COPIA

DELIBERAZIONE N. 25
del 08/03/2013

COMUNE di VIGARANO MAINARDA
Provincia di FERRARA

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

OGGETTO:
DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (DPSS) EX ART. 34 C1 LETT. G) D.LGS 196 DEL 30.6.2003 - AGGIORNAMENTO

L'anno duemilatredici, addì otto del mese di Marzo alle ore 09:30 nella Casa comunale.

Previa l'osservanza di tutte le formalità prescritte dalla legge, vennero convocati a seduta i componenti della giunta municipale.

All'appello risultano:

PARON BARBARA	Sindaco	Presente
GIORGI ANDREA	Vice Sindaco	Presente
MASSARI GIULIA	Assessore	Presente
TAGLIANI FLAVIO	Assessore	Presente
SCIANNACA MARIO	Assessore	Presente

Assiste alla seduta il Segretario Comunale Dr. MUSCO ANTONINO.

Essendo legale il numero degli intervenuti, PARON BARBARA - Sindaco - assume la presidenza e dichiara aperta la seduta per la trattazione dell'oggetto sopra indicato.

OGGETTO : DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (DPSS) EX ART. 34 C1 LETT. G) D.LGS 196 DEL 30.6.2003 - AGGIORNAMENTO

LA GIUNTA COMUNALE

VISTO il Decreto Legislativo n. 196 del 30.6.2003 "Codice in materia di protezione dei dati personali";

VISTO l'art.45 del dl 9.2.12 n.5 inerente "Disposizioni urgenti in materia di semplificazione e di sviluppo" che:
- ha soppresso la lettera g) del comma 1 del predetto decreto legislativo, il quale disponeva che il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico allegato sub B al decreto stesso, una serie di misure minime di sicurezza tra le quali la tenuta di un aggiornato Documento Programmatico sulla Sicurezza (DPSS);
- ha soppresso i paragrafi da 19 a 19.8 dell'allegato B "Disciplinare Tecnico in materia di misure minime di sicurezza" al sopracitato decreto legislativo, i quali stabilivano che entro il 31 marzo di ogni anno, il titolare di trattamenti di dati sensibili o giudiziari redige il documento programmatico sulla sicurezza (DPSS) contenente una serie di idonee informazioni rispetto alle banche dati e alle misure di sicurezza adottate;

RITENUTO peraltro opportuno,ancorchè non sussista più alcun obbligo al riguardo, aggiornare comunque il vigente Documento Programmatico Sulla Sicurezza adottato dall'ente, al fine di disciplinare compiutamente quanto già a suo tempo stabilito dal D.Lgs. 196/2003, ed in particolare:
1. l'elenco dei trattamenti di dati personali;
2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
3. l'analisi dei rischi che incombono sui dati;
4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonchè la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonchè in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato;

DATO ATTO che nel DPSS approvato con il presente atto è contenuto il piano di continuità operativa e di disaster recovery,previsto dall'art.50 bis del D.Lgs 30.12.2010 n.235 "Codice dell'Amministrazione Digitale", che definisce l'insieme dei metodi e degli strumenti finalizzati ad assicurare la continuità dei servizi istituzionali anche in presenza di eventi indesiderati che possono causare il fermo prolungato dei sistemi informatici;

RICHIAMATE la seguenti deliberazioni di Giunta comunale inerenti l'adozione e i successivi aggiornamenti al Documento programmatico sulla sicurezza;
n. 51 del 25.3.2004
n. 30 del 17.3.2005
n. 27 del 9.3.2006
n.26 del 2.3.2007
n.15 del 14.2.2008
n.22 del 6.3.2009
n.23 del 24.2.2010
n.30 del 10.3.2011
n.33 del 22.3.2012

RITENUTO di approvare il suddetto documento;

AD unanimità di voti,resi palesi

DELIBERA

1) di aggiornare il Documento Programmatico sulla Sicurezza (DPSS) adottato con delibera di giunta comunale n.51 del 25.3.2004 ed aggiornato con le deliberazioni di giunta comunale in premessa citate, come da allegato al presente atto di cui costituisce parte integrante e sostanziale;

2) di dare atto che nel DPSS approvato con il presente atto è contenuto il piano di continuità operativa e di disaster recovery,previsto dall'art.50 bis del D.Lgs 30.12.2010 n.235 "Codice dell'Amministrazione Digitale", che definisce l'insieme dei metodi e degli strumenti finalizzati ad assicurare la continuità dei servizi istituzionali anche in presenza di eventi indesiderati che possono causare il fermo prolungato dei sistemi informatici;

3) di dare atto che sulla proposta della presente deliberazione è stato espresso il parere tecnico di cui all'art. 49 del D.lgs. 267/2000,che si allega al presente atto,di cui costituisce parte integrante e sostanziale;

4) con separata votazione palese,ad esito unanime,la presente deliberazione viene dichiarata immediatamente eseguibile,ai sensi dell'art. 134 comma 4 del D.lgs. 267/2000, stante l'urgenza di provvedere.

COMUNE DI VIGARANO MAINARDA
Provincia di Ferrara

Proposta di Giunta

Giunta Comunale

Servizio/Ufficio: Affari Generali
Proposta N° 2013/21

Oggetto: DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (DPSS) EX ART. 34 C1 LETT. G) D.LGS 196 DEL 30.6.2003 - AGGIORNAMENTO

PARERE IN ORDINE ALLA REGOLARITA' TECNICA

[X] Favorevole [ ] Contrario

.....
.....

Li, 07/03/2013

Il Capo Settore

.....
.....

DELIBERAZIONE N° 25 DEL 08.03.13

COMUNE DI VIGARANO MAINARDA

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Indice

1. Tabella Revisioni

Revisione	Data	Descrizione	Redazione	Approvazione
0	25/03/2004	Prima emissione		DGC 51/2004
1	17/03/2005	Aggiornamento		DGC 30/2005
2	09/03/2006	Aggiornamento		DGC 27/2006
3	02/03/2007	Aggiornamento		DGC 26/2007
4	28/02/2008	Aggiornamento		DGC 15/2008
5	06/03/2009	Aggiornamento		DGC 22/2009
6	24/02/2010	Aggiornamento		DGC 23/2010
7	10/03/2011	Aggiornamento		DGC 30/2011
8	22/03/2012	Aggiornamento		DGC 33/2012

2. Definizioni

2.1 - Ai fini del presente documento si intende per:

a) **"trattamento"**, qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, 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 di dati;

b) **"dato personale"**, 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;

c) **"dati identificativi"**, i dati personali che permettono l'identificazione diretta dell'interessato;

d) **"dati sensibili"**, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonche' i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

e) **"dati giudiziari"**, i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 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 qualita' di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

f) **"titolare"**, 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 finalita', alle modalita' del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

g) **"responsabile"**, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

h) **"incaricati"**, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

i) **"amministratore di sistema"** la figura professionale finalizzata alla gestione ed alla manutenzione di un impianto di elaborazione o di sue componenti,nonché la figura ad essa equiparabile dal punto di vista dei rischi relativi alla protezione dei dati;

l) **interessato"**, la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

m) **"comunicazione"**, il dare conoscenza dei dati personali a uno o piu' soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

n) **"diffusione"**, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

o) **"dato anonimo"**, il dato che in origine, o a seguito di trattamento, non puo' essere associato ad un interessato identificato o identificabile;

p) **"blocco"**, la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

q) **"banca di dati"**, qualsiasi complesso organizzato di dati personali, ripartito in una o piu' unita' dislocate in uno o più siti;

r) **"Garante"**, l'autorita' di cui all'articolo 153 D.lgs. 196/2003, istituita dalla legge 31 dicembre 1996, n. 675.

2.2 - Ai fini del presente documento si intende, inoltre, per:

a) "**comunicazione elettronica**", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente identificato o identificabile;

b) "**chiamata**", la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;

c) "**reti di comunicazione elettronica**", i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato

d) "**rete pubblica di comunicazioni**", una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;
e) "**servizio di comunicazione elettronica**", i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;

f) "**abbonato**", qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;
g) "**utente**", qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;
h) "**dati relativi al traffico**", qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;
i) "**dati relativi all'ubicazione**", ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

l) "**servizio a valore aggiunto**", il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto e' necessario per la trasmissione di una comunicazione o della relativa fatturazione;

m) "**posta elettronica**", messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

2.3 Ai fini del presente documento si intende, altresi', per:

"misure minime", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'art.31 D.Lgs 165/2003;

b) **"strumenti elettronici"**, gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
c) **"autenticazione informatica"**, l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

d) **"credenziali di autenticazione"**, i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
e) **"parola chiave"**, componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
f) **"profilo di autorizzazione"**, l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti; l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

g) **"sistema di autorizzazione"**, l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

3. Scopo del Documento

Il documento sulla sicurezza, ha lo scopo di definire le politiche di sicurezza in materia di trattamento dei dati personali e i criteri operativi e organizzativi necessari alla loro applicazione.

4. Riferimenti Legislativi

I principali riferimenti normativi sono costituiti da:
- "Codice in materia di protezione dei dati personali" D.lgs n. 196 del 30.6.2003 e s.m. e i.
- "Codice dell'Amministrazione Digitale" D.lgs n.235 del 30.12.2010 e s.m.e i.

5. Analisi dei rischi

Premesso che la finalità del D. lgs. 196/2003 è quella di garantire il rispetto dei diritti, delle libertà fondamentali e della dignità dell'interessato, trattasi di identificare e ridurre al minimo i rischi che, anche in modo accidentale, possono incombere su ogni tipo di dato in relazione al trattamento effettuato.

5.1) - Analisi dei rischi che incombono sui dati

Tipicamente sui dati incombono i seguenti rischi generali:

- Rischio rispetto alla riservatezza
- Rischio rispetto l'integrità dei dati
- Rischio rispetto alla disponibilità

5.1.1) - Rischio rispetto alla riservatezza

Definito come insieme di modalità di trattamento non autorizzato che possono verificarsi durante le categorie di attività, di seguito riportate, previste dalla legge:

- Raccolta
- Registrazione
- Organizzazione
- Conservazione
- Comunicazione
- Diffusione
- Selezione
- Estrazione
- Raffronto
- Interconnessione
- Utilizzo

5.1.2) - Rischio rispetto all'integrità dei dati

Definito come insieme di modalità di trattamento non autorizzato, che contemplano il rischio di modifica delle informazioni durante le categorie di attività, di seguito riportate, previste dalla legge:

- Elaborazione
- Distruzione
- Modifica
- Cancellazione
- Blocco

5.1.3) - Rischio rispetto alla disponibilità dei dati

Definito come insieme di eventi in grado di ridurre la capacità dell'incaricato di compiere le operazioni di trattamento per i quali i dati stessi sono stati raccolti.

5.2) - Categorie di rischio

a) - **Rischi derivati da condizioni ambientali in cui operano le apparecchiature**
Tipicamente appartengono a questa categoria:
a) - I rischi connessi ad attività di manutenzione generale dei locali contenenti apparecchiature elettroniche destinate al memorizzazione e/o ricovero di dati

b) - **Rischi derivati da condizioni ambientali in cui vengono conservati supporti di memorizzazione contenenti le copie di sicurezza dei dati**
Tipicamente appartengono a questa categoria:
a) - I rischi connessi alla mancanza di opportune strutture conservative dei supporti di memorizzazione di massa destinati al backup

c) - **Rischi derivanti da non corretta manutenzione delle apparecchiature di backup**
Tipicamente appartengono a questa categoria:
a) - I rischi connessi alla mancanza di strategie di backup
b) - I rischi di distruzione parziale o totale dei supporti di massa per effetto di avarie parziali o totali degli stessi

d) - **Rischi dovuti a imperizia nell'uso delle apparecchiature e delle procedure**
Tipicamente appartengono a questa categoria:
a) - Distruzione parziale o totale dei medesimi per effetto di utilizzo non conforme delle apparecchiature di elaborazione.
b) - Cancellazioni parziali o totali di files contenenti dati soggetti al "codice "

e) - **Rischi di distruzione totale o parziale di archivi per effetto di eventi eccezionali (crolli, incendi, inondazioni ecc)**

f) - **Rischi connessi alla distruzione parziale o totale di dati per effetto di intrusioni non autorizzate o effettuate da personale non sufficientemente addestrato attraverso connessioni telefoniche o similari**

g) - **Rischi connessi alla distruzione parziale o totale di dati per effetto di intrusioni di virus informatici**

h) - **Rischi derivanti da cattiva manutenzione delle apparecchiature elettroniche di memorizzazione dei dati**

i) - **Rischi derivati dalla mancanza di personale perfettamente addestrato alla prassi operativa e conservativa dei supporti di memorizzazione di massa destinati al backup**

5.3) - Livelli di rischio

CODICE	DESCRIZIONE
Alto	Rischio da non correre
Medio	Rischio cui è possibile ovviare senza particolari problemi
Basso	Rischio estremamente improbabile

6. I compiti delle persone preposte alla protezione dei dati personali

Come riportato nelle definizioni, si indica come **"titolare del trattamento"**, 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 specie viene quindi individuato come titolare il **COMUNE DI VIGARANO MAINARDA** rappresentato nella persona del **Sindaco pro - tempore** del Comune stesso.

Viene indicato, **"responsabile del trattamento"**, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali. Nel caso di specie vengono quindi individuati quali responsabili del trattamento i singoli **Responsabili di settore** in carica alla data di estensione dell'ultima revisione del presente documento, operanti presso le rispettive strutture organizzative di competenza,come da prospetto di cui al successivo articolo. La qualità di responsabile decade per revoca o per cessazione dei compiti che comportano tale status.

Gli **"incaricati"** sono costituiti dalle persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile. La qualità di incaricato decade per revoca o per cessazione dei compiti che comportano tale status. Nel caso di specie vengono quindi individuati quali incaricati del trattamento i **dipendenti e/o i destinatari di incarico libero-professionale e di incarico di collaborazione coordinata e continuativa,nonché altri addetti espressamente incaricati (volontari AUSER) operanti presso le rispettive strutture organizzative di competenza**, come da prospetto di cui al successivo articolo.

Si definisce **"amministratore di sistema"** la **figura professionale finalizzata alla gestione ed alla manutenzione di un impianto di elaborazione o di sue componenti, nonché la figura equiparabile** 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.

6.1 Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati

TITOLARE DEL TRATTAMENTO

ENTE	*RAPPRESENTANZA*
COMUNE DI VIGARANO MAINARDA	Sindaco pro-tempore PARON BARBARA

RESPONSABILI DEL TRATTAMENTO

SETTORE	*NOMINATIVO*	*QUALIFICA*
AFFARI GENERALI ORGANIZZAZIONE RISORSE UMANE SERVIZI DEMOGRAFICI E CIMITERIALI	FERRANTE MARCO	Istruttore Direttivo Capo settore
FINANZE - BILANCIO	DROGHETTI LIA	Istruttore Direttivo Capo settore
TECNICO	CHIARELLI MASSIMO	Istruttore Direttivo Capo settore
COMMERCIO ATTIVITA' PRODUTTIVE POLIZIA MUNICIPALE	SICILIANO CARMELA	Istruttore Direttivo Capo settore
CULTURA-POLITICHE GIOVANILI - PUBBLICA ISTRUZIONE - SPORT-SERVIZI ALLA PERSONA SOCIALI E SANITARI	MASTRANGELO SILVIA	Istruttore Direttivo Capo settore

RESPONSABILI ESTERNI DEL TRATTAMENTO

AUTOMATIC DATA SYSTEM - ADS	Bologna
LEPIDA spa	Bologna

AMMINISTRATORE DI SISTEMA

	FUNZIONI ATTRIBUITE
MANGOLINI NORBERTO Titolare ditta SISTEMI LOGICI di Mangolini Norberto Via Panetti n.40 - Ferrara	quelle risultanti nell'elencazione contenuta nel decreto di nomina predisposto dal Sindaco - Titolare del trattamento,n.19 del 4.9.2009

INCARICATI DEL TRATTAMENTO

SETTORE	NOMINATIVO	QUALIFICA
AFFARI GENERALI	MUSCO ANTONINO	Segretario Comunale
ORGANIZZAZIONE RISORSE	FERRANTE MARCO	Istr. Direttivo capo settore
UMANE	ZANIBONI FIORELLA	Istruttore Amministrativo
SERVIZI DEMOGRAFICI E	TILOMELLI UMBERTA	Istruttore Amministrativo
CIMITERIALI	CAZZIARI CRISTINA	Istr. Direttivo Amministrativo
	PILATI NADIA	Istruttore Amministrativo
	GANZAROLI LORENA	Istruttore Amministrativo
	MANGOLINI NORBERTO	Amministratore di Sistema (Sistemi Logici)
	MANGOLINI MASSIMO	(Sistemi Logici)
	MANGOLINI ANDREA	(Sistemi Logici)
FINANZE - BILANCIO	DROGHETTI LIA	Istr. Direttivo Capo settore
	BARBIERI MARIA	Istruttore Direttivo Contabile
	GIRARDI DANIELA	Istruttore Contabile
	CROCE CRISTINA	Istruttore Contabile
	GUANDALINI CLARISSA	Istruttore Contabile
TECNICO	CHIARELLI MASSIMO	Istr. Direttivo Capo settore
	GIOVANNINI MILLER	Istruttore Direttivo Tecnico
	MASETTI MIRELLA	Istruttore Amministrativo
	ZANCOGHI PAOLA	Istruttore Direttivo Amm.vo
	RIGATTIERI VALENTINA	Istruttore Amministrativo
	CHIERICATI MARCO	C.Prof.le Coord.Servizi Esterni
COMMERCIO	SICILIANO CARMELA	Istr. Direttivo Capo settore
ATTIVITA' PRODUTTIVE	FERRON GABRIELLA	Istr. Direttivo Amministrativo
POLIZIA MUNICIPALE	BARBI MONICA	Istr. Agente Polizia Municipale
	MARCHESELLI ANGELA	Istr. Agente Polizia Municipale
	RIZZETTO MARCO	Istr. Agente Polizia Municipale
	GAMBARELLI ANGELA	Istr. Agente Polizia Municipale
	ISEPPI LEONARDO	Istr. Agente Polizia Municipale
	LODI DIEGO	Istr. Agente PM a tempo det.
	SITTA ROSA MARIA	Esecutore Messo Notificatore
CULTURA - POLITICHE	MASTRANGELO SILVIA	Istr. Direttivo Capo settore
GIOVANILI	BONAZZI STEFANIA	Istruttore Amministrativo
PUBBLICA ISTRUZIONE	BERGAMI FRANCESCA	Istruttore Amministrativo
SPORT E TEMPO LIBERO	ROMANI PAOLA	Istruttore Amministrativo a tempo det. (lav.somministrato)
SERVIZI ALLA PERSONA		
SOCIALI E SANITARI	MAZZONI BEATRICE	Istruttore Amministrativo
	PETAZZONI MORENA	Esecutore Amministrativo
	PANIGALLI STEFANO	Istruttore Amministrativo a tempo det. (lav.somministrato)
	CARLETTI IRENE	Incarico CO.CO.CO.
	BRESCANZIN ANTONIO	Volontario AUSER

6.2 Dati affidati ad enti o soggetti esterni per il trattamento dei dati all'esterno della struttura

Il Titolare del trattamento può decidere di affidare in tutto o in parte ad enti o soggetti esterni il trattamento dei dati all'esterno della struttura, nominandoli Responsabili del trattamento.

* Se i soggetti terzi vengono espressamente nominati Responsabili del trattamento, devono essere specificati:

- i soggetti interessati
- i luoghi dove fisicamente avviene il trattamento dei dati
- i responsabili del trattamento
- il tipo di trattamento effettuato

* Se i soggetti terzi non vengono espressamente nominati Responsabili del trattamento, gli stessi devono intendersi autonomi Titolari del trattamento, ai sensi dell'art. 28 del Codice, e quindi soggetti ai corrispettivi obblighi, e pertanto rispondono direttamente ed in via esclusiva per le eventuali violazioni di legge.

Possono essere nominati Responsabili del trattamento dei dati all'esterno della struttura, quei soggetti terzi che per esperienza,capacità ed affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento.

Il Responsabile del trattamento dei dati all'esterno della struttura deve rilasciare una dichiarazione scritta al Titolare del trattamento da cui risulti che sono state adottate le misure idonee di sicurezza per il trattamento dei dati secondo quanto disposto dal Codice e dal Disciplinare Tecnico.

7.Risorse da proteggere e piano di continuità operativa e di disaster recovery

Fondamentalmente le risorse da proteggere sono costituite da:

- Sistemi hardware
- Procedure software
- Banche dati

7.1 - Sistemi hardware

La tabella seguente riporta i principali sistemi da proteggere e le protezioni adottate.

Sistemi da proteggere:

Localizz.	Denominazione	S.O.	Banche dati
CED	Server Proliant ML 380 G6	VMWARE Vsphere 4	Server IP 102 Server IP 103 Server IP 105
CED	Server Proliant ML 380 - 421	S.C.O.	Archivi generali procedure ADS
CED	Server Virtuale IP 102 Server Virtuale IP 103 Server Virtuale IP 105	-	Archivi Terminalizzati procedure ADS eArchivi Gruppi Archivi Velocar
Biblioteca	Pc HP con funzione di Server	Win Xp SP3	Archivi Biblioteca
Casa Protetta	Workstation con funzioni "Server"	Win XP Pro Sp3	Archivi Casa Protetta *

Protezioni adottate:

Localizz.	Denominazione	Sist. BK	Antivirus	Alimentazione
CED	Server Virtuale IP 102 Server Virtuale IP 103 Server Virtuale IP 105	NAS Netgear RAID 5 QNAP Bk Full	Su Client e su firewall	Gr. Continuità
CED	Server Proliant ML 380 - 421	QNAP Bk Oracle	Su Client e su firewall	Gr. Continuità
Biblioteca	Pc HP con funzione di Server	NAS Netgear Dischi esterni	Su Client	Gr. Continuità In fase di installazione
Casa Protetta	Workstation "Server"	Su dischi esterni	Si	No

Principali Accessi Esterni:

Tipo Linea	Ubicazione	Utilizzo	Protezione	Antivirus
HDSL 2mb	Sede Municipale	Rete Lepida Internet Posta Elettronica	Firewall Hw	Si
ADSL 256	Sede Municipale	Controllo remoto client	Firewall Hw	Su Clients
ADSL 256	Casa Protetta	Internet Posta Elettronica	Firewall Hw	Su clients
ADSL 256	Biblioteca	Internet - Posta Elettronica	Firewall Hw	Su clients

7.2 - Misure adottate per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità (piano di continuità operativa e di disaster recovery)

7.2.1) - Garanzia di Integrità e Disponibilità dei dati

I dati sono mantenuti in linea da un server Compaq Proliant ML 380 - 421 dotato di n. 6 supporti di massa di tipo SCSI in modalità RAID 5. Il server in questione fa riferimento per il backup dei dati a un dispositivo QNAP che effettua giornalmente una copia fisica dei dati su supporti esterni al server. Il medesimo apparecchio effettua inoltre una copia completa dei server virtuali installati garantendo la massima sicurezza. E' in fase di approntamento, infine, il sistema secondario che permette di effettuare una seconda copia dei dati in questione sul NAS RAID 6 in dotazione al CED.
In tal modo viene garantita la completa integrità rispetto ai normali crash di tipo meccanico o elettronico di uno dei supporti costituenti il set dedicato.

7.2.2) - Protezione delle aree e dei Locali rilevanti ai fini della custodia e dell'accessibilità dei dati

La protezione delle aree e dei locali rilevanti rispetto alla custodia e accessibilità dei dati è assicurata nel locale CED da:

Rispetto alle intrusioni di personale non autorizzato da una porta a vetri, munita di idonea chiave di accesso;

Rispetto alla distruzione per incendio della copia di nastri di backup in servizio da un estintore a polvere.

Per quanto riguarda le caratteristiche di sicurezza della postazione CIE, si fa riferimento a quanto riportato nel Piano di Sicurezza presentato da questo Comune al Ministero dell'Interno.

7.2.3) - Piano di continuità operativa e di Disaster Recovery

L'ente ha commissionato l'elaborazione di un Disaster Recovery Planning che è stato approvato ed è pertanto completamente operativo. Tale piano viene allegato al presente DPSS a costituirne parte integrante e sostanziale

7.3 - Descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento.

In caso di parziale perdita di dati in linea e' possibile il loro recupero attraverso l'operazione di restore degli archivi relativi alle attività svolte il giorno precedente.
In caso di evento completamente distruttivo opera il Disaster Recovery Planning di cui al punto precedente.

8.Situazioni di criticità

8.1) - Aree Interessate

Di seguito verranno riportate le situazioni di rischio riferite ad ogni servizio:

Progr.	Denominazione	Composizione
1	Settore Affari generali Organizzazione Risorse umane Servizi Demografici e cimiteriali	Servizio Affari generali Servizio Organizzazione Risorse umane Servizio Demografici e cimiteriali
2	Settore Finanze e Bilancio	Servizio Ragioneria Servizio Tributi - Economato Servizio Contabilità del personale
3	Settore Tecnico	Servizio Lavori Pubblici Servizio Urbanistica - edilizia privata Servizio Ambiente - tutela del territorio
4	Settore Commercio - Att. Produttive - Polizia Municipale	Servizio Polizia Municipale Servizio Commercio - Attività produttive
5	Settore Cultura - Politiche Giovanili Pubblica Istruzione - Sport - Servizi alla persona sociali e sanitari	Servizio Cultura - politiche giovanili Servizio P.Istruzione-Sport e tempo libero Servizi alla persona sociali e sanitari

8.1.1) - Settore Affari Generali - Organizzazione Risorse Umane - Servizi Demografici e Cimiteriali

8.1.1.1) Composizione

Il settore è diretto dal Capo Settore Dr. Marco Ferrante ed e' così composto:

Funzionario	Funzione	Responsabilità ex D.Lgs 196/03
Musco Antonino	Segretario Comunale	Incaricato
Ferrante Marco	Capo settore	Responsabile
Zaniboni Fiorella	Istruttore Amministrativo	Incaricato
Tilomelli Umberta	Istruttore Amministrativo	Incaricato
Cazziari Cristina	Istruttore Direttivo	Incaricato
Pilati Nadia	Istruttore Amministrativo	Incaricato
Ganzaroli Lorena	Istruttore Amministrativo	Incaricato

8.1.1.2) - Dotazione Hardware

Il settore e' dotato di:

a) - 10 Unità di elaborazione elettronica interconnesse alla Lan Generale
b) - 2 unità di contenimento schede ad armadio motorizzato
c) - 3 Unità ad armadio non motorizzato

Le unità di elaborazione elettronica sono normalmente presidiate dal personale addetto. Accedono alla rete LAN attraverso **"autenticazione informatica"**, con **"credenziali di autenticazione** e relativa **parola chiave** per ogni addetto. Esiste infine un **"profilo di autorizzazione"** che consente ai componenti di accedere a un singolo segmento dedicato del sistema di memorizzazione di massa centrale.
Anche le unità di elaborazione individuali sono dotate individualmente di accesso attraverso **autenticazione informatica**, con **"credenziali di autenticazione** e relativa **"parola chiave** per ogni addetto. Le unità sono dotate di un proprio "profilo di autorizzazione" relativo ad ogni operatore del comparto. Le unità in questione sono dotate **di antivirus** locale.

Unità di contenimento schede ad armadio motorizzato
Le unità in questione sono dotate di sportello di chiusura e sono disposte in vista del personale addetto.

Unità ad armadio non motorizzato
Come per le unità motorizzate, sono fornite di serratura a chiave e sono in vista del personale addetto.

8.1.1.3) - Analisi dei rischi nel comparto

Tipo di Rischio	Livello Di rischio generalizzato	Impatto sui dati	Livello Locale	Azioni di contrasto
Furto di Credenziali di autenticazione	Basso	Danneggiamento parziale Archivi	Basso	Formazione agli operatori rispetto alle attenzioni da prestare all'inserimento delle credenziali
Spamming		Nessuno	-	- Antispamm su Firewall
Azione di Virus		Indiretto- Difficoltà di accesso	Basso	- Antivirus generale su accesso Internet - Antivirus Locale
Malfunzionamento o degrado strumenti informatici	Basso	Danneggiamento parziale Archivi	Basso	- Manutenzione continua e sostituzione apparecchiature non adeguate
Errore materiale	Basso	Danneggiamento parziale singolo record	Basso	Addestramento del personale
Asportazione e/o furto di strumenti contenenti dati	Basso	-	Basso	Sorveglianza dei locali operativi
Guasti agli impianti elettrici	Basso	Danneggiamento parziale Archivi	Basso	Manutenzione impianti elettrici

8.1.1.4) - Banche dati trattate

Banca Dati	Trattamento	Finalità	Dati Sensibili e Giudiziari	Trattamento Interno	Trattamento Esterno
Elenco Consiglieri e Assessori	Cartaceo Informatico	DPR 570/60	Sensibili	Registrazione Conservazione Consultazione	Comunicazione Diffusione DPR 570/60
Protocollo	Cartaceo Informatico	Finalità in ambito amm.vo e sociale DPR 445/00	Sensibili Giudiziari	Conservazione Registrazione Comunicazione Consultazione Selezione	-
Delibere e Determine	Cartaceo Informatico	Finalità in ambito amm.vo e sociale DLGS 267/00	Sensibili Giudiziari	Conservazione	Comunicazione Diffusione DLGS 267/00
Deposito Atti Giudiziari	Cartaceo	Attività sanzionatorie e di tutela Art. 140 C.P.C.	Giudiziari	Conservazione Registrazione	Comunicazione Art 140 C.P.C.
Elenco associazioni	Cartaceo Informatico	Finalità in ambito am.vo e sociale	-	Raccolta	Comunicazione
Ordinanze	Cartaceo	Attività sanzionatorie e di tutela. Finalità in ambito Amm.vo e sociale DLGS 267/00	Sensibili	Conservazione Consultazione	Comunicazione In funzione dell'ordinanza
Decreti del Sindaco e del Segretario Comunale	Cartaceo Informatico	Finalità in ambito amm.vo e sociale DLGS 267/00	-	Conservazione Consultazione	Comunicazione Funzioni istituzionali
Carte d'Identità	Cartaceo Informatico	Attività di PS R.D. 773/31 R.D. 635/40	Sensibili	Registrazione Conservazione Elaborazione	Comunicazione R.D. 635/40
Stato Civile	Cartaceo Informatico	Finalità in ambito Amm.vo e sociale DPR 396/00	Sensibili	Registrazione Conservazione Elaborazione Utilizzo Consultazione	Comunicazione Dlgs 322/89 L. 91/92 L. 127/97 Art 605 cpc
Anagrafe residenti, pensionati, cittadini stranieri	Cartaceo Informatico	Finalità in ambito Amm.vo e sociale L.1228/54 dpr 223/89 L.470/88	-	Registrazione Conservazione Elaborazione Utilizzo Consultazione	Comunicazione Dpr 394/99 Dm 18/12/00 L.470/88 L.903/65

		L.903/65			
Anagrafe italiani residenti all'estero	Cartaceo Informatico	Finalità in ambito Amm.vo e sociale L.470/88	-	Registrazione Conservazione Consultazione	Comunicazione L.470/88
Liste di Leva	Cartaceo Informatico	Finalità in ambito Amm.vo e sociale. DPR 237/64 L. 269/91	Sensibili	Registrazione Conservazione Elaborazione Organizzazione Utilizzo	Comunicazione Diffusione DPR 237/64 L. 191/75
Ruoli Matricolari	Cartaceo	Finalità in ambito Amm.vo e sociale. Regolam. Reg 1133/42 Circ. Minist. 487/29	Giudiziari	Registrazione Conservazione Elaborazione Organizzazione Utilizzo	Comunicazione Diffusione Regolam. Reg 1133/42 Circ. Minist. 487/29
Giudici Popolari	Cartaceo Informatico	Esercizio dei diritti politici. L. 287/51	Giudiziari	Registrazione Conservazione Elaborazione Organizzazione Utilizzo Modificazione Selezione	Comunicazione Diffusione L. 287/51
Liste Elettorali	Cartaceo Informatico	Esercizio dei diritti politici. T.U. 223/67 Circ.2600/86	Giudiziari	Registrazione Conservazione Elaborazione Utilizzo Consultazione Modificazione Selezione	Comunicazione T.U. 223/67 Circ.2600/86
Propaganda Elettorale	Cartaceo Informatico	Esercizio dei diritti politici. L.212/56 L.130/75 Circ. 1943/v 1980	Sensibili	Registrazione Conservazione Elaborazione Organizzazione Utilizzo Consultazione Selezione	Comunicazione L.212/56 L.130/75 Circ. 1943/v 1980
Albo scrutinatori e presidenti di seggio	Cartaceo Informatico	Esercizio dei diritti politici. L.120/99 L.53/90	Sensibili	Registrazione Conservazione Elaborazione Organizzazione Utilizzo Consultazione Selezione Modificazione	Comunicazione L.120/99 L.53/90
Liste di candidati Sottoscrittori Referendum e Proposte di legge	Cartaceo	Esercizio dei diritti politici e pubblicità dell'attività di determinati organi. T.U. 223/67	Sensibili	Registrazione Conservazione Raccolta	Comunicazione T.U. 223/67 L. 352/70

		L. 352/70			
Anagrafe Cimiteriale	Cartaceo Informatico	Attività Istituzionali DPR 285/90	-	Conservazione	-
Autorizzazioni cimiteriali	Cartaceo Informatico	Funzioni Istituzionali Dpr 285/90	-	Registrazione Conservazione Consultazione	-
Anagrafe utenti servizio luci votive	Cartaceo Informatico	Attività di controllo e ispettive	-	Raccolta Conservazione Organizzazione Utilizzo Selezione	Comunicazione
Albo beneficiari contributi	Cartaceo Informatico	Benefici economici e abilitazioni Dpr 118/00	-	Conservazione Organizzazione Utilizzo Elaborazione	Diffusione Dpr 118/2000
Comunicazione cessione di fabbricati	Cartaceo	Attività di controllo e ispettive	Sensibili	Registrazione Conservazione	Comunicazione
Schedine di prenotazione alberghiera	Cartaceo	Attività di controllo e ispettive	Sensibili	Registrazione Conservazione	Comunicazione

8.1.2) - Settore Finanze e Bilancio

8.1.2.1) Composizione

Il settore è diretto dal Capo Settore Rag. Lia Droghetti ed è così composto:

Funzionario	Funzione	Responsabilità ex D.Lgs 196/03
Droghetti Lia	Capo settore	Responsabile
Barbieri Maria	Istruttore Direttivo	Incaricato
Girardi Daniela	Istruttore Contabile	Incaricato
Croce Cristina	Istruttore Contabile	Incaricato
Guandalini Clarissa	Istruttore Contabile	Incaricato In comando all' Ufficio Associato del personale presso il Comune di Bondeno

8.1.2.2) - Dotazione Hardware

Il comparto e' dotato di:

a) - 5 Unità di elaborazione elettronica

b) - 2 Unità ad armadio non motorizzato

Le unità di elaborazione elettronica sono normalmente presidiate da personale addetto. Accedono alla rete LAN attraverso "**autenticazione informatica**",con "**credenziali di autenticazione** e relativa "**parola** chiave per ogni addetto. Esiste infine un "**profilo di autorizzazione**" che consente ai componenti di accedere a un singolo segmento dedicato del sistema di memorizzazione di massa centrale.
Anche le unità di elaborazione individuali sono dotate individualmente di accesso attraverso **autenticazione informatica**, con "**credenziali di autenticazione** e relativa "**parola chiave** per ogni addetto. Le unità sono dotate di un proprio "profilo di autorizzazione" relativo ad ogni operatore del comparto. Le unità in questione sono dotate **di antivirus** locale

Unità ad armadio non motorizzato
Come per le unità motorizzate, sono fornite di serratura a chiave e sono in vista del personale addetto.

8.1.2.3) - Analisi dei rischi nel comparto

Tipo di Rischio	Livello Di rischio generalizzato	Impatto sui dati	Livello Locale	Azioni di contrasto
Furto di Credenziali di autenticazione	Basso	Danneggiamento parziale Archivi	Basso	Formazione agli operatori rispetto alle attenzioni da prestare all'inserimento delle credenziali
Spamming		Nessuno	-	- Antispamm su Firewall
Azione di Virus		Indiretto- Difficoltà di accesso	Basso	- Antivirus generale su accesso Internet - Antivirus Locale
Malfunzionamento o degrado strumenti informatici	Basso	Danneggiamento parziale Archivi	Basso	- Manutenzione continua e sostituzione apparecchiature non adeguate
Errore materiale	Basso	Danneggiamento parziale singolo record	Basso	Addestramento del personale
Asportazione e/o furto di strumenti contenenti dati	Basso	-	Basso	Sorveglianza dei locali operativi
Guasti agli impianti elettrici	Basso	Danneggiamento parziale Archivi	Basso	Manutenzione impianti elettrici

8.1.2.4) - Banche dati trattate

Banca Dati	Trattamento	Finalità	Dati Sensibili e Giudiziari	Trattamento Interno	Trattamento Esterno
Anagrafe Tributaria	Cartaceo Informatico	Materia tributaria e doganale Prevista dal diritto tributario comunale	-	Registrazione Conservazione Elaborazione Organizzazione Utilizzo Modificazione Selezione	Comunicazione
Archivio Creditori Debitori	Cartaceo Informatico	Finalità in ambito amm.vo e sociale Dlgs 267/2000	Sensibili	Conservazione Modificazione Organizzazione Utilizzo Consultazione Selezione	Comunicazione Dlgs 267/2000
Personale dipendente, amministratori, collaboratori	Cartaceo Informatico	Finalità in ambito amm.vo e sociale Dlgs 267/2000	Sensibili Giudiziari	Modificazione Organizzazione Utilizzo Consultazione	-
Anagrafe Canina	Cartaceo Informatico	Attività di controllo e ispettive L.R. 27/00	-	Registrazione Conservazione Utilizzo Selezione Consultazione	Comunicazione L.R. 27/00
Richiedenti utilizzo sale di immobili comunali	Cartaceo	Funzioni istituzionali	Sensibili	Registrazione Conservazione Organizzazione Utilizzo	-
Autorizzazioni per l'esercizio dell'attività venatoria e della pesca	Cartaceo	Finalità in ambito amm.vo e sociale DPR 616/77	-	Conservazione Consultazione Modificazione Organizzazione	Comunicazione DPR 616/77
Denunce infortuni sul lavoro	Cartaceo	Finalità in ambito amm.vo e sociale DPR 1124/65	Sensibili	Registrazione Conservazione Utilizzo	Comunicazione DPR 1124/65

8.1.3) - Settore Tecnico

8.1.3.1) Composizione

Il settore è diretto dal Capo Settore Ing. Massimo Chiarelli ed e' così composto:

Funzionario	Funzione	Responsabilità ex D.Lgs 196/03
Chiarelli Massimo	Capo settore	Responsabile
Giovannini Miller	Istruttore Direttivo	Incaricato
Masetti Mirella	Istruttore Amministrativo	Incaricato
Zancoghi Paola	Istruttore Direttivo	Incaricato
Rigattieri Valentina	Istruttore Amministrativo	Incaricato In comando presso CMV servizi srl
Chiericati Marco	Collaboratore professionale Coordinatore Servizi Esterni	Incaricato

8.1.3.2) - Dotazione Hardware

Il comparto e' dotato di:

a) - 7 Unità di elaborazione elettronica
b) - 1 Unità ad armadio non motorizzato

Le unità di elaborazione elettronica sono normalmente presidiate da personale addetto. Accedono alla rete LAN attraverso "**autenticazione informatica**", con "**credenziali di autenticazione** e relativa "**parola** chiave per ogni addetto. Esiste infine un "**profilo di autorizzazione**" che consente ai componenti di accedere a un singolo segmento dedicato del sistema di memorizzazione di massa centrale.
Anche le unità di elaborazione individuali sono dotate individualmente di accesso attraverso **autenticazione informatica**, con "**credenziali di autenticazione** e relativa "**parola chiave** per ogni addetto. Le unità sono dotate di un proprio "profilo di autorizzazione" relativo ad ogni operatore del comparto. Le unità in questione sono dotate **di antivirus** locale

Unità ad armadio non motorizzato
Come per le unità motorizzate, sono fornite di serratura a chiave e sono in vista del personale addetto.

8.1.3.3) - Analisi dei rischi nel comparto

Tipo di Rischio	Livello Di rischio generalizzato	Impatto sui dati	Livello Locale	Azioni di contrasto
Furto di Credenziali di autenticazione	Basso	Danneggiamento parziale Archivi	Basso	Formazione agli operatori rispetto alle attenzioni da prestare all'inserimento delle credenziali
Spamming		Nessuno	-	- Antispamm su Firewall
Azione di Virus		Indiretto- Difficoltà di accesso		- Antivirus generale su accesso Internet - Antivirus Locale
Malfunzionamento o degrado strumenti informatici	Basso	Danneggiamento parziale Archivi	Basso	- Manutenzione continua e sostituzione apparecchiature non adeguate
Errore materiale	Basso	Danneggiamento parziale singolo record		Addestramento del personale
Asportazione e/o furto di strumenti contenenti dati	Basso	-		Sorveglianza dei locali operativi
Guasti agli impianti elettrici	Basso	Danneggiamento parziale Archivi	Basso	Manutenzione impianti elettrici

8.1.3.4) - Banche dati trattate

Banca Dati	Trattamento	Finalità	Dati Sensibili e Giudiziari	Trattamento Interno	Trattamento Esterno
Concessioni e autorizzazioni edilizie	Cartaceo Informatico	Finalità in ambito amm.vo e sociale L. 10/77 L. 47/35 L.R. 31/02	-	Registrazione Conservazione Consultazione	Comunicazione L. 10/77 L. 47/35 L.R. 31/02
Contributi per abbattimento barriere architettoniche	Cartaceo	Finalità in ambito amm.vo e sociale L. 13/89	Sensibili	Conservazione	Comunicazione L. 13/89
Contratti e Convenzioni Modelli GAP	Cartaceo Informatico	Attività di controllo ed ispettive L.726/82 L. 410/91	-	Registrazione Conservazione Consultazione	Comunicazione L.726/82 L. 410/91
Notifiche Atti notarili compravendita immobili	Cartaceo	Attività Istituzionali L. 47/85	-	Conservazione	-
Opere in Cemento armato o acciaio	Cartaceo	Attività Istituzionali L. 1086/71 DPR 425/94	-	Registrazione Conservazione	Comunicazione L. 1086/71 DPR 425/94
Insegne pubblicitarie	Cartaceo	Attività Istituzionali	-	Conservazione	-
Certificati di conformità impianti elettrici e idraulici	Cartaceo	Attività di controllo ed ispettive L. 46/90	-	Conservazione	-
Certificati di Destinazione urbanistica	Cartaceo	Attività Istituzionali L. 47/85	-	Conservazione	Comunicazione L. 47/85
Appaltatori opere pubbliche e soggetti partecipanti alle gare	Cartaceo Informatico	Attività di controllo ed ispettive L. 109/94	Giudiziari	Raccolta Conservazione Organizzazione	Comunicazione L. 109/94
Autorizzazioni scarico acque superficiali,corpo idrico,denunce pozzi	Cartaceo Informatico	Attività istituzionali D.lgs 152/99	-	Conservazione	Comunicazione D.lgs 152/99
Autorizzazioni emissioni in atmosfera	Cartaceo Informatico	Attività istituzionali L. 203/88	-	Conservazione	Comunicazione L. 203/88
Autorizzazioni abbattimento/potatura alberi	Cartaceo Informatico	Attività istituzionali	-	Conservazione	-
Associazioni ambientali	Cartaceo Informatico	Attività istituzionali	-	Conservazione	-
Autorizzazioni uso gas tossici	Cartaceo	Attività istituzionali RD 147/27	Giudiziari	Conservazione Modificazione	Comunicazione RD 147/27

8.1.4) - Settore Commercio - Attività Produttive - Polizia Municipale

8.1.4.1) Composizione

Il settore è diretto dal Capo Settore Dott.ssa Carmela Siciliano ed e' così composto:

Funzionario	Funzione	Responsabilità ex D.Lgs 196/03
Siciliano Carmela	Capo settore - Comandante PM	Responsabile
Ferron Gabriella	Istruttore Direttivo	Incaricato
Barbi Monica	Agente PM	Incaricato
Rizzetto Marco	Agente PM	Incaricato
Marcheselli Angela	Agente PM	Incaricato
Gambarelli Angela	Agente PM	Incaricato
Iseppi Leonardo	Agente PM	Incaricato
Lodi Diego	Agente PM a tempo determinato	Incaricato
Sitta Rosa Maria	Esecutore Messo Notificatore	Incaricato

8.1.4.2) - Dotazione Hardware

Il comparto e' dotato di:

a) - 7 Unità di elaborazione elettronica
b) - 3 Unità ad armadio non motorizzato

Le unità di elaborazione elettronica sono normalmente presidiate da personale addetto. Accedono alla rete LAN attraverso "**autenticazione informatica**",con "**credenziali di autenticazione** e relativa "**parola** chiave per ogni addetto. Esiste infine un "**profilo di autorizzazione**" che consente ai componenti di accedere a un singolo segmento dedicato del sistema di memorizzazione di massa centrale.
Anche le unità di elaborazione individuali sono dotate individualmente di accesso attraverso **autenticazione informatica**, con "**credenziali di autenticazione** e relativa "**parola chiave** per ogni addetto. Le unità sono dotate di un proprio "profilo di autorizzazione" relativo ad ogni operatore del comparto. Le unità in questione sono dotate **di antivirus** locale

Unità ad armadio non motorizzato
Come per le unità motorizzate, sono fornite di serratura a chiave e sono in vista del personale addetto.

8.1.4.3) - Analisi dei rischi nel comparto

Tipo di Rischio	Livello Di rischio generalizzato	Impatto sui dati	Livello Locale	Azioni di contrasto
Furto di Credenziali di autenticazione	Basso	Danneggiamento parziale Archivi	Basso	Formazione agli operatori rispetto alle attenzioni da prestare all'inserimento delle credenziali
Spamming	Alto	Nessuno	-	- Antispamm su Firewall
Azione di Virus	Alto	Indiretto- Difficoltà di accesso	Basso	- Antivirus generale su accesso Internet - Antivirus Locale
Malfunzionamento o degrado strumenti informatici	Basso	Danneggiamento parziale Archivi	Basso	- Manutenzione continua e sostituzione apparecchiature non adeguate
Errore materiale	Basso	Danneggiamento parziale singolo record	Basso	Addestramento del personale
Asportazione e/o furto di strumenti contenenti dati	Basso	-	Basso	Sorveglianza dei locali operativi
Guasti agli impianti elettrici	Basso	Danneggiamento parziale Archivi	Basso	Manutenzione impianti elettrici

8.1.4.4) - Banche dati trattati

Banca Dati	Trattamento	Finalità	Dati Sensibili e Giudiziari	Trattamento Interno	Trattamento Esterno
Dati anagrafici e di residenza	Cartaceo Informatico	Attività di controllo e ispettive. Attività sanzionatorie e di tutela Finalità in ambito amm.vo e sociale Art 201 CdS	-	Registrazione Conservazione Elaborazione Organizzazione Modificazione Consultazione	Comunicazione Art 201 CdS
Archivio soggetti destinatari di atti amm.vi relativi a seguito di violazioni varie	Cartaceo	Attività di controllo e ispettive. Attività sanzionatorie e di tutela C.P.P. C.d. S. T.U.L.P.S.	Sensibili Giudiziari	Registrazione Conservazione	Comunicazione C.P.P. C.P.
Comunicazione di cittadini extracomunitari assunti da ditte residenti nel territorio comunale	Cartaceo	Cittadinanza, immigrazione e condizione dello straniero Attività di controllo e ispettive. Attività sanzionatorie e di tutela D.lgs 50/48 D.lgs 286/98	Sensibili	Organizzazione Conservazione Selezione	Comunicazione D.lgs 50/48 D.lgs 286/98
Registro notifiche	Cartaceo	Funzioni istituzionali	Sensibili Giudiziari	Registrazione Conservazione Consultazione Utilizzo	Comunicazione Funzioni istituzionali
Agenzie d'affari, sostanze zuccherine, facchini, mestieri girovaghi, portieri custodi	Cartaceo	Attività istituzionali DPR 311/2001	Giudiziari	Conservazione	-
Attività di pianificazione, attività artigianali	Cartaceo	Attività istituzionali DPR 327/80 L. 1002/56	-	Registrazione Conservazone	Comunicazione DPR 327/80
Attività commerciali relative a edicole e rivendite di giornali	Cartaceo	Attività istituzionali L. 416/91 D.lgs 170/01 DGR 183/02	Giudiziari	Conservazione	-

Attività commerciali di barbiere,parrucchiere ed estetista	Cartaceo	Attività istituzionali L. 1/90 Lr 12/93	-	Conservazione Modificazione	Comunicazione
Pratiche rilascio licenze noleggio trasporti con/senza conducente	Cartaceo	Attività istituzionali DPR 480/01 L. 278/03	Giudiziari	Registrazione Conservazione	Comunicazionw DPR 480/01
Produttori vitivinicoli	Cartaceo	Attività istituzionali	-	Conservazione	Comunicazione
Commercio in sede fissa,su aree pubbliche Esercizi di somministrazione alimenti e bevande	Cartaceo Informatico	Attività istituzionali D.lgs 114/98 LR 12/99 LP 14/99 DPR 616/77 RD 773/31 DPR 311/01 LR 14/03	Giudiziari	Registrazione Conservazione	Comunicazione L. 310/93
Manifestazioni locali,sagre,fiere	Cartaceo Informatico	Attività istituzionali TULPS LR 12/00	Giudiziari	Conservazione Consultazione	Comunicazione TULPS LR 12/00
Pratiche rilascio autorizzazioni per attività produttive	Cartaceo Informatico	Attività istituzionali D.lgs 114/98 LR 14/99 DPR 447/98 LR 14/03	Giudiziari	Registrazione Conservazione	Comunicazione D.lgs 114/98 LR 14/99 DPR 447/98 LR 14/03
Ascensori e montacarichi	Cartaceo Informatico	Finalità in ambito amm.vo e sociale DPR 162/99	-	Registrazione Conservazione	Comunicazione DPR 162/99
Trattamento sanitario Obbligatorio	Cartaceo	Finalità in ambito amm.vo e sociale L. 833/78	Sensibili	Registrazione Conservazione Utilizzo Organizzazione Elaborazione	Comunicazione L. 833/78

8.1.5) - Settore Cultura - Politiche Giovanili - Pubblica Istruzione - Sport - Servizi alla persona Sociali e Sanitari

8.1.5.1) Composizione

Il settore è diretto dal Capo Settore Dott.ssa Mastrangelo Silvia ed e' così composto:

Funzionario	Funzione	Responsabilità ex D.Lgs 196/03
Mastrangelo Silvia	Capo settore	Responsabile
Bergami Francesca	Istruttore Amministrativo	Incaricato
Carletti Irene	CO.CO.CO.	Incaricato
Brescanzin Antonio	Volontario AUSER	Incaricato
Bonazzi Stefania	Istruttore Amministrativo	Incaricato
Romani Paola	Istruttore Amministrativo a tempo determinato (lav. somministrato)	Incaricato
Mazzoni Beatrice	Istruttore Amministrativo	Incaricato
Panigalli Stefano	Istruttore Amministrativo a tempo determinato (lav. somministrato)	Incaricato
Petazzoni Morena	Esecutore Amministrativo	Incaricato

8.1.5.2) - Dotazione Hardware

Il comparto e' dotato di:

a) - 9 Unità di elaborazione elettronica
b) - 4 Unità ad armadio non motorizzato
c) - 2 Connessioni telefoniche ISDN

Il servizio cultura-politiche giovanili e' dotato di una propria rete locale. I clients sono interconnessi attraverso appositi hubs.
Le unità di elaborazione elettronica sono normalmente presidiate da personale addetto. Accedono alla rete LAN attraverso "autenticazione informatica", con "credenziali di autenticazione e relativa "parola chiave per ogni addetto. Esiste infine un "profilo di autorizzazione" che consente ai componenti di accedere a un singolo segmento dedicato del sistema di memorizzazione di massa centrale.
Anche le unità di elaborazione individuali sono dotate individualmente di accesso attraverso autenticazione informatica, con "credenziali di autenticazione e relativa "parola chiave per ogni addetto. Le unità sono dotate di un proprio "profilo di autorizzazione" relativo ad ogni operatore del comparto. Le unità in questione sono dotate di antivirus locale

Unità ad armadio non motorizzato
Come per le unità motorizzate, sono fornite di serratura a chiave e sono in vista del personale addetto.

Connessioni telefoniche

Il servizio cultura-politiche giovanili e' dotato di due connessioni telefoniche ISDN che consentono di accedere a:

- Rete Pro.Fe.Ta
- Internet

Attraverso due distinti routers.

Entrambe le connessioni non sono protette contro eventuali intrusioni ma e' allo studio una soluzione di interconnessione con la sede municipale. In tal caso le protezioni presenti presso tale ultima sede agiranno anche sulla rete in uso presso la struttura.

8.1.5.3) - Analisi dei rischi nel comparto

Tipo di Rischio	Livello Di rischio generalizzato	Impatto sui dati	Livello Locale	Azioni di contrasto
Furto di Credenziali di autenticazione	Basso	Danneggiamento parziale Archivi	Basso	Formazione agli operatori rispetto alle attenzioni da prestare all'inserimento delle credenziali
Spamming	Alto	Nessuno	-	- Antispamm su Firewall
Azione di Virus	Alto	Indiretto- Difficoltà di accesso	Basso	- Antivirus generale su accesso Internet - Antivirus Locale
Malfunzionamento o degrado strumenti informatici	Basso	Danneggiamento parziale Archivi	Basso	- Manutenzione continua e sostituzione apparecchiature non adeguate
Errore materiale	Basso	Danneggiamento parziale singolo record	Basso	Addestramento del personale
Asportazione e/o furto di strumenti contenenti dati	Basso	-	Basso	Sorveglianza dei locali operativi
Guasti agli impianti elettrici	Basso	Danneggiamento parziale Archivi	Basso	Manutenzione impianti elettrici

8.1.5.4) - Banche dati trattati

Banca Dati	Trattamento	Finalità	Dati Sensibili e Giudiziari	Trattamento Interno	Trattamento Esterno
Archivio richiedenti assegno di maternità, nucleo familiare e secondo figlio, contributi a giovani coppie	Cartaceo Informatico	Benefici economici e abilitazioni L. 448/98 L. 326/03 Regolamanto Comunale	-	Registrazione Conservazione Elaborazione Organizzazione Utilizzo	Comunicazione L. 448/98 L. 326/03
Richiedenti contributi Fondo Sociale Affitto	Cartaceo Informatico	Benefici economici e abilitazioni L.R. 24/01	-	Registrazione Conservazione Elaborazione Utilizzo Organizzazione	Comunicazione L.R. 24/01
Richiedenti e assegnatari edilizia residenziale pubblica	Cartaceo Informatico	Finalità in ambito amm.vo e sociale L.R. 24/01	-	Registrazione Conservazione Organizzazione Elaborazione Utilizzo	Comunicazione Diffusione Regolamento assegnazione alloggi E.R.P.
Richiedenti indennità di accompagnamento	Cartaceo Informatico	Benefici economici e abilitazioni L. 388/00	Sensibili	Registrazione Conservazione Organizzazione Elaborazione Utilizzo	Comunicazione L. 388/00
Utenti Casa Protetta	Cartaceo Informatico	Finalità in ambito amm.vo e sociale Regolamento comunale	-	Registrazione Conservazione Organizzazione Utilizzo	Comunicazione Convenzione con ASL per rimborso oneri sanitari
Piani assistenziali e verifiche ospiti casa protetta	Cartaceo Informatico	Finalità in ambito amm.vo e sociale Direttiva Reg. 1378/99	Sensibili	Registrazione Conservazione Utilizzo	Comunicazione Dir. Reg 1378/99
Partecipanti vacanze anziani	Cartaceo Informatico	Finalità in ambito amm.vo e sociale	-	Registrazione Conservazione Utilizzo Organizzazione Elaborazione	Comunicazione
Appaltatori servizi sociali vari	Cartaceo	Finalità in ambito amm.vo e sociale L. 726/82 L. 410/91	Giudiziari	Registrazione Conservazione Utilizzo Organizzazione	Comunicazione L. 726/82 L. 410/91
Pratiche per il rilascio di autorizzazioni sanitarie e pareri igienico-sanitari	Cartaceo	Attività istituzionali L. 327/80	-	Registrazione Conservazione	Comunicazione

Erogazione contributi ad enti ed associazioni onlus ed a persone bisognose	Cartaceo Informatico	Benefici economici e abilitazioni Regolamento comunale	-	Registrazione Conservazione Organizzazione Utilizzo	Comunicazione Regolamento comunale
Volontari servizio civile	Cartaceo Informatico	Volontariato e obiezione di coscienza L. 230/98	Sensibili	Registrazione Conservazione Utilizzo Organizzazione Consultazione Selezione	Comunicazione L. 230/98
Contrassegni per invalidi	Cartaceo	Finalità in ambito amm.vo e sociale Art. 188 C.D.S.	Sensibili	Registrazione Conservazione Organizzazione	-
Richiedenti borse di studio	Cartaceo	Benefici economici e abilitazioni L. 26/01	-	Registrazione Conservazione Utilizzo Elaborazione	-
Richiedenti fornitura libri di testo	Cartaceo	Benefici economici e abilitazioni L. 448/98	-	Registrazione Conservazione Consultazione Utilizzo Elaborazione Selezione	-
Alunni fruitori trasporto scolastico	Cartaceo Informatico	Finalità in ambito amm.vo e sociale	-	Registrazione Conservazione Utilizzo Selezione Consultazione	Comunicazione
Alunni fruitori mensa scolastica	Cartaceo Informatico	Finalità in ambito amm.vo e sociale	Sensibili	Registrazione Consultazione Utilizzo Selezione Consultazione	Comunicazione
Utenti palestre ed impianti sportivi	Cartaceo Informatico	Finalità in ambito amm.vo e sociale	-	Registrazione Conservazione Utilizzo Organizzazione Elaborazione Selezione	Comunicazione
Associazioni sportive	Cartaceo	Finalità in ambito amm.vo e sociale	-	Conservazione Utilizzo	-
Associazioni Culturali e ricreative	Cartaceo Informatico	Finalità in ambito amm.vo e sociale	-	Registrazione Conservazione Utilizzo	-
Utenti Biblioteca e servizio biblionet	Cartaceo Informatico	Finalità in ambito amm.vo e sociale	-	Registrazione Conservazione Utilizzo	-
Associazioni assegnatarie di locali di proprietà comunale	Cartaceo Informatico	Funzioni istituzionali	Sensibili	Registrazione Conservazione Organizzazione Utilizzo	-

Erogazione contributi ad enti ed associazioni ultrali,ricreative,sportive, pro-loco	Cartaceo Informatico	Benefici economici e abilitazioni Regolamento comunale	-	Registrazione Conservazione Organizzazione Utilizzo	Comunicazione Regolamento comunale

9 - Formazione

Formazione continua degli incaricati del trattamento per renderli edotti dei rischi che incombono sui dati , delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare.
Distribuzione di un manualetto operativo contenente il riferimento ai modelli comportamentali da adottare in riferimento agli aspetti legati al trattamento di dati personali e sensibili con e senza apparecchiature elettroniche.
L'attività di formazione continua viene completata da una serie di "incontri" con i vari servizi onde chiarire eventuali particolarità. Tali incontri saranno opportunamente calendarizzati nel corso dell'anno.
Per ciò che attiene a nuovo personale assunto in servizio o in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali, verranno adottate misure informative specifiche.

10 - AMMINISTRATORE DI SISTEMA

10.1 Requisiti,nomina,compiti e verifica dell'attività

Per Amministratore di Sistema si intende la figura professionale finalizzata alla gestione ed alla manutenzione di un impianto di elaborazione o di sue componenti, nonché la figura ad essa equiparabile dal punto di vista dei rischi relativi alla protezione dei dati; nell'ambito dell'ente è il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo degli elaboratori della rete e di consentirne l'utilizzazione.

L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità ed affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

L'Amministratore di Sistema del COMUNE DI VIGARANO MAINARDA è individuato e nominato con apposito provvedimento del Sindaco.

E' compito dell'Amministratore di sistema:

- individuare 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 il Comune abbia adottato le misure minime di sicurezza per il trattamento dei dati personali, 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 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 (*oppure* semestrale *se si trattano 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;
- predisporre ed aggiornare, entro il 31 marzo di ogni anno, il 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 nell'ente.

Ai fini della verifica della propria attività da parte del titolare del trattamento, l'amministratore di sistema dovrà presentare al medesimo, entro il 30 marzo di ogni anno, apposita relazione sull'attività svolta durante l'anno precedente per attuare i compiti a lui affidati con l'atto di nomina e previsti dal presente Documento Programmatico Sulla Sicurezza, nonché sulla rispondenza della sua attività alle misure organizzative,tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle vigenti normative in materia.

11 - MISURE DI SICUREZZA DI TIPO LOGICO ADOTTATE

11.1 Tipologia di misure di sicurezza di tipo logico adotatte

Rientrano in tale categoria:

Misure per l'indicazione dei codici identificativi e delle parole chiave agli incaricati.
Agli incaricati sono assegnate le credenziali di autenticazione consistenti in un codice per l'identificazione, che neppure in futuro potrà essere associato ad altre persone, unito a una parola chiave riservata conosciuta solamente dall'incaricato.
La parola chiave è composta da otto caratteri; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi.
In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
Agli incaricati sono impartite le istruzioni necessarie per:

- assicurare la segretezza della componente riservata della credenziale
- custodire in modo diligente i dispositivi in possesso ed uso esclusivo dell'incaricato
- non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento
- cambiare autonomamente la componente riservata della credenziale

Misure per l'assegnazione ed autorizzazione degli elaboratori su cui effettuare i trattamenti.
Al fine di limitare l'accesso ai soli dati effettivamente necessari per effettuare le operazioni di trattamento, ad ogni incaricato è stato assegnato un profilo di autorizzazione tramite il quale potrà accedere agli archivi in formato elettronico su cui operare i trattamenti.

Misure per la protezione da accessi accidentali ad informazioni riservate.
Ad ogni incaricato sono assegnate le credenziali per l'autenticazione che consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo.
Sono impartite agli incaricati le istruzioni per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

La parola chiave è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

Misure di protezione da possibili danneggiamenti alle informazioni.
Al fine di rilevare immediatamente la presenza di codice maligno in un file, tutti gli elaboratori e i server sono dotati di programma antivirus che viene aggiornato automaticamente ogni giorno. L'Amministratore di Sistema periodicamente verifica che l'aggiornamento automatico avvenga regolarmente.

Misure per la registrazione degli "access log" dell'amministratore di sistema

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte dell' amministratore di sistema. Le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Per *access log* si intende la registrazione degli eventi generati dal sistema di autenticazione informatica all'atto dell'accesso o tentativo di accesso da parte di un amministratore di sistema o all'atto della sua disconnessione nell'ambito di collegamenti interattivi a sistemi di elaborazione o a sistemi *software*.

Gli *event records* generati dai sistemi di autenticazione contengono usualmente i riferimenti allo "username" utilizzato, alla data e all'ora dell'evento (*timestamp*), una descrizione dell'evento (sistema di elaborazione o *software* utilizzato, se si tratti di un evento di *log-in*, di *log-out*, o di una condizione di errore, quale linea di comunicazione o dispositivo terminale sia stato utilizzato...).

Sia i *server* che i *client*, intesi come "postazioni di lavoro informatizzate", sono compresi tra i sistemi per cui devono essere registrati gli accessi dell' Amministratore di sistema

Nei casi più semplici tale requisito può essere soddisfatto tramite funzionalità già disponibili nei più diffusi sistemi operativi, senza richiedere necessariamente l'uso di strumenti *software* o *hardware* aggiuntivi. Per esempio, la registrazione locale dei dati di accesso su una postazione, in determinati contesti, può essere ritenuta idonea al corretto adempimento qualora goda di sufficienti garanzie di integrità.

Sarà comunque con valutazione del titolare che dovrà essere considerata l'idoneità degli strumenti disponibili oppure l'adozione di strumenti più sofisticati, quali la raccolta dei *log* centralizzata e l'utilizzo di dispositivi non riscrivibili o di tecniche crittografiche per la verifica dell'integrità delle registrazioni.

Qualora il sistema di *log* adottato generi una raccolta dati più ampia, comunque non in contrasto con le disposizioni del codice e con i principi della protezione dei dati personali, il requisito del provvedimento del garante è certamente soddisfatto. Comunque è sempre possibile effettuare un'estrazione o un filtraggio dei *logfiles* al fine di selezionare i soli dati pertinenti agli AdS.

La caratteristica di completezza del log è riferita all'insieme degli eventi censiti nel sistema di *log*, che deve comprendere tutti gli eventi di accesso interattivo che interessino gli amministratori di sistema su tutti i sistemi di elaborazione con cui vengono trattati, anche indirettamente, dati personali. L'analisi dei rischi aiuta a valutare l'adeguatezza delle misure di sicurezza in genere, e anche delle misure tecniche per garantire attendibilità ai *log* qui richiesti.

Non è richiesta in alcun modo la registrazione di dati sull'attività interattiva (comandi impartiti, transazioni effettuate) degli amministratori di sistema.

La raccolta dei *log* serve per verificare anomalie nella frequenza degli accessi e nelle loro modalità (orari, durata, sistemi cui si è fatto accesso...). L'analisi dei *log* può essere compresa tra i criteri di valutazione dell'operato degli amministratori di sistema.

Misure di protezione da eventuali perdite di disponibilità dei dati.
L'integrità dei dati è garantita mediante idonee procedure di salvataggio periodico (backup). Detto salvataggio viene effettuato giornalmente in modalità automatica dal sistema e anche settimanalmente dagli operatori designati mediante backup su diverso supporto di registrazione.

Aggiornamento dei programmi software che trattano i dati personali.
Gli aggiornamenti periodici dei programmi per elaboratore, volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti, sono effettuati con cadenza almeno semestrale.

Rif. covi-p120522a1-ls-disaster recovery

Ferrara , 01/06/2012

COMUNE DI VIGARANO MAINARDA

Studio di Fattibilità per

"Disaster Recovery Planning"
Esempio di approccio metodologico al problema

Garantisco personale impegno affinché la soluzione proposta soddisfi i vantaggi di seguito descritti.

SOMMARIO

1. Introduzione

Gent.mo **Sindaco Dott.ssa Paron Barbara,**

scopo del presente documento è quello di illustrare al **Comune di Vigarano** la soluzione progettuale proposta da ESTECOM S.r.l. per la realizzazione di una soluzione di "Disaster Recovery" degli applicativi critici, basata su virtualizzazione dei sistemi operativi.

Per Disaster Recovery intendiamo tutte le misure tecnologiche e organizzative volte a ripristinare sistemi, dati e infrastrutture (se richiesto) necessarie all'erogazione di servizi di business a fronte di gravi emergenze. Si stima che la maggior parte delle grandi imprese spendano fra il 2% ed il 4% del proprio budget IT nella pianificazione della gestione dei disaster recovery, allo scopo di evitare impatti devastanti sui dati e la possibilità di continuare il ciclo produttivo. Fonti autorevoli stimano che delle imprese che hanno subito, a seguito di "disastri", pesanti perdite di dati, circa il 43% non hanno più ripreso l'attività, il 51% ha chiuso entro due anni e solo il 6% è riuscita a sopravvivere nel lungo termine. I disastri informatici con ingenti perdite di dati nella maggioranza dei casi provocano il fallimento dell'impresa o dell'organizzazione, ragion per cui investire in opportune strategie di recupero diventa una scelta quasi obbligatoria.

L'intero progetto è stato sviluppato con la precisa finalità di fornire al Cliente i seguenti VANTAGGI:

1. Indirizzamento verso efficienti piani di Disaster Recovery
2. Pieno rispetto delle direttive guida del "CAD" Codice dell'Amministrazione Digitale

Atto a produrre i seguenti BENEFICI:

1. Tempi di RTO (Recovery Time Objective) sempre più tendenti allo "0"
2. Tempi di RPO (Recovery Point Objective) sempre più prossimi allo "0"
3. Garanzie sulla consistenza dei processi di replica

2. Relazione

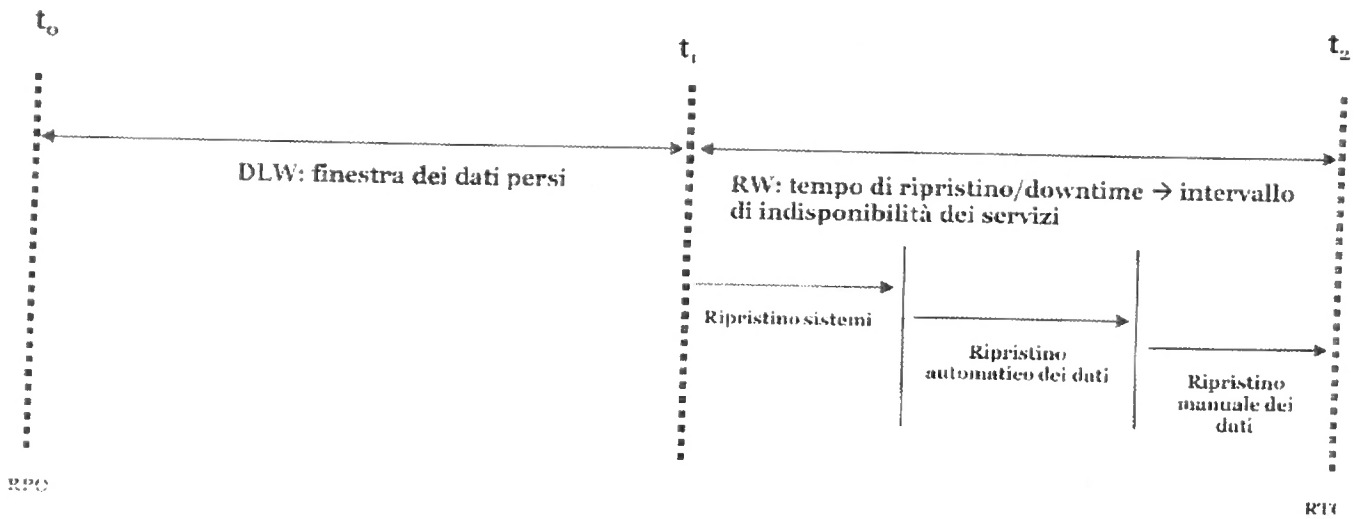
Definizioni e requisiti - Generalità

Nella realtà quotidiana, tutte le organizzazioni e perfino l'utente di casa dovrebbero predisporre un proprio piano di ripristino in caso di disastro. E' fin troppo ovvio che tale piano sarà commisurato alle caratteristiche stesse dell'azienda (dimensioni, tipo di attività, rilevanza sul mercato, criticità delle informazioni trattate e altri fattori che verranno analizzati successivamente). Tuttavia qualche precisazione è necessaria. I termini "Business Continuity" e "Disaster Recovery" fanno parte del "dominio dell'emergenza" e sono spesso erroneamente usati come sinonimi. La "Business Continuity" ha come obbiettivo quello di evitare l'interruzione del business in generale e prende quindi in considerazione tutti i servizi ed i processi aziendali. Il Disaster Recovery invece tiene conto solo di eventi disastrosi, che si possono definire "estremi" (quegli eventi cioè a scarsa probabilità di accadimento, ma ad alto impatto sul business) e che sono in grado di provocare un danno di rilevante entità sulla continuità operativa dei servizi IT. In poche parole il Disaster Recovery si colloca all'interno della Business Continuity e considera solo l'IT ovvero l'insieme del sistema informatico e di tutte le risorse ad esso relative (le persone che lo gestiscono, l'organizzazione, le politiche e le procedure correlate, i siti ove è collocato).
Si potrebbe quasi dire che obbiettivo ultimo di un progetto di Business Continuity sia la definizione di un Disaster Recovery, che dunque rappresenta l'insieme di quegli adempimenti di tipo fisico, logico, organizzativo, amministrativo, logistico e legale, atti a fronteggiare un evento a carattere catastrofico, che renda indisponibili le risorse deputate alle operazioni di elaborazione dei dati. Il Disaster Recovery è in sostanza un "processo" che consente di ripristinare il normale o indispensabile funzionamento dell'operatività aziendale e il trattamento dei dati precedentemente interrotti da un evento indesiderato di natura eccezionale e cioè da quello che può definirsi quale vero e proprio "disastro" in un sistema informatico automatizzato.

Obiettivi generici di progetto

I progetti per l'implementazione di un processo di Disaster Recovery sono spesso caratterizzati dalla loro capacità di raggiungere tre obiettivi: il punto di ripristino, il tempo di ripristino ed il budget.

La figura seguente può aiutare ad illustrare questi concetti



- T1 rappresenta l'ora dell'evento disastroso.

- T0 è il tempo al quale i dati salvati possono ritenersi certamente validi. T0 è il punto di ripristino e rappresenta lo stato in cui i dati regrediscono dopo il ripristino (es. ripristino dall'ultimo backup). L'intervallo DLW (Data Loss Window) tra T0 e T1 identifica il periodo in cui i dati prodotti dal sistema informativo non sono recuperabili ovvero la quantità di dati persi. (es. intervallo di tempo tra il momento dell'evento disastroso e l'ultimo backup valido usabile per il ripristino).
- T2 è l'ora di completo ripristino dei dati. T2 rappresenta il momento in cui i dati vengono ripristinati nello stato in cui si trovavano al momento del disastro T1 (es. ripristino dall'ultimo backup + caricamento manuale)
- RW (Recovery Windows) è il tempo necessario per il pieno ripristino del sistema informativo.
- RPO (Recovery Point Objective) corrisponde alla dimensione della finestra di tempo DLW e rappresenta l'obiettivo del progetto di recovery. Minore il valore e migliore è il risultato.
- RTO (Recovery Time Objective) coincide con il tempo di fermo dei sistemi e quindi di indisponibilità dei servizi applicativi. E' uno degli obiettivi di progetto; minore il valore e migliore è il risultato.

Livelli di servizio del Disaster Recovery - Tipologie di soluzioni tecniche -

Le soluzioni di DR sono spesso descritte in termini di livello di servizio. Questi livelli di servizio furono inizialmente introdotti nel 1993 dal Technical Steering Committee di SHARE (www.share.org) e variano dal livello 0, che non prevede alcuna soluzione di DR, al livello 6 che implementa una soluzione integrata hardware e software per raggiungere l'obiettivo "zero perdita dati" e ripartenza immediata.
Uno degli obiettivi che si prefigge il Codice dell'Amministrazione Digitale è quello di giungere ad un'omogeneizzazione delle soluzioni di continuità operativa e disaster recovery.
A tal fine si è proceduto ad individuare delle soluzioni, indicate convenzionalmente come Tier 1, Tier 2, ..., Tier 6; ciascuna classe di criticità dovrebbe condurre all'individuazione almeno dei tier che come ipotizzato nello schema di seguito riportato, si ritiene siano quelli più adatti; resta ferma la discrezionalità dell'Amministrazione di decidere eventualmente soluzioni, modalità di backup e ripristino più elevate di quelle minimali individuate per la classe di criticità ed indicate in via esemplificativa nella tabella seguente (non escludendo quindi ad es. la possibilità di adottare, per servizi con classe di criticità bassa o media, modalità di backup e soluzioni tipiche di una classe di criticità più elevata; ovvero non eliminando, la possibilità, per casi riconducibili a soluzioni tier 1 e 2, di adottare modalità di back up "via rete").

		Classe di criticità			
		Bassa	Media	Alta	Critica
Soluzioni	Tier 1				
	Tier 2				
	Tier 3				
	Tier 4				
	Tier 5				
	Tier 6				

Come si vede nello schema, in alcune fasce coesistono diverse soluzioni, la scelta delle quali dipende da ulteriori fattori legati al contesto organizzativo e/o tecnologico nonché finanziario di riferimento. Ove ad esempio il profilo finanziario comporti un ostacolo all'adozione della soluzione più adeguata alla classe di rischio individuata al termine del percorso, imponendo ad es. la scelta di una soluzione tier 4 per una classe "critica", l'Amministrazione, dovrà dare evidenza delle motivazioni e dei vincoli che determinano la scelta adottata e dei tempi stimati per realizzare invece le soluzioni che sarebbero più confacenti alla classe di rischio individuata.

È necessario comunque sottolineare che, indipendentemente dal tipo di soluzione che la singola amministrazione intende adottare, essa deve sempre assicurare la conformità con quanto previsto dal D. Lgs. 196/03 ("Testo unico in materia di protezione dei dati personali") e s.m.i . relativamente alle misure tecniche ed organizzative da adottare per la protezione dei dati personali trattati dall'Amministrazione.
Le tipologie di soluzioni tecniche elencate qui di seguito sono definite in senso generale con riguardo alle funzionalità richieste e/o da assicurare, e come tali non fanno riferimento a specifiche tecnologie e/o prodotti o soluzioni di mercato.

Tier 1: è la soluzione minimale coerente con quanto previsto dall'articolo 50-bis.Prevede il backup dei dati presso un altro sito tramite trasporto di supporto nastro. I dati sono conservati presso il sito remoto. In tale sito, deve essere prevista, la disponibilità, in caso di emergenza, sia dello storage su disco, dove riversare i dati conservati, sia di un sistema elaborativo in grado di permettere il ripristino delle funzionalità IT. Nel caso di affidamento del servizio di custodia ad un fornitore, tale disponibilità deve essere regolamentata contrattualmente.

Questi servizi aggiuntivi possono essere minimali:
- non sono previste procedure di verifica della coerenza dei dati ed esiste un'unica copia storage;
- la disponibilità dei dispositivi (storage su disco e sistemi di elaborazione) prevede tempi non brevi (anche più settimane per l'assegnazione da parte del fornitore);
- la disponibilità dei dispositivi non garantisce le performance rispetto al sistema primario;
- la disponibilità dei dispositivi è assegnata per un periodo di tempo limitato.

Poiché i dati salvati possono essere relativi all'intera immagine dello storage primario o solo ai dati delle elaborazioni, la disponibilità dei dispositivi ausiliari deve essere chiaramente definita in termini di ambiente hardware e software di riferimento.
Viene quindi assicurata la esecuzione e conservazione dei backup e che, per i casi in cui si renda necessario assicurare il ripristino, vi è un sito "vuoto" attrezzato pronto a ricevere le componenti e configurazioni necessarie, ove fosse richiesto, per far fronte all'emergenza (on demand).

Tier 2: la soluzione è simile a quella del Tier 1, con la differenza che le risorse elaborative possono essere disponibili in tempi sensibilmente più brevi (ad es. max. 3 giorni), viene garantito anche l'allineamento delle performance rispetto ai sistemi primari ed esiste la possibilità di prorogare, per un tempo limitato, la disponibilità delle risorse elaborative oltre il massimo periodo di base.
Viene assicurata la esecuzione e conservazione dei backup e la disponibilità presso il sito dei sistemi e delle configurazioni da poter utilizzare per i casi in cui si renda necessario assicurare ilripristino.

Tier 3: la soluzione è simile a quella di Tier 2 con la differenza che il trasferimento dei dati dal sito primario e quello di DR avviene attraverso un collegamento di rete tra i due siti. Questa soluzione, che permette tempi di ripristino più veloci, rende necessario dotarsi di collegamenti di rete con adeguati parametri di disponibilità, velocità di trasferimento e sicurezza (sia della linea sia delle caratteristiche dipendenti dalla quantità di dati da trasportare).

Tier 4: la soluzione prevede che le risorse elaborative, garantite coerenti con quelle del centro primario, siano sempre disponibili, permettendo la ripartenza delle funzionalità in tempi rapidi (ad es.2-4 ore).
Le altre caratteristiche sono quelle del Tier 3, con la possibilità, però, di un prolungamento della disponibilità delle risorse elaborative più lungo (almeno fino a 6 mesi) e con l'aggiornamento dei dati (RPO) con frequenza molto alta (ad es. max 5 minuti), ma non bloccante per le attività transazionali del centro primario (aggiornamento asincrono).

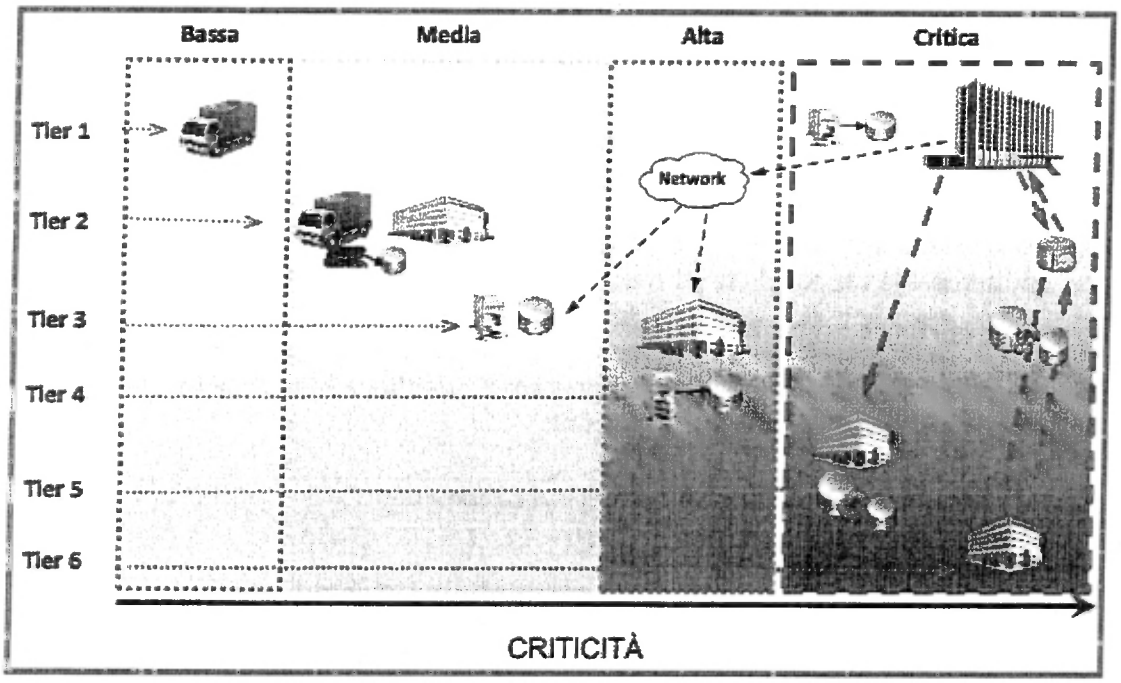
Tier 5: la soluzione è analoga a quella del Tier4, con la differenza che l'aggiornamento finale dei dati avviene solo quando entrambi i siti hanno eseguito e completato i rispettivi aggiornamenti. Allo stato attuale della tecnologia

questa soluzione, non può prescindere dalle caratteristiche della connettività sia in termini di distanza che di latenza; ne consegue che tale modalità (sincronizzazione), nonché l'eventuale bilanciamento geografico del carico di lavoro, non è possibile al di sopra di certe distanze fisiche fra sito primario e secondario.

Tier 6: la soluzione prevede che nel sito di DR le risorse elaborative, oltre ad essere sempre attive, siano funzionalmente speculari a quelle del sito primario, rendendo così possibile ripristinare l'operatività dell'IT in tempi molto rapidi (max 1 ora).
Le altre caratteristiche sono uguali a quelle del Tier 5, ma è previsto che l'opzione di prolungamento sia limitata solamente dalla durata contrattuale.

La figura che segue riassume quanto sopra esposto.

Linee Guida CO/DR art. 50 bis CAD



Modalità di implementazione - Generalità -

Lo studio proposto è finalizzato a definire gli aspetti tecnici (rilevazione dell'architettura attuale del sistema informativo e definizione di alcune alternative tecnologiche per l'implementazione del DR), strategici (obbiettivi e budget), organizzativi (definizione di ruoli e procedure, formazione del personale), economici (analisi dei costi) e, non ultimi, quelli legali (leggi, regolamenti, codici di condotta, raccomandazioni) di un piano di Disaster Recovery.
La metodologia generale di progetto proposta consiste di otto fasi separate; la metodologia è conforme alle direttive del DLGs 196/2003.

Fase 1 - Attività propedeutiche al progetto (Project Initiation)

Questa fase è usata per ottenere un conoscenza base dell'ambiente IT corrente e dei piani di sviluppo. Vengono definiti:

- Rifinitura degli obiettivi di progetto

- Definizione dettagliata delle attività
- Definizione del gruppo di lavoro
- Pianificazione delle attività
- Analisi preliminare dei rischi di progetto

Metodo: Incontri presso la sede del cliente, documentazione
Deliverables: DRPDR101 Obiettivi ed introduzione

Fase 2 – Analisi degli assets.

In questa fase debbono essere considerati e attentamente valutati gli "asset", ossia le componenti base del sistema informativo aziendale.
Occorre anzitutto stabilire (in ordine di priorità) quali elementi hardware e quali applicazioni software (incluse le banche-dati) siano indispensabili per l'attuazione dei processi automatizzati di trattamento dei dati. La classificazione delle applicazioni viene fatta in base a fattori che ne determinano il rispettivo peso. Tali fattori sono i seguenti: livello di criticità attribuito alle applicazioni, valutazione qualitativa e tempo massimo di indisponibilità delle stesse.
Sul piano della valutazione qualitativa, occorre effettuare una stima della possibile o probabile perdita economica dovuta al mancato utilizzo di ognuna delle applicazioni. Siffatta stima può essere rappresentata attraverso diversi livelli di danno
E' infine necessario stabilire il tempo massimo di indisponibilità e di inoperatività delle applicazioni sopportabile dall'azienda per non perdere la sua posizione sul mercato e la sua credibilità (vedi RTO).
Tuttavia l'analisi degli asset non può esaurirsi con le valutazioni pertinenti alle applicazioni. È necessario classificare anche gli elementi idonei al corretto ripristino. E ovviamente non si può prescindere né dall'esistenza di un sito alternativo ove ricoverare le infrastrutture prima che sia riattivato il sito principale né dalla analisi delle procedure di "backup" e dei relativi metodi di archiviazione.

Metodo: Workshop, raccolta documentazione esistenze, documentazione
Deliverables: DRPDR102 Architettura di sistema

Fase 3 - Analisi degli impatti (Business Impact Assessment).

In tale fase vengono evidenziati i principali rischi conseguenti a calamità naturali o ad altri eventi imprevisti di rilevante entità, che possono avere impatti estremi sulla funzionalità dell'infrastruttura I.T. e quindi sul funzionamento del business in generale. È chiaro quindi che il piano di DR deve prendere in considerazione solo alcuni tipi di minacce (quelle relative al dominio dell'emergenza), come è altrettanto ovvio che, per quel che concerne i dati personali (sensibili e giudiziari), l'analisi dei rischi fatta in tale sede si colloca all'interno della più generale analisi dei rischi prevista parte integrante del contenuto del D.P.S richiesto dal DLGs 196/2003.
Analizzate le tipologie di rischi che interessano il piano di DR si passa a svolgere una dettagliata analisi sull'impatto che tali rischi possono avere sull'azienda. Tramite tale analisi si considerano le conseguenze del disastro in relazione a determinate variabili, rappresentate dal tempo massimo di ripartenza (strettamente collegato al tempo massimo di indisponibilità delle applicazioni, come si è visto in precedenza) e dalla definizione delle priorità di ripristino (e cioè dall'individuazione dei dati e dei sistemi, che vanno ripristinati con precedenza assoluta sugli altri). Riguardo ai dati personali, la legge fissa il tempo massimo di ripristino in sette, ma naturalmente i tempi dipendono dal tipo di dati trattati e dai diritti oggetto di tutela. A questo punto si può stabilire quale sia la massima perdita tollerabile di dati e cioè quale sia il massimo rischio sostenibile, in relazione ad una certa scala di valori.

Metodo: Workshop, raccolta documentazione esistenze, documentazione

Deliverables: DRPDR103 Inventario dei sistemi critici

Fase 4 - Definizione dettagliata dei requisiti e della fattibilità

I fattori da considerare ai fini della scelta della soluzione di DR più aderente alle esigenze dell'organizzazione sono molteplici. Anzitutto va tenuta in conto la situazione iniziale dell'infrastruttura con tutti i suoi asset; è necessario poi verificare i risultati sia dell'analisi dei rischi attinenti al dominio dell'emergenza sia della B.I.A.; infine c'è da valutare l'infrastruttura per il recovery (ubicazione, struttura del datacenter alternativo, risorse di rete, back-up, personale, elementi di supporto). Il tutto è finalizzato a rispondere ai seguenti quesiti fondamentali:

- se la soluzione di DR prescelta sia funzionale al ripristino;
- se consenta un ripristino solo parziale o totale (RPO);
- in quanto tempo si ottenga il ripristino e inoltre come, dove, quando e ad opera di chi (RTO); quanti e quali soggetti e infrastrutture debba interessare.

A questo punto è necessaria l'analisi dei costi, (analisi di tipo quantitativo) che si affianca alla precedente valutazione qualitativa dei danni effettuata nella fase di analisi degli asset, poiché la scelta dell'una o dell'altra soluzione di DR potrà essere più o meno economica: maggior sicurezza è sinonimo di costi alti, viceversa a costi bassi si otterrà un livello di sicurezza minore.
Occorrerà trovare un giusto equilibrio tra i costi di infrastruttura per il D.R. ("sopportabile livello di spesa") e le perdite economiche dovute all'evento disastroso ("ragionevole controllo del rischio"). Quest'ultima variabile è molto importante in quanto in essa rientrano non soltanto le perdite patrimoniali e quelle di dati critici, ma anche i costi pertinenti alla gestione del periodo post-crisi e al rischio di una pubblicità negativa per l'azienda, soprattutto nei casi in cui il disastro sia stato causato da attività umana. Per altro vanno valutati gli obblighi e le responsabilità in caso di propagazione dei danni ad un'altra organizzazione.

Metodo: Workshop, raccolta documentazione esistenze, documentazione
Deliverables: DRPDR104 Principi di base

Fase 5 – Sviluppo del piano di Disaster Recovery

La fase di progettazione del DR si articola essenzialmente in due sottofasi: un piano generale o di massima ed un piano di dettaglio.
Il piano generale deve, in primo luogo, descrivere l'architettura complessiva da realizzare (aspetti logistici), comprensiva delle componenti hardware e software. Si devono cioè individuare, oltre al sito del datacenter alternativo, i luoghi ove collocare fisicamente i singoli elementi di ripristino. In secondo luogo occorre fissare gli obbiettivi da perseguire (aspetti strategici), in relazione alle priorità stabilite nelle precedenti analisi degli asset, dei rischi e del corrispondente impatto sui dati, sui sistemi e sui beni patrimoniali. Infine bisognerà rispettare i vincoli economici (rispetto del budget stanziato dai vertici aziendali per la realizzazione del piano) e legali (v. le prescrizioni del DLGs 196/2003 e dell'All.B per il trattamento di dati personali e v. altre normative menzionate in precedenza).
Al piano di massima segue il piano di dettaglio sviluppato secondo le usuali "best practice" di gestione dei progetti informatici; in generale il piano si sviluppa in due momenti:

a) Progettazione.
a. Analisi di dettaglio delle componenti hardware e software, gap analysis
b. Definizione delle procedure di gestione del sistema con definizione di ruoli, funzioni e responsabilità (chi-deve-fare-cosa).
c. Definizione delle fasi di gestione dell'emergenza:

i. fase di contenimento
ii. attivazione del livello minimo di operatività da DR site
iii. attivazione del livello massimo di operatività da DR site
iv. valutazione dei danni
v. riacquisto dei beni danneggiati
vi. ripristino del site di produzione
vii. riattivazione dei servizi sul site di produzione

b) **Pianificazione delle attività. Vengono qui indicate le attività e il tempo necessari alla realizzazione del progetto**, i gruppi di lavoro, le conoscenze richieste per ogni singola attività, le modalità di coinvolgimento del personale.

Metodo: Workshop, documentazione piano

Deliverables: Sezione 2-3-4-5 del piano di DR (vedi allegato), DPRDR105 Gap Analysis

Fase 6 – Sviluppo del piano di test/verifica

I test in questione sono quelli relativi alla progettazione del piano, non alla simulazione del disastro. Verranno definiti test da effettuarsi periodicamente per verificare la funzionalità dei vari elementi di ripristino, delle applicazioni e delle singole unità operative, in modo da valutare l'efficienza dell'intera infrastruttura. Di siffatte verifiche si dovranno stendere precisi rapporti, secondo modalità prestabilite. Pianificazione della fase di collaudo.

Metodo: Workshop, documentazione

Deliverables: Sezione 6 del piano di DR (vedi allegato)

Fase 7 – Sviluppo del piano di manutenzione del sistema

In questa fase devono essere definite le procedure per la gestione dei cambiamenti e delle revisioni del progetto. Gli aggiornamenti sono infatti necessari e, con riguardo ai dati personali, l'art. 31 del Cod. (disposizione questa estensibile a tutti gli altri dati rilevanti per l'organizzazione) pone l'obbligo di custodire e controllare i dati "anche in relazione alle conoscenze acquisite in base al progresso tecnico". In tal modo, alla natura dei dati e alla tipologia dei trattamenti si aggiunge un altro elemento che permette di determinare quali siano le misure di sicurezza più adatte a ridurre al minimo il rischio di perdita dei dati per qualsivoglia
causa ("anche accidentale").
Il piano di gestione dei cambiamenti deve tener conto sia delle variazioni tecnologiche apportate al sistema di produzione che delle mutate esigenze aziendali ed allineare di conseguenza le conoscenze del personale con opportuni piani di formazione.

Metodo: Workshop, documentazione

Deliverables: Sezione 7 del piano di DR (vedi allegato)

Fase 8 – Implementazione iniziale e collaudo

E' la fase del piano che prevede la realizzazione delle componenti infrastrutturali (siti di backup, tecnologie di replica, ridondanza delle infrastrutture di rete, ..), organizzative (DR team) e gestionali (procedure di allineamento, monitoraggio, ...) direttamente legate al DR e non ancora implementate nel sistema informativo aziendale. La fase di implementazione è seguita dalla fase di collaudo.

Metodo: Installazione e test, documentazione

Deliverables: Sezione 6 del piano di DR (vedi allegato)

3. Indice del piano di Disaster Recovery

Il piano di Disaster Recovery include le informazioni necessarie alla migrazione dei servizi applicativi dal sito primario a quello secondario in caso di sinistro. La struttura del documento è la seguente:

Sezione 1: Informazioni generali sul piano
- DRPDR101: Obiettivi ed introduzione
- DRPDR102: Architettura di sistema
- DRPDR103: Inventario dei sistemi critici
- DRPDR104: Principi di base
- DRPDR105: Gap analysis (infrastruttura, applicazione e procedure)

Sezione 2: Operatività normale
- DRPDR201: Inizializzazione infrastruttura
- DRPDR202: Inizializzazione banche dati
- DRPDR203: Inizializzazione applicazioni
- DRPDR204: Sincronizzazione siti
- DRPDR205: Monitoraggio siti
- DRPDR206: Piano di training del personale
- DRPDR207: Simulazione periodica di ripristino
- DRPDR208: Documentazione delle attività svolte (reporting)

Sezione 3: Lancio della procedura di emergenza
- DRPDR301: Criteri di sicurezza
- DRPDR302: Comunicazioni (Lista dei contatti in caso di disastro, modalità di contatto)
- DRPDR303: Disaster recovery team (ruoli e responsabilità)
- DRPDR304: Attivazione del piano di disaster recovery
- DRPDR306: Valutazione dei danni
- DRPDR307: Procedure di acquisto in emergenza
- DRPDR308: Documentazione delle attività svolte (reporting)

Sezione 4: Lancio delle procedure di avviamento del sito secondario
- DRPDR401: Preparazione del sito di disaster recovery
- DRPDR402: Procedura di ripristino dell'infrastruttura
- DRPDR403: Procedura di ripristino della banche dati
- DRPDR404: Procedura di ripristino delle applicazioni
- DRPDR405: Procedura di ripristino delle operazioni

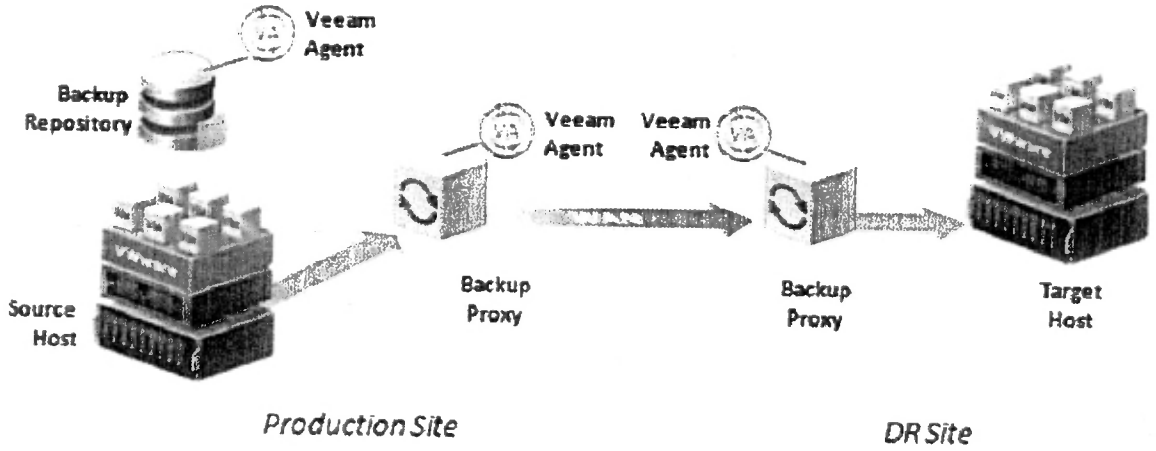
Sezione 5: Ripristino del sito di produzione
- DRPDR500: Condizioni per il ritorno al sito di produzione
- DRPDR501: Ripristino dell'infrastruttura
- DRPDR502: Ripristino della banche dati
- DRPDR503: Ripristino delle applicazioni
- DRPDR503: Ripristino delle operazioni

Sezione 6: Verifica/test del piano
- DRPDR601: Obiettivi e strategie di test
- DRPDR602: Procedure di test e verifica

Sezione 7: Manutenzione del piano
- DRPDR701: Aggiornamento del piano
- DRPDR702: Lista di riferimento dei documenti di piano

4. Lo scenario

Una volta ottimizzato il proprio sito di produzione VMware, e averlo messo in sicurezza con l'utilizzo di Veeam Backup & Replication, il passo successivo nella ricerca di una protezione di livello sempre maggiore è l'utilizzo di un sito di Disaster Recovery.



Veeam Backup & Replication prevede svariate configurazioni per ottenere questo risultato, tutte ugualmente valide; quali di queste utilizzare in un determinato scenario dipende profondamente dalle scelte progettuali che verranno prese.

Lo scopo del sito di DR

Capire in modo preciso lo scopo che ci si è prefissati dal proprio sito di Disaster Recovery influenza profondamente le configurazioni che implementeremo in Veeam Backup & Replication. Il sito di DR non è un semplice deposito remoto dei file di backup; **al contrario è in ultima analisi una replica (a volte ridotta) del nostro virtual datacenter dove dobbiamo poter avviare le nostre VM in caso di problemi al sito principale.**

Questa semplice considerazione è alla base delle scelte progettuali.

Durante le attività di replica infatti, Veeam procederà a replicare le varie Virtual Machine copiandole nello storage remoto, e contemporaneamente registrerà queste VM all'interno dei nodi ESXi remoti.

In caso di necessità, sarà sufficiente collegarsi ai nodi ESXi remoti ed accendere la virtual machine ivi registrata e già pronta all'uso.

Questa soluzione, realizzabile con le funzioni di replica di Veeam Backup & Replication, consente di ottenere i **minimi valori di RTO (Recovery Time Objective)** e **RPO (Recovery Point Objective)** già oggetto di approfondimenti della presente.

Nel sito di DR Estecom mette a disposizione più server fisici IBM ESXi in ALTA AFFIDABILITA', e un datastore IBM DS4700 di classe Enterprise.

La connettività tra sito di Produzione e DR

Solitamente, i backup di una infrastruttura VMware avvengono attraverso connessioni interne alla rete aziendale. Queste presentano velocità di almeno 1 Gbit, e permettono tutta una serie di configurazioni per ottenere il massimo risultato in termini di finestre di backup (il tempo necessario a realizzare un backup) e possibilità di ripristino.

In presenza di siti di Disaster Recovery, non sempre la connettività tra i due siti è così performante. Spesso la linea presenta velocità nell'ordine delle decine di Mbits, se non inferiori.

In uno scenario così limitato, dobbiamo mettere in atto tutte le possibili accortezze per limitare al massimo

l'impatto che la velocità di trasferimento ci impone.

Aggiornamento della connettività

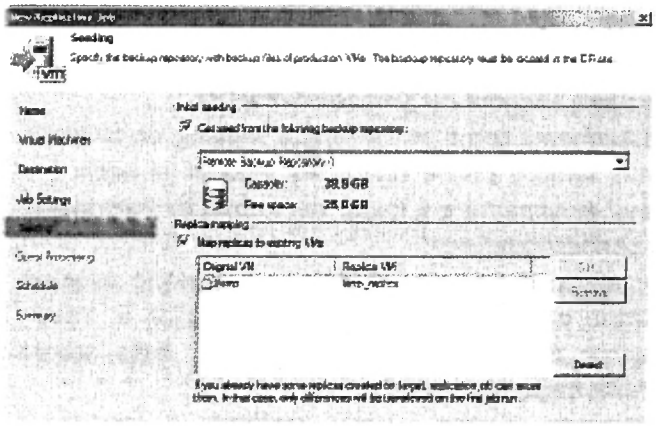
Sembra la soluzione più ovvia, eppure è la meno percorsa. Ci si imbatte in progetti molto complessi, con strutture e politiche di replica altrettanto complesse, per poi capire che si sarebbero potuti ottenere risultati migliori semplicemente aumentando, se possibile, la velocità di banda disponibile.

Il fatto che Veeam sia in grado di operare anche con connessioni a banda ridotta e alta latenza, non vuol dire che dobbiamo per forza di cose metterlo in esercizio in condizioni limite. **Valutate come prima cosa questo.**

Una domanda potrebbe sorgere spontanea: qual è una velocità sufficiente, oltre la quale posso anche smettere di aumentarla? Purtroppo non c'è una formula magica, e nemmeno un valore ottimale per tutti. A parte la banale risposta "più ne avete meglio è", la valutazione che dovete fare è basata sulla quantità di dati che viene prodotta ad ogni replica incrementale, e quanto tempo impiegherete a replicare questa mole di dati da un sito all'altro. Se il tempo risultante è inferiore al vostro RTO, allora siete a posto. In caso contrario, l'incremento della connettività sarà da considerare.

La prima replica

Qualunque siano le varie opzioni che andrete a scegliere, la prima replica consisterà in una copia integrale delle vostre Virtual Machines.



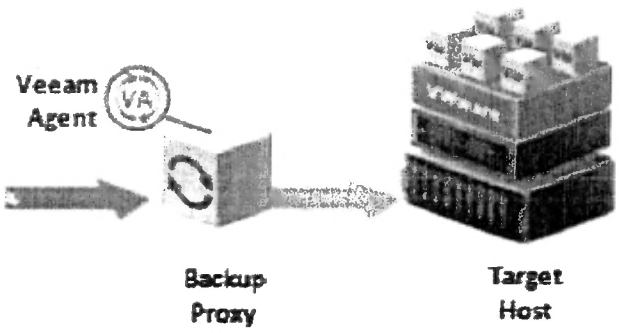
Se analizzando la mole totale di dati vi doveste accorgere che si tratta di svariati Gb, se non Tb, è probabile che la prima replica possa impiegare diversi giorni. In questo caso, una funzione sicuramente da utilizzare è la Replica Seeding.

Tramite questa funzione, potremo salvare l'intera mole di VM su un supporto removibile locale, e in seguito trasportare manualmente questo supporto presso il sito di DR. Qui, i backup verranno caricati in un "backup repository" verso il quale punteranno i job di replica. I job caricheranno inizialmente gli ultimi punti di ripristino contenuti nel seeding, ripristineranno le varie VM nei datastore remoti, e da qui una seconda attività replicherà unicamente le differenze tra il seeding e le VM presenti in produzione. Questo strumento consente di salvare letteralmente giorni di attività durante l'inizio delle repliche.

L'uso di un backup proxy dedicato

Grazie alla nuova struttura scalabile di Veeam Backup & Replication, è possibile utilizzare differenti Backup Proxies cui assegnare i vari Job che si programmano.

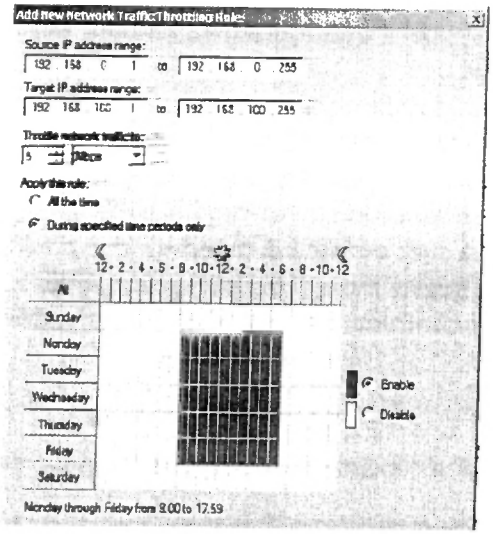
Per i processi di replica con connessioni lente è preferibile creare un backup proxy dedicato, meglio se posizionato direttamente nel sito di DR. Veeam Backup può essere installato sia su versioni Full che Core di Windows 2008 R2; una Virtual Machine Windows 2008 R2 Core costituisce un ottimo target per questo compito, garantendo un'installazione snella il cui unico ruolo sarà appunto quello di backup proxy.



In questo modo, è possibile modificare i parametri di funzionamento di questo proxy senza inficiare le performance degli altri. Agiremo in particolare su questi aspetti:

Transport Mode: sarà possibile, dovendo attraversare reti pubbliche, abilitare la cifratura del traffico in Network

Mode. Questa configurazione introduce un peggioramento delle prestazioni a fronte di una maggiore confidenzialità dei dati trasmessi. Se utilizziamo invece connessioni sicure come VPN o reti dedicate, è possibile ignorare questa scelta.



Throttling: se la rete attraverso la quale inviamo le repliche al sito di DR è condivisa con altri servizi, come ad esempio la navigazione su internet, è possibile gestire regole multiple che limitino la banda utilizzata.

E' possibile imporre limitazioni all'uso della rete in base alle subnet sorgenti o di destinazione, così come in base ai periodi del giorno e della settimana.

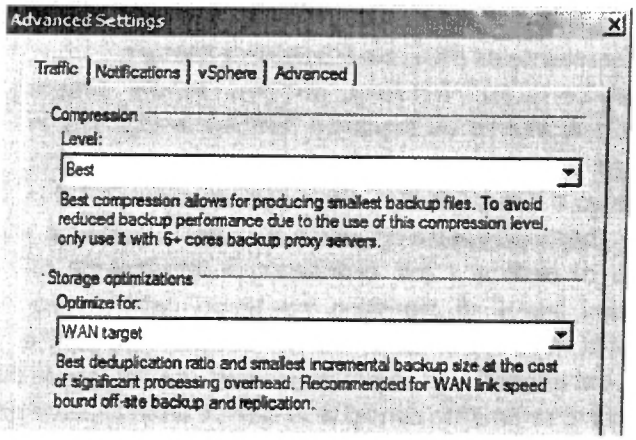
Nell'esempio riportato, stiamo limitando il nostro backup proxy ad usare non più di 5 mbits ogni giorno dal lunedì al venerdì dalle 8 alle 18, in modo che il lavoro dei dipendenti non sia danneggiato dalle repliche.

Le configurazioni dei processi di Replica

Esattamente come per la Replica Seeding, un obiettivo deve sempre essere chiaro nei processi di Replica: si deve movimentare il minor numero di dati attraverso la connessione lenta.

Per ottenere questo risultato, è necessario scegliere alcune opzioni che il processo di Replica di Veeam Backup & Replication offre, presenti nella scheda Traffic degli Advanced Settings.

Attraverso questa sezione, andremo a scegliere il livello di compressione massimo disponibile, ovvero Best. Teniamo presente che a fronte di un incremento del livello di compressione, dovremo prevedere un maggiore carico sulle CPU dei backup proxies.



Selezioneremo poi l'ottimizzazione per "WAN target", attivando di fatto il livello di deduplica maggiore, che ci consentirà quindi di trasferire il minor numero di dati possibile. Anche questo parametro potrebbe influire negativamente sul carico delle CPU.

Andare oltre: Ottimizzatori WAN

Se non abbiamo possibilità di aumentare la connettività tra i due siti, o il costo di questo aggiornamento dovesse risultare economicamente impegnativo, una possibile alternativa sono gli Ottimizzatori WAN.

Si tratta di appliance, hardware o software, alcune delle quali disponibili direttamente come virtual machines, che comprimono e ottimizzano il traffico in transito e permettono quindi di sfruttare appieno la connettività posseduta.

Ne esistono diverse, alcune delle quali hanno stretto accordi direttamente con Veeam per offrire soluzioni integrate per la replica su reti WAN.

In diversi casi il loro costo è decisamente inferiore agli upgrade di connettività, pur offrendo in ultima analisi gli stessi risultati.

5. Servizi Professionali

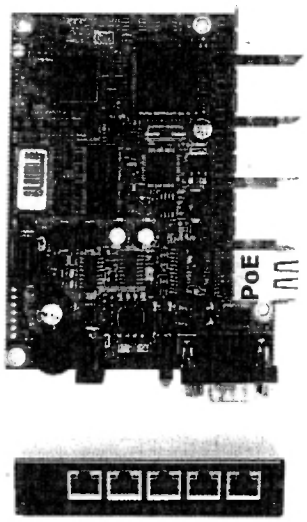
I servizi di seguito descritti verranno erogati attraverso un contratto per un minimo di 3 = (tre) anni e necessario a fornire adeguato supporto di Start up e monitoraggio della funzionalità del Disaster Recovery.
Nella fattispecie sono da intendersi come oggetto della presente tutti i servivi prettamente tecnici, progettuali, logistici, implementativi, tuning e monitoraggio della infrastruttura di Disaster Rocovery, nella fattispecie:

FASE 5 - punto a) "Progettazione"
FASE 6 - Sviluppo del piano di test e verifica
FASE 7 - Sviluppo del piano di manutenzione del sistema
FASE 8 - Implementazione iniziale e collaudo

Tutti i servizi di consulenza legale e organizzativa finalizzati alla predisposizione dei documenti previsti dall'art. 50 bis, *comma* 4 del CAD, da inviare a DigitPA per ottenere il necessario parere di conformità sono da intendersi come servizi accessori alla presente e come tali, se richiesti, quotati separatamente.
Nella fattispecie si intendono i processi citati nelle **FASI 1 / 2 / 3 / 4 / 5 (b)**

6. Hardware e Software

Hardware – Router VPN

Prodotto	Descrizione - MIKROTIK VPN
	La routerborad RB450G è un router a cinque porte ethernet Gigabit. Il dispositivo è alimentato da una veloce CPU Atheros AR7161 680MHz, e comprende anche un sensore di temperatura e controllo di tensione. La Routerboard RB450G comprende RouterOS - il sistema operativo, che trasforma questo potente hardware in un router altamente sofisticato, firewall o gestore di banda. **Informazioni Aggiuntive** Velocità Processore: 680MHz RAM: 256MB Architettura: MIPS-BE Porte Lan: 5 Gigabit: si MiniPCI: 0 Wireless Integrata: 0 USB: 0 Memory Cards: 1 Memory card: microSD Power Jack: 10-28V PoE over Datalines PoE: 10-28V Voltage Monitor: Yes

Software – Necessaria opportuna verifica

Letto,approvato e sottoscritto

IL PRESIDENTE	IL SEGRETARIO COMUNALE
F.to PARON BARBARA	F.to MUSCO ANTONINO

CERTIFICATO DI PUBBLICAZIONE

Copia della presente viene pubblicata all'Albo Pretorio del Comune per rimanervi 15 giorni consecutivi. (art. 124 D.Lgs. 267/2000 e art. 32 legge 69/2009)

Addì 22 MAR. 2013

Il Messo Comunale
F.to SITTA ROSA MARIA

Il Capo Settore Segreteria
F.to FERRANTE MARCO

Copia conforme all'originale
Addì 22 MAR. 2013

Il Capo Settore Segreteria
MARCO FERRANTE

ATTESTAZIONI

la presente deliberazione:

è stata comunicata con elenco n. 4512 del 22 MAR. 2013 contestualmente alla pubblicazione all'albo pretorio ai capigruppo consiliari ex art. 125 D.Lgs. 267/2000.

è stata ratificata con atto del consiglio comunale n. del .

ESECUTIVITÀ

la presente deliberazione è divenuta esecutiva il

decorsi 10 giorni dalla pubblicazione, (art. 134 comma 3° D.Lgs. 267/2000).

Lì, _____

Il Capo Settore Segreteria
F.to MARCO FERRANTE