault tramite il sistema di monitoraggio
2. Rilevazione dell'impatto sui servizi
3. Nel caso il fault sia limitato a una singola macchina spostamento delle macchine virtuali su altre macchine
4. Attivazione delle richieste di assistenza hardware e sistemistica
5. In caso di eventi disastrosi che coinvolgono vari server, recupero dei backup e reinstallazione dei server anche in una sede diversa

Switch

Tutti gli switch garantiscono il lavoro di tutti gli utenti e quindi <u>devono funzionare sempre</u>. In caso di fault di uno switch le operazioni che il responsabile del CED dell'ente devono fare sono due:

1. accedere immediatamente al magazzino e recuperare uno switch o un hub di scorta;

2. provvedere alla sostituzione dello switch danneggiato con uno di scorta: gli utenti potranno

così ricominciare a lavorare anche se con prestazioni ridotte;

3. provvedere alla reintegrazione del router di scorta

Firewall e connessione ad Internet

1. In caso di fallimento del firewall verifica che il sistema secondario sia partito correttamente
2. In caso di problemi contattare l'assistenza System Service
3. In caso di fault delle connessioni Lepida viene contattato il numero di assistenza Lepida attivo 24 x 7
4. In caso di fault prolungato della rete Lepida deve essere attivato il collegamento con la linea HDSL

Sistema di storage

1. In caso di fault di un disco del sistema Storage (FAS NetApp 2020) avviene la richiesta automatica al fornitore che invia un disco sostitutivo e un tecnico per l'installazione entro la giornata lavorativa; tale attività non richiede interventi del personale del servizio informatico che devono solamente presidiare la corretta evoluzione delle attività (si noti che il blocco di un disco non causa il blocco del sistema come evidenziato in precedenza).
2. In caso di altri fault e in caso di mancato riavvio dei sistemi viene attivata una richiesta di assistenza alla ditta 3Cime Technology che risponde entro 2 ore dalla richieste e interviene entro la giornata lavorativa

Alimentazione elettrica

1. Verifica che i gruppi di continuità siano entrati in funzione
2. In caso di prolungato fermo progressivo spegnimento dei server e delle postazioni di lavoro

Azioni da intraprendere per il disaster recovery

Dobbiamo innanzi tutto definire quali sono le sedi interessate allo studio di disaster recovery. Attualmente c'è la sede principale (CED presso Argelato) e la sede di disaster recovery su cui sono anche salvati i backup

Azione preventive da eseguire nella sede principale

1. eseguire giornalmente il back-up dei dati
2. controllare la corretta esecuzione dei back-up
3. controllare due volte alla settimana la buona riuscita dei back-up "disaster copy"
4. controllare che le versioni del software di back-up siano quelle presenti nei CD-ROM di installazione
5. provvedere a centralizzare in luogo definito e sicuro, esterno all'ente, o interno ma in luogo sicuro, CD ROM dei sistemi operativi e dei software di sistema e di back-up, in modo da averli sempre a disposizione in caso di bisogno

Procedure da seguire in caso di disaster

1. Innanzi abbiamo definito ed attivato una procedura che permette di avere periodicamente i dati ricoverati in un luogo sicuro, nel nostro caso la sede di "archiviazione dei dati di back-up-disaster". Nel nostro caso dunque ogni giorno una copia incrementale dei back-up definita "disaster copy" viene effettuata dalla sede principale alla sede di disaster recovery.
2. In secondo luogo si ricorda che giornalmente si eseguono e si controllano i back-up ordinari
3. nella sede di Disaster Recovery sono salvati anche i modelli delle macchine virtuali più utilizzate
4. Presso la sede di disaster sono disponibili alcuni server non utilizzati da attivare in caso di disastro;
5. avvertire del disastro i partner System Service, Datagraph, Ambito, ADS, 3Cime Technology perché si tenga pronto ad intervenire
6. definire gli utenti che dovranno ripartire nella sede di disaster
7. configurare la rete dati affinchè le postazioni di lavoro puntino ai server di disaster

8. riattivare il sistema di back-up sul nuovo server

Considerazioni su Router e Wan Link

1. avvertire del disastro il partner System Service perché si tenga ad intervenire
2. la sede di disaster è dotata di collegamento Lepida e quindi non è necessario attivare nuovi collegamenti o abbonamenti
3. provvedere alla riconfigurazione dei servizi firewall

Sistema di Storage e Alimentazione elettrica

1. Nella sede di disaster si dispone di un sistema di storage con caratteristiche inferiori ed è quindi necessario provvedere ad una ottimizzazione delle risorse e degli accessi
2. La sede di disaster è dotata di alimentazione elettrica adeguata

Conclusioni

La realizzazione di un ambiente strutturato e centralizzato avvenuta in questi anni ha reso più critiche le politiche di sicurezza perché il fault della server farm centrale implica il blocco di tutti gli utenti di tutti i comuni.

Le attività di fault tolerance e soprattutto di disater recovery sono rese difficili dalle caratteristiche del nostro sistema che di seguito evidenziamo:

- numero di applicazioni molto elevato
- in conseguenza c'è un elevato numero di server (oltre 60 server virtuali e 12 fisici) e una occupazione di spazio intorno agli 8 TB (otto TeraByte)

Per questo si è cercato negli ultimi anni di attivare misure più forti per favorire la continuità operativa e il ripristino in caso di eventi disastrosi. Tra queste evidenziamo:

- una continua verifica delle procedure e la formazione agli operatori;
- l'attivazione di linee di backup
- potenziamento degli apparati di rete, in particolare di quelli di fascia alta

Riferimenti

In conclusione si riepilogano gli atti rilevanti citati nei presenti documenti

- il piano di informatizzazione delle procedure, determina CED 13 del 14/02/2015
- comunicazione ad AGID del piano di Disaster Recovery Prot. 6851/2012 del 23/04/2012
- disciplinare d'uso dei sistemi informativi, approvato con delibera di Giunta 19 del 29/06/2010