



# DPS documento programmatico sicurezza dell'ente

Marzo 2010

# Indice

<b>INDICE</b>	<b>2</b>
<b>I REFERENTI</b>	<b>7</b>
Tavola 1. i referenti del Cliente	7
Tavola 2.: i referenti di AltaVia Consulting	7
<b>LA SICUREZZA: PREMESSA</b>	<b>8</b>
<b>PROTEZIONE CONTRO L'ACCESSO INDEBITO ALLE RISORSE ED APPLICAZIONE DEL D.LGS. N. 196/2003.</b>	<b>11</b>
<b>LO SCHEMA DEL PIANO DI SICUREZZA DI MARZO 2010</b>	<b>12</b>
<b>SECUREANALISYS</b>	<b>14</b>
<b>Il censimento delle banche dati dell'ente</b>	<b>14</b>
Regola 19.1 dell'Allegato B al Codice: elenco dei trattamenti di dati personali, sensibili, giudiziari.	14
Tavola 3. Elenco dei trattamenti: cessioni a terzi di dati	15
<b>Il censimento dei beni che rientrano nel piano di sicurezza</b>	<b>19</b>
Tavola 4.riepilogo delle sedi dell'ente	19
Tavola 5. Riepilogo del censimento dei beni informatici che rientrano nel piano di sicurezza dell'ente	20
<b>Analisi organizzativa dell'ente</b>	<b>23</b>
Tavola 6.riepilogo degli incaricati	25
Tavola 7.riepilogo dei profili	41
Rapporti con professionisti ed incaricati non dipendenti dell'ente	42
<b>Distribuzione dei compiti e delle responsabilità (regola 19.2 dell'Allegato B al Codice)</b>	<b>43</b>
Tavola 8.distribuzione dei compiti e delle responsabilità	44
L'accesso alle strutture fisiche dell'ente	49
Tavola 9.: assegnazione delle chiavi di accesso ai locali dell'ente	49
<b>Analisi tecnologica dei dati elettronici</b>	<b>58</b>
Lo schema generale della rete	58
Analisi ambientale	59
Casi particolari: i posti di lavoro degli asili nido e del centro famiglie	60
Analisi del sistema di cablaggio	60

Analisi dell'architettura LAN/WAN -----	60
LAN-----	60
WAN -----	61
Analisi delle vulnerabilità interne e dell'accesso ai dati -----	61
Analisi delle applicazioni: regola 19.8 dell'Allegato B al Codice -----	62
Tavola 10.riepilogativa del censimento dei software applicativi che rientrano nel piano di sicurezza dell'ente----	64
Analisi delle comunicazioni verso Internet-----	67
Analisi dei servizi pubblicati sulla rete Internet -----	67
<b>Analisi dei dati cartacei-----</b>	<b>69</b>
Analisi ambientale-----	69
Analisi delle vulnerabilità interne e dell'accesso dei dati-----	69
<b>Le criticità dei beni informatici preposti al trattamento dei dati elettronici -----</b>	<b>70</b>
Il fault tolerance-----	70
Tavola 11.: Tabella riepilogativa dei device presenti nell'ente: censimento dei beni informatici -----	71
Il disaster recovery -----	73
Tavola 12.: Tabella riepilogativa dei fattori di criticità per il servizio di disaster recovery -----	74
<b>L'analisi dei rischi a cui possono essere soggetti i dati elettronici e i dati cartacei: regola 19.3 dell'Allegato B al Codice -----</b>	<b>77</b>
Analisi dei rischi dei dati elettronici-----	77
Presentazione sintetica dei rischi a cui sono soggetti i dati elettronici trattati dal Comune di Casalecchio di Reno.78	
Tavola 13.: I rischi a cui sono soggetti i dati elettronici trattati dal Comune di Casalecchio di Reno sono di seguito riepilogati: -----	78
Analisi dei rischi dei dati cartacei-----	80
Presentazione sintetica dei rischi a cui possono essere soggetti i dati cartacei trattati dall'ente -----	80
Tavola 14.: I rischi a cui possono essere soggetti i dati cartacei trattati dall'ente possono essere così riepilogati:--	80
<b>L'analisi dei sistemi di videosorveglianza-----</b>	<b>82</b>
Tavola 15.: Tabella riepilogativa dei sistemi di videosorveglianza-----	82
Adempimenti ottemperati adottati nel regolamento interno-----	83
DOVERE DI INFORMAZIONE -----	83
MISURE DI SICUREZZA -----	83
DURATA DELL'EVENTUALE CONSERVAZIONE -----	83
<b>La definizione della politica di sicurezza dell'ente -----</b>	<b>84</b>
Chi-fa-cosa dentro-----	84
Tavola 16.: chi-fa-cosa dentro-----	84
Chi-fa-cosa fuori-----	88
Tavola 17.: chi-fa-cosa fuori-----	88

Chi, interno, fa cosa da fuori-----	89
Tavola 18.: chi, interno, fa-cosa da fuori -----	89
Chi, esterno, può fare cosa da fuori o, in casi definiti, da dentro -----	91
Tavola 19.: chi, esterno,può fare-cosa da fuori o, in casi definiti, da dentro -----	91
Rapporti con aziende esterne all'organizzazione assimilabili a titolari del trattamento: regola 19.7 dell'Allegato B al Codice -----	94

**SECURELAW----- 95**

**Securelaw: verifica degli adempimenti formali-----95**

Dati residenti su elaboratori elettronici -----	95
Tavola 20.: riepilogo adempimenti formali per dati residenti su elaboratori elettronici-----	95

**Securelaw: verifica degli adempimenti sostanziali -----97**

Adempimenti sostanziali dati elettronici -----	98
Tavola 21.: riepilogo adempimenti sostanziali per dati residenti su elaboratori elettronici-----	98

**Securelaw: verifica degli adempimenti formali-----99**

Dati residenti su archivi cartacei -----	99
Tavola 22.: riepilogo adempimenti formali per dati residenti su archivi cartacei -----	99
Adempimenti sostanziali dati cartacei -----	101
Tavola 23.: riepilogo adempimenti sostanziali per dati residenti su archivi cartacei -----	101

**Securelaw: piano formativo degli incaricati: regola 19.6 dell'Allegato B al Codice ----- 102**

Tavola 24.: piano di formazione degli utenti -----	104
--	-----

**DPS DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI: LE AZIONI 105**

**Dati residenti su supporto cartaceo ----- 105**

Analisi dei rischi-----	105
Analisi dei rischi e delle azioni intraprese per cautela relativamente al trattamento dei dati cartacei: regola 19.4 dell'Allegato B al Codice -----	105
Tavola 25.: riepilogo dei rischi e delle azioni legate al trattamento dei dati cartacei -----	105

**Dati residenti su elaboratori elettronici ----- 107**

Analisi dei rischi-----	107
Analisi dei rischi e delle azioni intraprese per cautela: regola 19.4 dell'Allegato B al Codice-----	107
Tavola 26.: analisi dei rischi e azioni intraprese per i dati residenti su supporto elettronico -----	107

**Le operazioni di salvataggio dei dati: regola 19.5 dell'Allegato B al Codice ----- 110**

Tavola 27.: riepilogo delle operazioni di salvataggio dei dati -----	110
--	-----

<b>I controlli anti-intrusione dall'esterno-----</b>	<b>111</b>
Tavola 28.: riepilogo delle operazioni di controlli anti-intrusione dall'esterno-----	111

**AZIONI INTRAPRESE PER IL FAULT TOLERANCE: REGOLA 19.5 DELL'ALLEGATO B AL CODICE----- 112**

Server Novell Netware-----	112
Server Windows Server 200X-----	113
Server Linux Red Hat Enterprise - Oracle-----	113
Switch-----	114
Firewall e Router-----	115

**PROCEDURE DA SEGUIRE IN CASO DI FAULT ----- 116**

Server-----	116
Server Novell-----	116
Server Windows 200X-----	117
Server Linx - Oracle-----	117
Server Windows 200X – SQL Server-----	118
Sistema di SAN Storage Area Network-----	118
Switch-----	118
Firewall e connessione ad Internet-----	119
Router e connessioni WAN-----	119
Linee di collegamento in fibra ottica-----	120

**AZIONI DA INTRAPRENDERE PER IL DISASTER RECOVERY ----- 121**

**PROCEDURE DA SEGUIRE PER AFFRONTARE UNA SITUAZIONE DI DISASTER RECOVERY ----- 123**

Server-----	123
Procedure da eseguire per i server di cui è presente il servizio di disaster recovery sul software di back-up dei dati	123

Tavola 29.: riepilogo procedure di disaster recovery per la sede del Municipio di Casalecchio di Reno legate ai dati  
----- 123

**Router e Wan Link ----- 125**

Tavola 30.: riepilogo procedure di disaster recovery per la sede di Casalecchio di Reno legate ai Wan Link ----- 125

**DOCUMENTI AGGIUNTIVI: DISCIPLINARE INTERNET ----- 126**

**AMMINISTRATORI DI SISTEMA ----- 127**

**RELAZIONE ALLEGATA AL BILANCIO ----- 128**

**CONCLUSIONI ----- 129**

**TERMINI E DEFINIZIONI ----- 130**

## I referenti

Riepiloghiamo ora i referenti del Cliente e di AltaVia Consulting Snc di Giuseppe Mazzoli e C. coinvolti nel progetto.

*Tavola 1. i referenti del Cliente*

Nome e Cognome	Mansione	Funzione specifica nel progetto
Andrea Ventura	Sistemi Informativi	Coordinatore
Alessandro Marchetti	Sistemi Informativi	Fornitore di informazioni
Elisa Neretti	Sistemi Informativi	Raccolta informazioni interne

*Tavola 2.: i referenti di AltaVia Consulting*

Nome e Cognome	Mansione	Funzione specifica nel progetto
Giuseppe Mazzoli	Progettista	Coordinatore

## La sicurezza: premessa

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

Da quanto esposto sopra deriva la necessità di rafforzare, in un quadro di evoluzione tecnologica, le misure di sicurezza contro i rischi di distruzione o perdita, anche accidentale, dei dati personali, di accesso non autorizzato o di uso improprio dei dati stessi. A tal fine alle precauzioni già previste nella normativa precedente (password, codici identificativi, antivirus etc.), se ne aggiungono altre come: password di non meno di otto caratteri, autenticazione informatica, sistemi di cifratura, procedure per il ripristino dei dati, ecc., nonché la tenuta di un aggiornato documento programmatico sulla sicurezza.

Nonostante sia utopistico credere che possa esistere la sicurezza assoluta, questo non esime qualsiasi titolare, responsabile o incaricato del trattamento dei dati personali a predisporre un piano di sicurezza dell'ente. Occorre però individuare, in via preliminare, quali sono i requisiti minimi di sicurezza di un sistema informativo basato su strumenti elettronici o su strumenti cartacei per poterli applicare al sistema stesso nella totalità o in parte.

L'obiettivo è quindi quello di stabilire il livello di sicurezza da raggiungere in relazione al valore del bene intangibile da proteggere (informazione) ed al rischio sostenibile, senza ridurre la possibilità di fruizione dello stesso.

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

- accesso indebito alle risorse;
- azioni dolose;
- errori operativi;
- manomissioni o furti;
- fault di servizi;
- eventi dannosi o disastrosi

offrendo al contempo garanzia di:

- autenticità e integrità delle registrazioni elettroniche

ed assicurando:

- facilità di auditing

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

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

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

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

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

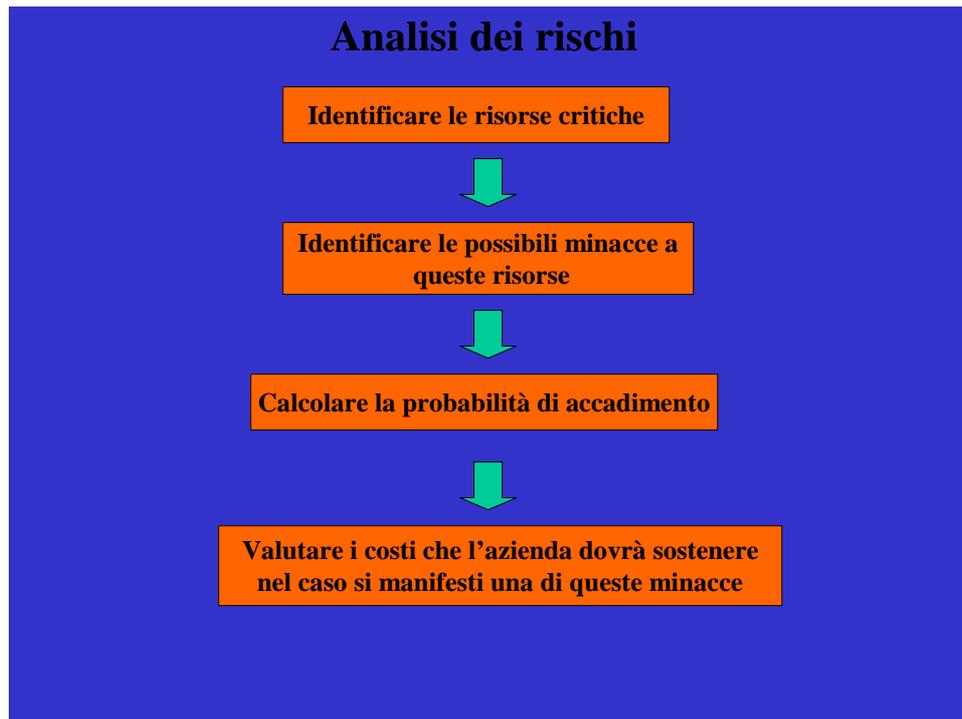
Infine per **protezione contro eventi dannosi o disastrosi** s'intende che è necessario che il sistema informativo preveda contromisure per tutelarlo da eventi dannosi (assenza di alimentazione elettrica o condizionamento) o disastrosi (incendi ecc.).

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

Per quanto riguarda i **requisiti di auditing** essi riguardano quelle caratteristiche del sistema informativo che possono facilitare le attività ispettive necessarie per assicurare il mantenimento del livello di sicurezza.

Il primo passo da fare per decidere la politica da seguire nel garantire la sicurezza di un sistema è l'analisi del rischio. L'obiettivo di tale analisi è quello di identificare le minacce alle risorse critiche del sistema per valutare le perdite derivanti dal verificarsi di tali minacce e potere eventualmente giustificare i costi da sostenere per la gestione della sicurezza.

Il processo è quindi il seguente:



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

## **Protezione contro l'accesso indebito alle risorse ed applicazione del d.lgs. n. 196/2003.**

In primo luogo è utile riassumere quali sono gli strumenti ordinari di sicurezza che gli utenti già utilizzano per accedere ai dati elettronici e/o ai dati cartacei.

Ogni utente è dotato di uno username ed una password per l'accesso alla rete dell'ente. Detto username è fisso ed è assegnato dal gruppo sistemistico del servizio sistemi informativi del Comune di Casalecchio di Reno.. La password invece è gestita dall'utente che deve forzatamente modificarla ogni 90 giorni. Il primo identificativo dell'utente permette l'accesso a tutte le risorse di rete; alcuni servizi però richiedono un ulteriore livello di identificazione quale, per esempio, l'accesso alla posta elettronica.

Ciascun application server ha poi la sua applicazione: Contabilità, Gestione del Personale, Lotus Domino Notes ecc. Gli utenti hanno, a questo punto, un ulteriore livello di autenticazione sulla procedura: uno username ed una password fissi sono assegnati all'utente a questo livello per ciascuna delle applicazioni software alle quali ha accesso.

Per ciò che concerne le misure minime di sicurezza richieste dalla nuova normativa, l'ente si è opportunamente attrezzato in base a quanto previsto dal Titolo V, Capo II del Codice in materia di protezione dei dati personali e dall'Allegato B dello stesso Codice.

In primo luogo occorre precisare che il Comune di Casalecchio di Reno tratta dati che si configurano sia come dati personali, sia come dati sensibili, e ancora dati giudiziari in base all'interpretazione letterale del d.lgs. n. 196/2003. In secondo luogo durante le sessioni formative ai dipendenti è presentato il regolamento al quale attenersi nel trattamento dei dati nello svolgimento dei compiti assegnati. Sono stati, inoltre, definiti il responsabile del trattamento dei dati, gli incaricati autorizzati a compiere specifiche operazioni e le procedure relative alla gestione dei dati stessi.

Tutti i dettagli del piano di sicurezza verranno approfonditi nei capitoli successivi.

## Lo schema del piano di sicurezza di marzo 2010

Il piano di sicurezza 2010, è un aggiornamento di quello dell'anno precedente, che aveva cercato di mettere in risalto le misure adottate dall'ente, che superano di gran lunga quelle minime previste dalla nuova normativa in materia di sicurezza dell'ente dei dati.

L'intero lavoro è denominato DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI ai sensi del d.lgs. n. 196/2003, ma si presenta come un vero e proprio PIANO DI SICUREZZA DELL'ENTE.

Il PIANO DI SICUREZZA DELL'ENTE prevede due ambiti di analisi:

- un'analisi interna articolata in otto punti denominata *secureanalysis*;
- un'analisi legislativa per accertare il rispetto dei requisiti richiesti dalla normativa attualmente in vigore denominata *securelaw*.

Prosegue poi con il Documento programmatico sulla sicurezza vero e proprio

### Secureanalysis

Gli obiettivi di questa fase, come sopra anticipato, sono nove:

1. censimento delle banche dati trattati;
2. definizione e censimento di tutti i beni che rientrano nel piano di sicurezza dell'ente;
3. analisi organizzativa dell'ente;
4. analisi tecnologica dei dati elettronici:
  - a. analisi ambientale;
  - b. analisi del sistema di cablaggio;
  - c. analisi dell'architettura LAN e WAN;
  - d. analisi delle vulnerabilità interne e dell'accesso ai dati;
  - e. analisi delle comunicazioni verso Internet;
  - f. analisi dei servizi pubblicati sulla rete Internet.
5. analisi tecnologica dei dati cartacei:
  - a. analisi ambientale;
  - b. analisi delle vulnerabilità interne e dell'accesso ai dati.
6. Definizione dei livelli di criticità dei beni informatici preposti al trattamento dei dati elettronici
7. l'analisi dei rischi a cui possono essere soggetti i dati elettronici e i dati cartacei;

8. analisi dei sistemi di videosorveglianza;
9. Definizione di una politica di sicurezza dell'ente.

### **Securelaw**

Con la fase “securelaw” si intende verificare che tutti i requisiti normativi circa il rispetto del d.lgs. n. 196/2003 denominato “Codice in materia di protezione dei dati personali” siano rispettati ed assecondati.

Per fare ciò è necessario affrontare i seguenti quattro punti:

1. verifica degli adempimenti formali;
2. verifica degli adempimenti sostanziali;
3. piano formativo degli incaricati;
4. predisposizione di un *Documento programmatico sulla sicurezza dei dati*.

Si incomincia ora con l'analisi dei singoli punti della *secureanalysis*.

# Secureanalysisys

## Il censimento delle banche dati dell'ente

In questa sezione del documento censiamo tutte le banche dati, personali e sensibili che sono oggetto di trattamento all'interno dell'ente.

***Regola 19.1 dell'Allegato B al Codice: elenco dei trattamenti di dati personali, sensibili, giudiziari.***

L'elenco completo dei trattamenti e delle banche dati è disponibile sul server Nettuno

Di seguito presentiamo l'elenco delle cessioni a terzi di dati, censito dai singoli uffici, a documentazione delle operazioni effettuate e dei potenziali rischi. Questa documentazione dimostra l'accuratezza che i responsabili mettono nelle operazioni di trattamento dei dati personali all'interno dell'ente.

Tavola 3. Elenco dei trattamenti: cessioni a terzi di dati

Progressivo	Struttura	Ente verso il quale avviene il trasferimento dei dati	Tipologia di trasmissione
1.	Servizio Affari Istituzionali	Comunicazione alla UTG – Prefettura della anagrafe degli Amministratori Comunali ed eventuali aggiornamenti legati a sostituzione o surroghe degli stessi	Elettronica
2.	Servizio Affari Istituzionali	Comunicazioni a altri Enti Pubblici (Regioni, Province, altri Comuni) di dati inerenti l'anagrafe degli amministratori Comunali	Cartacea, elettronica
3.	Servizio Affari Istituzionali	Comunicazione alla Agenzia delle entrate competente per territorio ed ad altre Amministrazioni Pubbliche richiedenti la notificazione degli atti di dati anagrafici dei destinatari della notificazione	Cartacea, elettronica
4.	Servizio Ragioneria Bilancio	Ragioneria generale dello Stato	certificazione patto di stabilità (cartaceo, elettronica)
		Regione Emilia Romagna	delibera approvazione bilancio preventivo e approvazione rendiconto – (cartaceo)
		Tesoriere Unicredit Banca	delibera approvazione bilancio, rendiconto e variazioni (cartaceo)
		Ministero dell'interno tramite Prefettura	certificazione iva trasporti preventivo/consuntivo, iva servizi esternalizzati, mutui (cartaceo)
		Lavoratori autonomi	certificazioni fiscali (cartaceo)
		Corte dei Conti giurisdizionale	Agenti contabili e consegnatari (cartaceo)
		Corte dei Conti	Certificazione consuntivo, relazioni al bilancio preventivo, questionario partecipate, relazione dal rendiconto (cartaceo)
		Revisori dei Conti	materiale inerente al bilancio, variazioni, rendiconto (cartaceo, elettronica)
		Garante editoria	certificazione spese relative alla pubblicità (elettronica)
		Presidenza Consiglio dei Ministri funzione pubblica	certificazione anagrafe delle prestazioni per società partecipate e consorzi (elettronica)
		Regione Emilia Romagna e Ministero dell'interno tramite Prefettura	certificato al bilancio preventivo e rendiconto (cartaceo, elettronica)
		Ministero delle finanze	dichiarazione Iva e IRAP (elettronica)
		Gies.	conto del patrimonio (cartaceo, elettronica)
5.	Servizio Contratti acquisti economato e patrimonio	Agenzia dell'entrate Ministero dell'Economia e delle Finanze	Anagrafe tributaria (elettronica) adempimenti connessi art. 2, comma 222 legge finanziaria 2010 elenco identificativo immobili (elettronica)
		Ministero dell'economia e delle finanze	Rilevazione prezzi per beni e servizi per P.A. (elettronica)
6.	Servizio Gestione Amministrativa del personale	INPDAP	Invio denuncia mensile analitica oneri contributivi per dipendenti – file; Invio gestione crediti – file cessioni; Documentazione TFR – cartacea; Pratiche pensioni – invio file; Modulistica per ricongiunzioni, riscatti, ecc. – cartaceo

Progressivo	Struttura	Ente verso il quale avviene il trasferimento dei dati	Tipologia di trasmissione
7.	Servizio Gestione Amministrativa del personale	AGENZIA ENTRATE	Modello 770 – file
8.	Servizio Gestione Amministrativa del personale	INPS	Invio Emens con dati contributivi personale a tempo determinato, cococo e Sindaco – compilazione on line
9.	Servizio Gestione Amministrativa del personale	SINDACATI	Invio elenco iscritti – file
10.	Servizio Gestione Amministrativa del personale	INAIL	Denuncia inizio, modifica, fine servizi per dipendenti sia ruolo che tempo determinato, cocco, infortuni sul lavoro – compilazione on line
11.	Servizio Gestione Amministrativa del personale	CENTRO IMPIEGO ZOLA PREDOSA	Denuncia inizio, modifica, fine servizi per dipendenti sia ruolo che tempo determinato, cocco – invio file
12.	Servizio Gestione Amministrativa del personale	BANCA UNICREDIT	Cedolini stipendiali – file
13.	Servizio Gestione Amministrativa del personale	DIPARTIMENTO FUNZIONE PUBBLICA	Rilevazione permessi sindacali con indicazione dei nominativi degli interessati – compilazione on line; Dati incarichi anagrafe prestazioni – compilazione on line
14.	Servizio Entrate	Ministero delle Finanze	Archivio TARSU (Provvedimento Direttore Agenzia delle Entrate 14 dicembre 2007)
15.	Servizio Entrate	Ministero dell'Economia e delle Finanze	Versamenti ICI non già trasferiti da POSTE e Agenzia delle Entrate (DM 10 dicembre 2008)
16.	Servizio Entrate	HERA spa (in qualità di gestore del servizio di N.U.)	Dati dell'archivio TARSU per aggiornamento del software di gestione della Stazione Ecologica Attrezzata (SEA)
17.	Servizio Entrate	Ministero dell'Economia e delle Finanze	Delibere di approvazione aliquote e tariffe dei tributi e dei Regolamenti di applicazione dei tributi
18.	Servizio Entrate	Equitalia Servizi e circuito Agenti della riscossione Equitalia	Tutti i dati necessari per la predisposizione e gestione informatizzata dei ruoli di riscossione volontaria e coattiva; Discarichi in versione informatizzata e/o cartacei
19.	Servizio Entrate	Engineering spa	Backup e trattamenti in sede o presso filiale o mediante FTP per amministrazione banca dati
20.	Servizio Entrate	Agenzia delle Entrate	Dati trasmessi mediante piattaforma SIATEL nell'ambito dell'accordo di partecipazione all'accertamento dei tributi erariali (DL. 203/2005)
21.	Servizio Entrate	Ministero dell'Interno	Certificazione perdita di gettito ICI per esenzione prima casa; per accatastamento immobili di categoria catastale D; per incremento di gettito conseguente all'accatastamento degli immobili ex rurali, B ed E
22.	Servizio Entrate	Corte dei Conti	Certificazione per perdita di gettito ICI conseguente a esenzione sulla prima casa; Relazioni illustrative Cartacea, elettronica
23.	Area Comunicazione e Servizi al cittadino- Servizi Demografici	Trasmissione dati variazioni anagrafiche all'AUSL (mensile)	
24.	Area Comunicazione e Servizi al cittadino- Servizi Demografici	Trasmissione deceduti all'INPS (settimanale)	Elettronica

Progressivo	Struttura		Ente verso il quale avviene il trasferimento dei dati	Tipologia di trasmissione
25.	Area Comunicazione e Servizi cittadino- Servizi Demografici	al	Trasmissione dati variazioni anagrafiche al CSND tramite S.A:I.A. (settimanale)	Elettronica
26.	Area Comunicazione e Servizi cittadino- Servizi Demografici	al	Trasmissione dati variazioni anagrafiche AIRE al Ministero dell'Interno ((settimanale)	Elettronica
27.	Area Comunicazione e Servizi cittadino- Servizi Demografici	al	Trasmissione dati anagrafici All'agenzia delle entrate SAT di Torino (annuale)	Elettronica
28.	Area Comunicazione e Servizi cittadino- Servizi Demografici	al	Trasmissione dati tramite SIATEL all'Agenzia delle entrate per parifica codici fiscali (periodica)	Elettronica
29.	Area Comunicazione e Servizi cittadino- Servizi Demografici	al	Trasmissione dati anagrafici a pubbliche amministrazioni ai sensi dell'art.34 DPR 223/89 e art.177 D.lgs 196/2003 (a richiesta)	Cartacea, elettronica
30.	Area Comunicazione e Servizi cittadino- Servizi Demografici	al	Trasmissione dati anagrafici ed elenchi ad altri uffici del Comune (a richiesta)	Cartacea, elettronica
31.	Area Comunicazione e Servizi cittadino- Servizi Demografici	al	Trasmissione dati anagrafici ATO5 – Hera (a richiesta)	Elettronica
32.	Area Comunicazione e Servizi cittadino- Servizi Demografici	al	Trasmissione va variazioni anagrafiche enti previsti (mensile)	Cartacea, elettronica
33.	Area Comunicazione e Servizi cittadino- Servizi Demografici	al	Rilascio copia delle liste elettorali a chi ne fa richiesta per gli usi consentiti	Cartacea, elettronica
34.	Area Comunicazione e Servizi cittadino- Servizi Demografici	al	Invio dati all'ISTAT (estrazioni di residenti per indagini e movimenti demografici) a richiesta e mensile	Cartacea, elettronica
35.	Area Comunicazione e Servizi cittadino- Servizi Demografici	al	Trasmissione dei nati per servizio pediatrico dell'AUSL (mensile)	Elettronico
36.	Area Comunicazione e Servizi cittadino- Servizi Demografici	al	Trasmissione dati alla Motorizzazione Civile di Roma (mensile)	Cartacea
37.	Sport e volontariato sociale		Enti richiedenti Elenchi/Albi Associazioni, Consulte; tipologia	Cartacea ed elettronica
38.	Dati relativi a Piano acustico, PGTU, POC		Comune di Bologna	Via e-mail
39.	Dati relativi a Piano acustico, PGTU, POC		UNIBO	Via e-mail
40.	Dati relativi all'incarico assegnato: Bonifica Cantagallo		Dott. Umberto Meletti	Carta e e-mail
41.	Dati relativi all'incarico assegnato: Progetto CAMBIERESTI		Ass. CAMBIERESTI	Carta
42.	Dati relativi all'incarico assegnato: verifica e monitoraggio popolazioni chiroterri entro il Parco della Chiusa		Dott. Massimo Bertozzi	Carta
43.	Dati relativi all'incarico assegnato		Roberto Ciacci	
44.	Istituzione Casalecchio delle Culture		Studio Rag. Fabrizia Palma: Cessione fatture e note fornitori Istituzione.	Cartacea, elettronica.
45.	Area Servizi al Territorio		SARE (assunzioni e tirocini) Comunicazioni alla camera di commercio dell'elenco delle nuove costruzioni, ampliamenti e sopraelevazioni da trasmettersi entro il 5 di ogni mese su modulo ISTAT	Elettronico
46.	Area Servizi al Territorio Servizio Edilizia Pubblica e Privata		Invio entro il 30 giugno di ogni anno, all'anagrafe tributaria di Roma presso il Ministero delle Finanze, dei dati relativi a autorizzazioni rilasciate e dia in materia di attività commerciali	Cartacea
47.	Area Servizi al Territorio Servizio Attività Produttive			Elettronica

Progressivo	Struttura	Ente verso il quale avviene il trasferimento dei dati	Tipologia di trasmissione
48.	Area Servizi alla Persona educativi e scolastici	-Servizi MELAMANGIO Trasmissione flussi dei pagamenti da emettere per rette di mensa scolastica, la cui titolarità di incasso spetta a Melamangio. In accordo tra le parti i flussi possono essere trasmessi direttamente a Equitalia, con la quale Melamangio ha attivato una convenzione per l'emissione e l'incasso.	Elettronica
49.	Area Servizi alla Persona educativi e scolastici	-Servizi POSTE ITALIANE Trasmissione flussi dei pagamenti da emettere per rette di servizi scolastici ed educativi	Elettronica
50.	Area Servizi alla Persona educativi e scolastici	- Servizi Coop Sociale CADIAI Comunicazione dei dati personali e sensibili degli iscritti nei nidi e servizi per l'infanzia in convenzione con il Comune.	Cartaceo, elettronico
51.	Area Servizi alla Persona educativi e scolastici	- Servizi Consorzio KARABAK 2 Comunicazione dei dati personali e sensibili degli iscritti nei nidi e servizi per l'infanzia in convenzione con il Comune.	Cartaceo, elettronico
52.	Area Servizi alla Persona educativi e scolastici	- Servizi Polisportiva Giovanni Masi Comunicazione dei dati personali e sensibili degli iscritti nei nidi e servizi per l'infanzia in convenzione con il Comune.	Cartaceo, elettronico
53.	Area Servizi alla Persona educativi e scolastici	- Servizi Polisportiva Giovanni Masi Comunicazione dei dati personali e sensibili dei minori disabili che fruiscono del servizio di accompagnamento scolastico	Cartaceo, elettronico
54.	Area Servizi alla Persona educativi e scolastici	- Servizi Coop. Sociale Quadrifoglio Comunicazione dei dati personali e sensibili degli iscritti al servizio di orario prolungato dei nidi comunali	Cartaceo, elettronico
55.	Area Servizi alla Persona educativi e scolastici	- Servizi ASC Insieme 1) Cessione banche dati degli utenti dei servizi sociali 2) Comunicazione dati personali e sensibili di minori in stato di disagio socio-economico per i quali sono richieste agevolazioni per servizi educativi e scolastici.	Cartaceo, elettronico

Data di aggiornamento: 15/03/2010

## Il censimento dei beni che rientrano nel piano di sicurezza

In questa sezione del documento censiamo tutti gli strumenti informatici che hanno una qualche interferenza con il piano di sicurezza dell'ente e che contengono delle banche dati. In primo luogo presentiamo l'elenco delle sedi interessate dal progetto.

*Tavola 4.riepilogo delle sedi dell'ente*

Progressivo	Denominazione sede	Indirizzo	Tipo di collegamento
1.	Municipio	via dei Mille, 9	
2.	Sede Istituzionale	via dei Mille, 9	Fibra con Municipio
3.	Casa della Conoscenza	via Porrettana, 360	Fibra con Municipio
4.	Istituzione Casalecchio delle Culture	via Marconi, 14	Hiperlan con Casa della Conoscenza
5.	Centro di Documentazione Pedagogico	via del Fanciullo, 6	Fibra con Magazzino
6.	Magazzino - Adopera S.r.l.	via Guido Rossa, 1-3	Fibra con Municipio
7.	Cimitero	via Piave, 37	Fibra con Municipio
8.	Asilo Nido Don Fornasini	via Monte Sole, 3	Hiperlan con Municipio
9.	Asilo Nido Vighi	via Puccini, 17	Hiperlan con Municipio
10.	Stazione Carabinieri	via Marzocchi, 6	Fibra con Magazzino
11.	Centro Giovanile "Il Blogos"	via dei Mille, 25	Fibra con Municipio
12.	Centro Famiglie	via Galilei 8	Nessuno
<b>Data di aggiornamento: 25/03/2010</b>			

Di seguito presentiamo l'elenco dei beni informatici che sono atti a contenere banche dati o a permetterne in un qualunque modo l'utilizzo.

Tavola 5. Riepilogo del censimento dei beni informatici che rientrano nel piano di sicurezza dell'ente

Servizi funzionali										
Device	File server	Altri server	DB Server gestionale	E-mail	Apps gestionali	Servizi di gestione	Router o switch	Marca	S.O	F.T.
<b>Municipio Via dei Mille, 9</b>										
Cluster6-n1				X				HP	Windows Server 2003	Cluster Domino
Cluster6-n2				X				HP	Windows Server 2003	Cluster Domino
Cluster4-n1	X					E-directory		HP	Novell Netware 6.5	Cluster Netware
Cluster4-n2	X					E-directory		HP	Novell Netware 6.5	Cluster Netware
NwPrint						Printer Server - Identity Manager		ASUS	Novell Netware 6.5	Cluster Netware
Cluster5-n1			X					HP	Linux RedHat + Oracle	Cluster Linux
Cluster5-n2			X					HP	Linux RedHat + Oracle	Cluster Linux
Cluster8-n1			X					HP	Windows Server 2003 + Ms-Sql DB	Cluster Microsoft
Cluster8-n2			X					HP	Windows 2000 Server + Progress DB	Cluster Microsoft
Cluster7-n1		X						HP	Windows Server 2003	Cluster Microsoft + IIS + Apache web server
Cluster7-n2		X						HP	Windows Server 2003	Cluster Microsoft + IIS + Apache web server
WebLab						Reverse Proxy		ASUS	Windows Server 2003	Raid 5
Webapp01					X			HP	Linux	Raid 5
Webapp02					X			HP	Linux	Raid 5

Servizi funzionali										
Device	File server	Altri server	DB Server gestionale	E-mail	Apps gestionali	Servizi di gestione	Router o switch	Marca	S.O	F.T.
Castor						PDC - DNS - DHCP		ASUS	Windows Server 2003	Macchina Citrix XenServer
Pollux						PDC - DNS - DHCP		Server virtuale	Windows Server 2003	HA e Motion Citrix XenServer
Patch						WSUS		Server virtuale	Windows Server 2003	HA e Motion Citrix XenServer
Perseus						Backup Server		HP	Windows Server 2003	Raid 5
Titano						PDC - DNS - DHCP biblioteca		HP	Windows Server 2003	Raid 5
Hiperstream						Deduplica backup		Server virtuale	Windows Server 2003	HA e Motion Citrix XenServer
Winwkf						X		Server virtuale	Windows Server 2003	HA e Motion Citrix XenServer
Centralino		X						Server virtuale	Fedora	HA e Motion Citrix XenServer
TestLab			X Oracle - SIT					ACER	Windows Server 2003	Raid 5
Gespage						Printer Server Biblioteca		HP	Linux Fedora	Raid 5
Server		X						PRIMERGY	Windows Server 2003	Raid 1
Fortigate 01						Firewall		Fortinet	N.a.	Cluster
Fortigate 02						Firewall		Fortinet	N.a.	Cluster
FortiAnalyzer						Log di navigazione		Fortine	N.a.	Nessuno
Router vari							X	CISCO	CISCO IOS	/
Apparecchiature rete HyperLan							X	Varie		/
Switch vari							X	CISCO	CISCO IOS	/
<b>Magazzino – Via Guido Rossa, 1-3</b>										
OraStdb			X					HP	Linux RedHat + Oracle	Oracle Standby DB

Servizi funzionali										
Device	File server	Altri server	DB Server gestionale	E-mail	Apps gestionali	Servizi di gestione	Router o switch	Marca	S.O	F.T.
Cluster8-stdb			X					HP	Windows Server 2003	Microsoft MS-Sql Standby DB
Switch vari							X	Vari	n.a.	
<b>Altre sedi</b>										
Router							X	CISCO	CISCO IOS	/
Apparecchiature rete HyperLan							X	Varie		/
Switch vari							X	Vari	n.a.	Nessuno
Data di aggiornamento: 15/03/2010										

## **Analisi organizzativa dell'ente**

Scopo di questa fase è capire l'impatto che la sicurezza ha determinato nella definizione dell'organigramma dell'ente, se di impatto si può parlare.

Si tratta di partire dall'organigramma dell'ente per capire quali sono i centri di decisione che hanno influito o potranno influire sulle decisioni in merito alla sicurezza. Per le aziende certificate ISO questo processo è già stato largamente affrontato e documentato; nonostante questo rimane la necessità di controllare detto processo e di valutarne l'aggiornamento.

A titolo esemplificativo dell'impatto che una non accurata analisi organizzativa e giuridica dello stato dell'organizzazione può avere, presentiamo un esempio emblematico circa i rischi che corre l'ente dando il problema della sicurezza, "per scontato".

Il problema riguarda la teoria della downstream liability, un tema scottante in cause civili per fenomeni di hacking. Il problema sorge quando una organizzazione colpita non potrà essere risarcita nei danni subiti da un hacker (che spenderà tutti i suoi soldi per un legale). La moderna giurisprudenza afferma che l'organizzazione lesa potrà rivalersi "a valle" nei confronti dell'organizzazione che ha permesso all'hacker di entrare nei suoi sistemi consentendogli l'attacco!!

L'organizzazione chiamata in causa dovrà dimostrare di non essere stata negligente, di disporre di misure di sicurezza aggiornate ed adeguate.

Questa analisi ha, quindi, lo scopo di analizzare l'organizzazione del Comune di Casalecchio di Reno per fare in modo che essa non possa essere trovata "negligente".

Presentiamo in primo luogo l'organigramma dell'ente, evidenziando in colore giallo i centri di decisione in merito alla sicurezza dei dati:

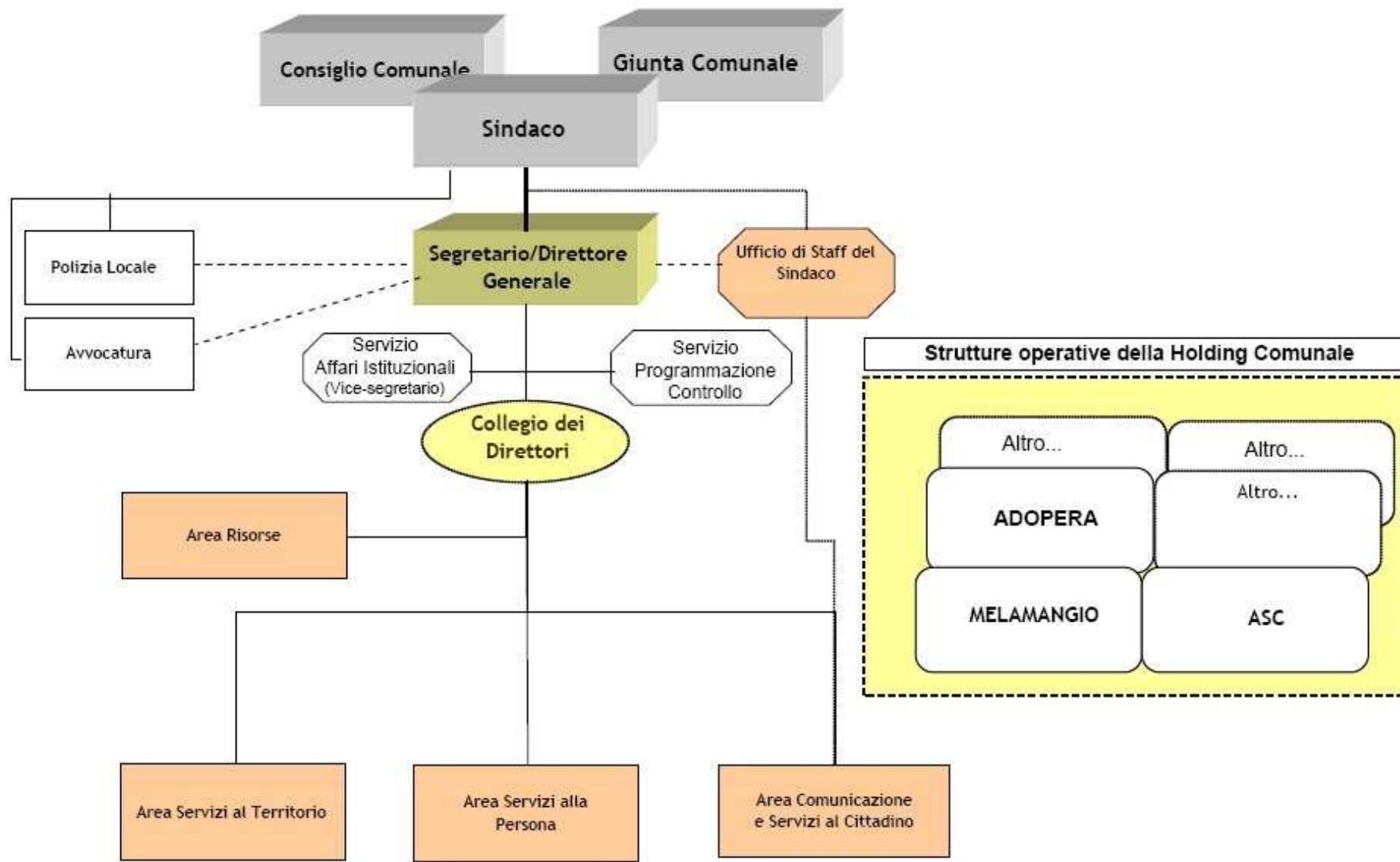


Figura 1 L'organigramma del Comune di Casalecchio di Reno

Da una semplice lettura si può comprendere chi nell'organizzazione del Comune di Casalecchio di Reno, con la sua attività e con le sue decisioni, può influire sulla sicurezza nella gestione dei dati. Tali persone sono state oggetto di percorsi di motivazione e di processi formativi, circa l'argomento.

Presentiamo a questo punto l'elenco degli incaricati, il gruppo di appartenenza ed il profilo ad essi associato.

*Tavola 6.riepilogo degli incaricati*

<b>NOME E COGNOME</b>	<b>GRUPPO</b>	<b>SEDE</b>	<b>PROFILO</b>
BATTISTINI TAMARA	ACCESSO SCOLAST.SERV. AMM.VI	Municipio	normale
CANETI MARCO	ACCESSO SCOLAST.SERV. AMM.VI	Municipio	normale
COBIANCHI ALBERTO	ACCESSO SCOLAST.SERV. AMM.VI	Municipio	normale
DEGLI ESPOSTI AMBRA	ACCESSO SCOLAST.SERV. AMM.VI	Municipio	normale
FERRONI MARA	ACCESSO SCOLAST.SERV. AMM.VI	Municipio	normale
MARI VALERIA	ACCESSO SCOLAST.SERV. AMM.VI	Municipio	normale
BAZZANI MAURO	AFFARI ISTITUZIONALI	Municipio	normale
BERTOZZI MARIA ROSARIA	AFFARI ISTITUZIONALI	Municipio	normale
DELLI CARRI LUCIA	AFFARI ISTITUZIONALI	Municipio	normale
SERPI ROCCO	AFFARI ISTITUZIONALI	Municipio	normale
ZANARINI MIRELLA	AFFARI ISTITUZIONALI	Municipio	normale
GIORDANO ARIANNA	AMBIENTE E PROTEZIONE CIVILE	Municipio	normale
MONINI RITA MARIA	AMBIENTE E PROTEZIONE CIVILE	Municipio	normale
PASSERINI ANDREA	AMBIENTE E PROTEZIONE CIVILE	Municipio	normale
PERI MARIA ANGELA	AMBIENTE E PROTEZIONE CIVILE	Municipio	normale

ZANASI SERGIO	AMBIENTE E PROTEZIONE CIVILE	Municipio	normale
BATTACCHI GIANLUCA	ANAGRAFE/STATO CIVILE/ELETT.LE	Municipio	normale
BERNARDI GIORGIA	ANAGRAFE/STATO CIVILE/ELETT.LE	Municipio	normale
BOSIO ANGELO	ANAGRAFE/STATO CIVILE/ELETT.LE	Municipio	normale
CAMPAGNOLI ELISABETTA	ANAGRAFE/STATO CIVILE/ELETT.LE	Municipio	normale
CAMPANI FIORELLA	ANAGRAFE/STATO CIVILE/ELETT.LE	Municipio	normale
DEGLI ESPOSTI DANIELA	ANAGRAFE/STATO CIVILE/ELETT.LE	Municipio	normale
FARNE' MASSIMO	ANAGRAFE/STATO CIVILE/ELETT.LE	Municipio	normale
GUIZZARDI ANTONELLA	ANAGRAFE/STATO CIVILE/ELETT.LE	Municipio	normale
OCCHIPINTI EVA	ANAGRAFE/STATO CIVILE/ELETT.LE	Municipio	normale
CERFOGLI ERMANNA	ASILI NIDO E SERV. EDUCATIVI		normale
ALBERI RITA	ASILI NIDO E SERV. EDUCATIVI		normale
ANDRISANI ANGELA	ASILI NIDO E SERV. EDUCATIVI		normale
ARMIENTO LUISA	ASILI NIDO E SERV. EDUCATIVI		normale
ARPI VALERIA	ASILI NIDO E SERV. EDUCATIVI		normale
BALESTRA AURORA	ASILI NIDO E SERV. EDUCATIVI		normale
BALESTRI SUSANNA	ASILI NIDO E SERV. EDUCATIVI		normale
BARONI PATRIZIA	ASILI NIDO E SERV. EDUCATIVI		normale
BELLONI FABIANA	ASILI NIDO E SERV. EDUCATIVI		normale
BERTONCELLI CRISTINA	ASILI NIDO E SERV. EDUCATIVI		normale
BETELLI MARINA	ASILI NIDO E SERV. EDUCATIVI		normale

BUSI TIZIANA	ASILI NIDO E SERV. EDUCATIVI	normale
CALIRI GIUSEPPA	ASILI NIDO E SERV. EDUCATIVI	normale
CALVARUSO GIUSEPPA	ASILI NIDO E SERV. EDUCATIVI	normale
CAPALDO ASSUNTA	ASILI NIDO E SERV. EDUCATIVI	normale
CAPODIFERRO MONICA	ASILI NIDO E SERV. EDUCATIVI	normale
CARBOTTI ANTONIA	ASILI NIDO E SERV. EDUCATIVI	normale
CARDONE ELISABETTA	ASILI NIDO E SERV. EDUCATIVI	normale
CAVASSA FEDERICA	ASILI NIDO E SERV. EDUCATIVI	normale
CAVICCHIOLI VALERIA	ASILI NIDO E SERV. EDUCATIVI	normale
CIVALE ANTONIO	ASILI NIDO E SERV. EDUCATIVI	normale
COMERCI FONTINA	ASILI NIDO E SERV. EDUCATIVI	normale
CRIVELLARO PAOLA	ASILI NIDO E SERV. EDUCATIVI	normale
CUSMA' PICCIONE SILVANA	ASILI NIDO E SERV. EDUCATIVI	normale
D'ANGELO ERIKA	ASILI NIDO E SERV. EDUCATIVI	normale
DEGLI ESPOSTI MANUELA	ASILI NIDO E SERV. EDUCATIVI	normale
DEGLI ESPOSTI PATRIZIA	ASILI NIDO E SERV. EDUCATIVI	normale
DONATI SIMONA	ASILI NIDO E SERV. EDUCATIVI	normale
DRAGONE DARIO	ASILI NIDO E SERV. EDUCATIVI	normale
FANCHINI INES	ASILI NIDO E SERV. EDUCATIVI	normale
FANTI ANTONELLA	ASILI NIDO E SERV. EDUCATIVI	normale
FERO VALERIA	ASILI NIDO E SERV. EDUCATIVI	normale
FERRARI FADIA	ASILI NIDO E SERV. EDUCATIVI	normale
FONTANELLI ANTONELLA	ASILI NIDO E SERV. EDUCATIVI	normale

GAMBERINI IRENE	ASILI NIDO E SERV. EDUCATIVI	normale
GAMBERINI PAOLA	ASILI NIDO E SERV. EDUCATIVI	normale
GARDINI SABRINA	ASILI NIDO E SERV. EDUCATIVI	normale
GINNETTI CARMELINA	ASILI NIDO E SERV. EDUCATIVI	normale
GRAGNOLINI ADELE	ASILI NIDO E SERV. EDUCATIVI	normale
GUIDORENI MARILENA	ASILI NIDO E SERV. EDUCATIVI	normale
LANDI SILVIA	ASILI NIDO E SERV. EDUCATIVI	normale
LIDAKI ANNA	ASILI NIDO E SERV. EDUCATIVI	normale
LORENZANO MARIA	ASILI NIDO E SERV. EDUCATIVI	normale
MAESTRAMI SANDRA	ASILI NIDO E SERV. EDUCATIVI	normale
MAMMARELLA ALFREDINA	ASILI NIDO E SERV. EDUCATIVI	normale
MARCHI MARIACHIARA	ASILI NIDO E SERV. EDUCATIVI	normale
MARCHI RITA	ASILI NIDO E SERV. EDUCATIVI	normale
MARESCA GABRIELLA	ASILI NIDO E SERV. EDUCATIVI	normale
MARI ANGELA	ASILI NIDO E SERV. EDUCATIVI	normale
MARSAN MANUELA	ASILI NIDO E SERV. EDUCATIVI	normale
MASETTI ELISABETTA	ASILI NIDO E SERV. EDUCATIVI	normale
MELOTTI GRAZIELLA	ASILI NIDO E SERV. EDUCATIVI	normale
MIGLIORI LORENZA	ASILI NIDO E SERV. EDUCATIVI	normale
MINGARELLI RITA	ASILI NIDO E SERV. EDUCATIVI	normale
MONDADORI KATIA	ASILI NIDO E SERV. EDUCATIVI	normale
MONTOLLI MARIA KATIA	ASILI NIDO E SERV. EDUCATIVI	normale
MUSIANI ALESSIO	ASILI NIDO E SERV. EDUCATIVI	normale

NOTO ELENA	ASILI NIDO E SERV. EDUCATIVI	normale
NOTO ROSALBA	ASILI NIDO E SERV. EDUCATIVI	normale
PALMIERI SILVIA	ASILI NIDO E SERV. EDUCATIVI	normale
PATRIZI ANTONELLA	ASILI NIDO E SERV. EDUCATIVI	normale
PEZZOLI PATRIZIA	ASILI NIDO E SERV. EDUCATIVI	normale
PICCININI NADIA	ASILI NIDO E SERV. EDUCATIVI	normale
PISU MICHELA	ASILI NIDO E SERV. EDUCATIVI	normale
PORCACCIO PATRIZIA	ASILI NIDO E SERV. EDUCATIVI	normale
RIZZOLI CRISTINA	ASILI NIDO E SERV. EDUCATIVI	normale
ROMANO CONCETTINA	ASILI NIDO E SERV. EDUCATIVI	normale
RUGGERI NADIA	ASILI NIDO E SERV. EDUCATIVI	normale
SABATTINI PATRIZIA	ASILI NIDO E SERV. EDUCATIVI	normale
SAGONA LUIGIA	ASILI NIDO E SERV. EDUCATIVI	normale
SALVATORI FRANCHI LAURA	ASILI NIDO E SERV. EDUCATIVI	normale
SCAMANDRI BARBARA	ASILI NIDO E SERV. EDUCATIVI	normale
SCHINELLI MARIA ROSA	ASILI NIDO E SERV. EDUCATIVI	normale
SCIANNA CATERINA	ASILI NIDO E SERV. EDUCATIVI	normale
STANZANI MARISA	ASILI NIDO E SERV. EDUCATIVI	normale
TOMESANI ELISABETTA	ASILI NIDO E SERV. EDUCATIVI	normale
VASSALLO MARIA VALERIA	ASILI NIDO E SERV. EDUCATIVI	normale
VELLUCCI CATERINA	ASILI NIDO E SERV. EDUCATIVI	normale
VENTURA LINA	ASILI NIDO E SERV. EDUCATIVI	normale
VENTURI LAURA	ASILI NIDO E SERV. EDUCATIVI	normale

VIGHI ANNA MARIA	ASILI NIDO E SERV. EDUCATIVI	normale
VIGNI NADIA	ASILI NIDO E SERV. EDUCATIVI	normale
ZANARDI ANNA MARIA	ASILI NIDO E SERV. EDUCATIVI	normale
ZANOTTI MONICA	ASILI NIDO E SERV. EDUCATIVI	normale
TATTINI SILVIA	ASILI NIDO E SERV. EDUCATIVI	normale
TORCELLO FEDERICA ANNA	ASILI NIDO E SERV. EDUCATIVI	normale
STASI MARIELLA	ASILI NIDO E SERV. EDUCATIVI	normale
TERRAZZINO FRANCESCA	ASILI NIDO E SERV. EDUCATIVI	normale
ALTINAR LIVIA RAMONA	ASILI NIDO E SERV. EDUCATIVI	normale
AMENTA VIRGINIA	ASILI NIDO E SERV. EDUCATIVI	normale
CALANDRA LOREDANA SANTINA	ASILI NIDO E SERV. EDUCATIVI	normale
CAMPORESI CRISTINA	ASILI NIDO E SERV. EDUCATIVI	normale
CORELUPI TIZIANA	ASILI NIDO E SERV. EDUCATIVI	normale
EMIGRI ILARIA	ASILI NIDO E SERV. EDUCATIVI	normale
JEBALI LAMIA	ASILI NIDO E SERV. EDUCATIVI	normale
MAESTRINI ANTONELLA	ASILI NIDO E SERV. EDUCATIVI	normale
MATTEI LISA	ASILI NIDO E SERV. EDUCATIVI	normale
NERI LONGINOTTI ELENA	ASILI NIDO E SERV. EDUCATIVI	normale
PAPA VERONICA	ASILI NIDO E SERV. EDUCATIVI	normale
PAVIGNANI PAOLA	ASILI NIDO E SERV. EDUCATIVI	normale
PERNICONE AGATA	ASILI NIDO E SERV. EDUCATIVI	normale
PETRELLA TOMMASO	ASILI NIDO E SERV. EDUCATIVI	normale
PINTABONA KATIUSCIA	ASILI NIDO E SERV. EDUCATIVI	normale

SEFERI FLORESHA	ASILI NIDO E SERV. EDUCATIVI		normale
TOSSANI FRANCESCA	ASILI NIDO E SERV. EDUCATIVI		normale
VECCHIET IRENE	ASILI NIDO E SERV. EDUCATIVI		normale
VILUCCHIO CRISTINA	ASILI NIDO E SERV. EDUCATIVI		normale
MONTANARO ISABELLA	ASILI NIDO E SERV. EDUCATIVI		normale
BIGNAMI MARIA PAOLA	ASSOCIAZION.O VOLONTAR.E GEMEL	Municipio	normale
BORSARI FRANCESCO	ASSOCIAZION.O VOLONTAR.E GEMEL	Municipio	normale
CREMONINI FRANCESCO	ASSOCIAZION.O VOLONTAR.E GEMEL	Municipio	normale
MATTEI MAURA	ATTIVITA' PRODUTTIVE E SUAP	Municipio	normale
BIANCHI DENISE	ATTIVITA' PRODUTTIVE E SUAP	Municipio	normale
CIAMPI MARCELLO	ATTIVITA' PRODUTTIVE E SUAP	Municipio	normale
COMMISSARI ANNALISA	ATTIVITA' PRODUTTIVE E SUAP	Municipio	normale
MELLO PIERA	ATTIVITA' PRODUTTIVE E SUAP	Municipio	normale
BATTAGLIA LILIA	BIBLIOTECA	biblioteca Via Porrettana n. 360	normale
BONI MANUELA	BIBLIOTECA	biblioteca Via Porrettana n. 361	normale
DE MARTINO FIORINA	BIBLIOTECA	biblioteca Via Porrettana n. 362	normale
LOLLI PAOLA	BIBLIOTECA	biblioteca Via Porrettana n. 363	normale
LONGHI NICOLA	BIBLIOTECA	biblioteca Via Porrettana n. 364	normale
NERI MASSIMILIANO	BIBLIOTECA	biblioteca Via Porrettana n. 365	normale
PATRIZI MIRELLA	BIBLIOTECA	biblioteca Via Porrettana n. 366	normale
ROPA LUCIANA	BIBLIOTECA	biblioteca Via	normale

		Porrettana n. 367	
STEFANINI VIRGINIA	BIBLIOTECA	biblioteca Via Porrettana n. 368	normale
TOMESANI VALERIA	CIOP	Municipio	normale
CALVO GIANLUCA	COLLAB.COORDINATI CONTINUATIVI	Municipio	normale
CAMPAZZI CHIARA	COLLAB.COORDINATI CONTINUATIVI	Municipio	normale
DI CAMILLO CATIA	COLLAB.COORDINATI CONTINUATIVI	Municipio	normale
DI TORO MAMMARELLA MASSIM	COLLAB.COORDINATI CONTINUATIVI	Municipio	normale
GUIDI CHIARA	COLLAB.COORDINATI CONTINUATIVI	Municipio	normale
MELOTTI NICOLO'	COLLAB.COORDINATI CONTINUATIVI	Municipio	normale
PICCINNI ANTONIO	COLLAB.COORDINATI CONTINUATIVI	Municipio	normale
SACHS ALICE	COLLAB.COORDINATI CONTINUATIVI	Municipio	normale
BONFATTI ANNA	CONTRATTI PATRIM.E BENI IMMOB.	Municipio	normale
CLO' LUCIA	CONTRATTI PATRIM.E BENI IMMOB.	Municipio	normale
EMILIANI CARLO	CONTRATTI PATRIM.E BENI IMMOB.	Municipio	normale
FARNE' ROSELLA	CONTRATTI PATRIM.E BENI IMMOB.	Municipio	normale
LORENZONI CRISTINA	CONTRATTI PATRIM.E BENI IMMOB.	Municipio	normale
MANGANIELLO ROBERTO	CONTRATTI PATRIM.E BENI IMMOB.	Municipio	normale
MONTANARI CARMEN	CONTRATTI PATRIM.E BENI IMMOB.	Municipio	normale
BIANCHI DANIELE	CONTROLLO EDILIZ. EDIL.PRIVATA	Municipio	normale

CORTI RENZO	CONTROLLO EDILIZ. EDIL.PRIVATA	Municipio	normale
VERONESI SILVIA	CONTROLLO EDILIZ. EDIL.PRIVATA	Municipio	normale
RIEFOLO GIOVANNA	CONTROLLO GESTIONE ORGAN MET.	Municipio	normale
STEFANELLI MARCO	CONTROLLO GESTIONE ORGAN MET.	Municipio	normale
MATTIOLI EMILIANO	CONTROLLO GESTIONE ORGAN MET.	Municipio	normale
SANNINO MARIA ROSARIA	CONTROLLO SERV.A GEST.ESTERNA	Municipio	normale
BERGAMINI CINZIA	COORDINAMENTO PEDAGOGICO	via del fanciullo casa solidarieta'	normale
FERRARI ANGELA	COORDINAMENTO PEDAGOGICO	Municipio	normale
GIUDICI ALESSANDRA	COORDINAMENTO PEDAGOGICO	via del fanciullo casa solidarieta'	normale
GUERRA PATRIZIA	COORDINAMENTO PEDAGOGICO	via del fanciullo casa solidarieta'	normale
PALMERI MARIETTINA	COORDINAMENTO PEDAGOGICO	via del fanciullo casa solidarieta'	normale
PREITE GIULIANA LUCIA	COORDINAMENTO PEDAGOGICO	via del fanciullo casa solidarieta'	normale
RUGGIERO AMELIA	COORDINAMENTO PEDAGOGICO	via del fanciullo casa solidarieta'	normale
MASCAGNI FEDERICA	CULTURA E BENI CULTURALI	biblioteca Via Porrettana n. 360	normale
MONTANARI DAVIDE	CULTURA E BENI CULTURALI	Istituzione Via Marconi	Alto
PANIERI MANUELA	CULTURA E BENI CULTURALI	Istituzione Via Marconi	normale
PATETTA NICOLA	CULTURA E BENI CULTURALI	Istituzione Via Marconi	normale
RUBBI MASSIMILIANO	CULTURA E BENI CULTURALI	Istituzione Via Marconi	normale
TROTTA MAURIZIO	CULTURA E BENI CULTURALI	Istituzione Via Marconi	normale

ZANETTI JENNIFER	CULTURA E BENI CULTURALI	Istituzione Via Marconi	normale
CINQUE MICHELE	CULTURA E BENI CULTURALI	biblioteca Via Porrettana n. 360	normale
GAGGIOLI AIDA	DIRIGENTI	Municipio	Alto
GALLIANI RAFFAELLA	DIRIGENTI	Municipio	Alto
BATTISTINI FABIANA	DIRIGENTI	Municipio	Alto
BIANCHI VITTORIO EMANUELE	DIRIGENTI	Municipio	Alto
CAVINA GIAN PAOLO	DIRIGENTI	Municipio	Alto
SALVAGNO MICHELA	ELEZIONI PROV.LI E REGIONALI	Municipio	normale
ERCOLINI MOSE'	ENTRATE	Municipio	normale
FAVA MARA	ENTRATE	Municipio	normale
FRANCESCONI DANIELA	ENTRATE	Municipio	normale
GIOVAGNONI GABRIELLA	ENTRATE	Municipio	normale
GOTTI GRAZIELLA	ENTRATE	Municipio	normale
PEDRETTI SARA	ENTRATE	Municipio	normale
FINI LISA	INFORMATICA E CENTRO ELETTRON.	Municipio	normale
MARCHETTI ALESSANDRO	INFORMATICA E CENTRO ELETTRON.	Municipio	normale
NERETTI ELISA	INFORMATICA E CENTRO ELETTRON.	Municipio	normale
TREBBI BRUNO	INFORMATICA E CENTRO ELETTRON.	Municipio	normale
VENTURA ANDREA	INFORMATICA E CENTRO ELETTRON.	Municipio	normale
BOSELLI BARBARA	INFORMATICA E CENTRO ELETTRON.	Municipio	normale
BREDA PAOLO	PERS.COMANDATO C/O ALTRI ENTI		normale

MINGARELLI ALBERTO	PERS.COMANDATO C/O ALTRI ENTI		normale
BRANDOLINI ANDREA	PERS.COMANDATO C/O ASC	via cimarosa c/o USL	normale
CARUSO LAURA	PERS.COMANDATO C/O ASC	via cimarosa c/o USL	normale
CIOFFI NORMA	PERS.COMANDATO C/O ASC	via cimarosa c/o USL	normale
COLLINA SABRINA	PERS.COMANDATO C/O ASC	via cimarosa c/o USL	normale
CONTI MADDALENA	PERS.COMANDATO C/O ASC	via cimarosa c/o USL	normale
FRANGINI SUSANNA	PERS.COMANDATO C/O ASC	via cimarosa c/o USL	normale
GANDOLFI ANTONELLA	PERS.COMANDATO C/O ASC	via cimarosa c/o USL	normale
GNUDI STEFANO	PERS.COMANDATO C/O ASC	via cimarosa c/o USL	normale
LEPERA DOMENICA	PERS.COMANDATO C/O ASC	via cimarosa c/o USL	normale
LOTITO PAOLO	PERS.COMANDATO C/O ASC	via cimarosa c/o USL	normale
MAGAGNI MARIA CRISTINA	PERS.COMANDATO C/O ASC	via cimarosa c/o USL	normale
MAGRI VALERIA	PERS.COMANDATO C/O ASC	via cimarosa c/o USL	normale
MAIORANO NICOLETTA	PERS.COMANDATO C/O ASC	via cimarosa c/o USL	normale
NATALINI LAURA	PERS.COMANDATO C/O ASC	via cimarosa c/o USL	normale
NEGRONI ELENA	PERS.COMANDATO C/O ASC	via cimarosa c/o USL	normale
PAIOLI MARINA	PERS.COMANDATO C/O ASC	via cimarosa c/o USL	normale
PARINI ALESSANDRA	PERS.COMANDATO C/O ASC	via cimarosa c/o USL	normale
PARISI PAOLA	PERS.COMANDATO C/O ASC	via cimarosa c/o USL	normale
PUCCINI ANTONELLA	PERS.COMANDATO C/O ASC	via cimarosa c/o USL	normale
PUNGINELLI MARIA GRAZIA	PERS.COMANDATO C/O ASC	via cimarosa c/o USL	normale
RENNA CARLOTTA	PERS.COMANDATO C/O ASC	via cimarosa c/o USL	normale
ROVERI MICHELA	PERS.COMANDATO C/O ASC	via cimarosa c/o USL	normale

RUSSO LUIGINA	PERS.COMANDATO C/O ASC	via cimarosa c/o USL	normale
TORRI LORENZO	PERS.COMANDATO C/O ASC	via cimarosa c/o USL	normale
VERBOSCHI FRANCA	PERS.COMANDATO C/O ASC	via cimarosa c/o USL	normale
BARBANI GALLI MAGDA	PIANIFICAZIONE TERRITORIALE	Municipio	normale
BEGGIATO TIZIANA	PIANIFICAZIONE TERRITORIALE	Municipio	normale
DIPAOLA DONATELLA	PIANIFICAZIONE TERRITORIALE	Municipio	normale
POMI LUCA	PIANIFICAZIONE TERRITORIALE	Municipio	normale
ACCARISI SIMONA	POLIZIA MUNICIPALE	Municipio	normale
BENVENUTI GIORGIO	POLIZIA MUNICIPALE	Municipio	normale
BERNARDI EMMA	POLIZIA MUNICIPALE	Municipio	normale
BOLDRINI MATTEO	POLIZIA MUNICIPALE	Municipio	normale
CASADEI MANUELA	POLIZIA MUNICIPALE	Municipio	normale
DOBBOLETTA MAURIZIO	POLIZIA MUNICIPALE	Municipio	normale
EVANGELISTI DANIELE	POLIZIA MUNICIPALE	Municipio	normale
FABBRI FABIO	POLIZIA MUNICIPALE	Municipio	normale
FANTINI GIOVANNI	POLIZIA MUNICIPALE	Municipio	normale
FANTINI MAURIZIO	POLIZIA MUNICIPALE	Municipio	normale
FLORENZANO FAUSTO	POLIZIA MUNICIPALE	Municipio	normale
FONTANA ROBERTA	POLIZIA MUNICIPALE	Municipio	normale
GAMBERINI FEDERICA	POLIZIA MUNICIPALE	Municipio	normale
LOBBA PAOLO	POLIZIA MUNICIPALE	Municipio	normale
MACCANTI PAOLA	POLIZIA MUNICIPALE	Municipio	normale
MIGLIORINI ALESSIA	POLIZIA MUNICIPALE	Municipio	normale

MIGNANI MONICA	POLIZIA MUNICIPALE	Municipio	normale
MONDELLO VINCENZO	POLIZIA MUNICIPALE	Municipio	normale
MORA VALENTINA	POLIZIA MUNICIPALE	Municipio	normale
PACCHIONI RICCARDO	POLIZIA MUNICIPALE	Municipio	normale
PACE EMILIA	POLIZIA MUNICIPALE	Municipio	normale
PARRELLA CRISTIAN	POLIZIA MUNICIPALE	Municipio	normale
RETTONDINI MICHELA	POLIZIA MUNICIPALE	Municipio	normale
SANDRI LUCA	POLIZIA MUNICIPALE	Municipio	normale
SERAFINI MICAELA	POLIZIA MUNICIPALE	Municipio	normale
SPERLI LAURA	POLIZIA MUNICIPALE	Municipio	normale
TOFFALONI PAOLO	POLIZIA MUNICIPALE	Municipio	normale
URBINATI LUCIA	POLIZIA MUNICIPALE	Municipio	normale
VENTURA ANDREA	POLIZIA MUNICIPALE	Municipio	normale
BOLOGNESI STEFANO	POLIZIA MUNICIPALE	Municipio	Alto
CEROLINI CRISTINA	PROGETT.ENTE OPERE PUBBLICHE	Municipio	normale
MARCHI MARCO	PROGETT.ENTE OPERE PUBBLICHE	Municipio	normale
PASSERI ROSELLA	PROTOCOLLO ARCHIVIO	Municipio	normale
RABBI CLAUDIA	PROTOCOLLO ARCHIVIO	Municipio	normale
SERRA MAURIZIO	PROTOCOLLO ARCHIVIO	Municipio	normale
CASSANELLI ALBINA	RAGIONERIA E BILANCIO	Municipio	normale
DALLE OLLE BARBARA	RAGIONERIA E BILANCIO	Municipio	normale
GRIMANDI TIZIANA	RAGIONERIA E BILANCIO	Municipio	normale

GUIDI SILVIA	RAGIONERIA E BILANCIO	Municipio	normale
RODOLFI ERIKA	RAGIONERIA E BILANCIO	Municipio	normale
VITALI MORENA	RAGIONERIA E BILANCIO	Municipio	normale
TRENTINI ANTONELLA	SPESE LEGALI	Municipio	normale
AMANTI CINZIA	SPESE LEGALI CONSULENZA GIURID	Municipio	normale
ANTONI FIAMMETTA	SPORTELLO POLIFUNZIONALE	Municipio	normale
BALDI EMANUELA	SPORTELLO POLIFUNZIONALE	Municipio	normale
CAMARDA LUCIA	SPORTELLO POLIFUNZIONALE	Municipio	normale
CIRILLO MICHELE	SPORTELLO POLIFUNZIONALE	Municipio	normale
COLLIVA ENRICO	SPORTELLO POLIFUNZIONALE	Municipio	normale
FUSCO MARIA TERESA	SPORTELLO POLIFUNZIONALE	Municipio	normale
GROSSI BARBARA	SPORTELLO POLIFUNZIONALE	Municipio	normale
MASINI FABRIZIA	SPORTELLO POLIFUNZIONALE	Municipio	normale
MORARA SILVIA	SPORTELLO POLIFUNZIONALE	Municipio	normale
PAGANELLI PATRIZIA	SPORTELLO POLIFUNZIONALE	Municipio	normale
PULEGA AMANDA	SPORTELLO POLIFUNZIONALE	Municipio	normale
RIVETTO SILVIA	SPORTELLO POLIFUNZIONALE	Municipio	normale
VANNACCI MARIA GRAZIA	SPORTELLO POLIFUNZIONALE	Municipio	normale
VITALE SILVIA	SPORTELLO POLIFUNZIONALE	Municipio	normale
DONATI DANILO	TRASPORTO SCOLASTICO	Municipio	normale
GIANNONE ROSANNA	TRASPORTO SCOLASTICO	Municipio	normale
MARCHI COSETTA	TRASPORTO SCOLASTICO	Municipio	normale
RIZZI ROBERTO	TRASPORTO SCOLASTICO	Municipio	normale

BERNARDINI VIVIANA	TRATT.ECON.DEL PERS.E ORG.IST.	Municipio	normale
CANDICE RENATA	TRATT.ECON.DEL PERS.E ORG.IST.	Municipio	normale
FANARA ORIETTA	TRATT.ECON.DEL PERS.E ORG.IST.	Municipio	normale
PREVEDELLO OMBRETTA	TRATT.ECON.DEL PERS.E ORG.IST.	Municipio	normale
VENTURA GIULIANO	TRATT.ECON.DEL PERS.E ORG.IST.	Municipio	normale
MARANI LORENZA	TRATT.GIURID.E AMM.VO DEL PERS	Municipio	normale
PAIARI PATRIZIA	TRATT.GIURID.E AMM.VO DEL PERS	Municipio	normale
PIERAGNOLO ROBERTA	TRATT.GIURID.E AMM.VO DEL PERS	Municipio	normale
RICCI MARINELLA	TRATT.GIURID.E AMM.VO DEL PERS	Municipio	normale
SORDILLO CARMELA	TRATT.GIURID.E AMM.VO DEL PERS	Municipio	normale
STAGNI ROBERTA	TRATT.GIURID.E AMM.VO DEL PERS	Municipio	normale
STANZANI SERENA	TRATT.GIURID.E AMM.VO DEL PERS	Municipio	normale
VALPONDI FABIO	TRATT.GIURID.E AMM.VO DEL PERS	Municipio	normale
CARBONI SARA	UFF.GABINETTO SINDACO/COMUNIC.	Municipio	normale
GUIDASTRI MARIA CECILIA	UFF.GABINETTO SINDACO/COMUNIC.	Municipio	normale
LELLI LAURA	UFF.GABINETTO SINDACO/COMUNIC.	Municipio	normale
UNGARELLI MAURO	UFF.GABINETTO SINDACO/COMUNIC.	Municipio	normale
ZANNONI CLAUDIA	UFF.GABINETTO SINDACO/COMUNIC.	Municipio	normale
GRILLI MARA	UFF.GABINETTO SINDACO/COMUNIC.	Municipio	normale

CORAZZA VALERIA	UFFICIO AMM.VO PIANIFICAZIONE	Municipio	normale
GRUPPIONI SABRINA	UFFICIO AMM.VO PIANIFICAZIONE	Municipio	normale
MARZOCCHI ANNA	UFFICIO AMM.VO PIANIFICAZIONE	Municipio	normale
PUNGETTI PATRIZIA	UFFICIO AMM.VO PIANIFICAZIONE	Municipio	normale
REGAZZI MARIA TERESA	UFFICIO AMM.VO PIANIFICAZIONE	Municipio	normale
SAVINI MARIA	UFFICIO AMM.VO PIANIFICAZIONE	Municipio	normale
VENTURA PAOLA	UFFICIO AMM.VO PIANIFICAZIONE	Municipio	normale
BOLELLI EMANUELE	UFFICIO COMMESSI	Municipio	normale
GIACOBINO LUCIA	UFFICIO COMMESSI	Municipio	normale
LIETZ SILVANA	UFFICIO COMMESSI	Municipio	normale
PALLOTTI RENZO	UFFICIO COMMESSI	Municipio	normale
VESPIA ANTONIO	UFFICIO COMMESSI	Municipio	normale
ZIMPERI MASSIMO	UFFICIO COMMESSI	Municipio	normale
MUSOLESI PAOLA	UFFICIO COMMESSI	Municipio	normale
VENTURA NARA	VIABILITA' E TRAFFICO	Municipio	normale
Data di aggiornamento 15/03/2010			

*Tavola 7.riepilogo dei profili*

<b>GRUPPO</b>	<b>PROFILO</b>	<b>CARATTERISTICHE DEL PROFILO</b>
Tutti i gruppi	Normale	Sono consentite tutte e sole le operazioni di lettura e scrittura dei dati (quindi di modifica) per l'ordinario svolgimento della propria mansione
Tutti i gruppi	Minimo	Sono consentite tutte e sole le operazioni di lettura per l'ordinario svolgimento della propria mansione
Tutti i gruppi	Alto	Sono consentite tutte e sole le operazioni di lettura e scrittura (quindi di modifica) per l'ordinario svolgimento della propria mansione e la possibilità di modificare i diritti degli altri membri del gruppo

## ***Rapporti con professionisti ed incaricati non dipendenti dell'ente***

Allo scopo di assicurare il rispetto del codice sulla tutela dei dati personali, anche coloro che entrano in qualche modo in rapporto con l'ente senza diventarne dipendenti a tempo indeterminato, sono tenuti ad un comportamento corretto.

Per essere sicuri di ciò, il comune, nella sottoscrizione dell'incarico, ha aggiunto i seguenti punti:

- L'incaricato è autorizzato ad intervenire sui dati e sui sistemi informativi gestiti dal comune solo con atti strettamente necessari alla prestazione dei servizi oggetto di contratto, ed è fatto esplicito divieto di consultare, copiare, cancellare e fare qualunque operazione sui dati oggetto di trattamento, a meno di diversa autorizzazione scritta da parte del responsabile del trattamento dei dati.
- Il titolare si riserva di fare controlli sull'operato del responsabile esterno in qualunque momento e con qualunque mezzo consentito dalla legge.
- Il soggetto cui le attività sono affidate dichiara:
  - di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, possono essere dati personali e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali;
  - di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali;
  - di adottare le istruzioni specifiche ricevute per il trattamento dei dati personali attraverso il manuale degli incaricati;
  - di impegnarsi a relazionare ogni volta che è reputato necessario sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze;
  - di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

Le suddette dichiarazioni sono oggetto di specifica firma di accettazione da parte dell'incaricato.

## **Distribuzione dei compiti e delle responsabilità (regola 19.2 dell'Allegato B al Codice)**

In questa sezione è costruita una mappa che associa ad ogni struttura (o reparto, dipartimento, ufficio) i trattamenti da questa effettuati, descrivendo sinteticamente l'organizzazione della struttura medesima e le relative responsabilità. Ci si può riferire anche ad analoghe documentazioni già predisposte dal titolare (ordinamenti, ordini di servizio, regolamenti interni).

Tavola 8.distribuzione dei compiti e delle responsabilità

Area	Responsabile del trattamento	Settore/Servizio	Responsabile di settore/servizio P.O.	Trattamenti operati dalla struttura	Compiti della struttura
Direzione Generale	Raffaella Galliani	Segretario/Direttore Generale	Raffaella Galliani	Vedi allegato censimento trattamenti	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Ufficio Staff del Sindaco	Gian Paolo Cavina	Ufficio Staff del Sindaco	Gian Paolo Cavina	Vedi allegato censimento trattamenti	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Avvocatura	avv. Antonella Trentini	Avvocatura	avv. Antonella Trentini	Vedi allegato censimento trattamenti	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Direzione Generale	Raffaella Galliani	Servizio Affari Istituzionale	Maria Rosa Bertozzi	Vedi allegato censimento trattamenti	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Direzione Generale	Raffaella Galliani	Servizio Programmazione e controllo	Marco Stefanelli	Vedi allegato censimento trattamenti	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Risorse	Fabiana Battistini	Servizio Ragioneria e Bilancio	Barbara DalleOlle	Vedi allegato censimento trattamenti	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Risorse	Fabiana Battistini	Servizio Acquisti, gare e contratti	Carlo Emiliani	Vedi allegato censimento trattamenti	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa

Area	Responsabile del trattamento	Settore/Servizio	Responsabile di settore/servizio P.O.	Trattamenti operati dalla struttura	Compiti della struttura
Area Risorse	Fabiana Battistini	Servizio Entrate	Mosè Ercolini	Vedi allegato censimento trattamenti	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Risorse	Fabiana Battistini	Servizio Amministrativa del Personale	Serena Stanzani	Vedi allegato censimento trattamenti	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa-conservazione
Area Servizi al Territorio	Vittorio Emanuele Bianchi	Servizio Pianificazione e mobilità	Renzo Corti	Vedi allegato censimento trattamenti	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Servizi al Territorio	Vittorio Emanuele Bianchi	SIT Sistema Informativo Territoriale	Vittorio Emanuele Bianchi	Vedi allegato censimento trattamenti	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Servizi al Territorio	Vittorio Emanuele Bianchi	Servizio Amministrativo di Area	Vittorio Emanuele Bianchi	Vedi allegato censimento trattamenti	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Servizi al Territorio	Vittorio Emanuele Bianchi	Servizio Edilizia Pubblica e Privata	Renzo Corti	Vedi allegato censimento trattamenti	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa

Area	Responsabile del trattamento	Settore/Servizio	Responsabile di settore/servizio P.O.	Trattamenti operati dalla struttura	Compiti della struttura
Area Servizi al Territorio	Vittorio Emanuele Bianchi	Servizio Programmazione Opere Pubbliche	Andrea Passerini	Vedi allegato censimento trattamenti	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Servizi al Territorio	Vittorio Emanuele Bianchi	Servizio Ambiente e Sostenibilità	Andrea Passerini	Vedi allegato censimento trattamenti	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Servizi al Territorio	Vittorio Emanuele Bianchi	Servizio Attività Produttive	Denis Bianchi	Vedi allegato censimento trattamenti	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Servizi alla Persona	Elisabetta Scoccati	Ufficio di Piano Sociale	Mara Ferroni	Vedi allegato censimento trattamenti	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Servizi alla Persona	Elisabetta Scoccati	Pari opportunità	Maria Rosaria Bertozzi	Vedi allegato censimento trattamenti	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Servizi alla Persona	Elisabetta Scoccati	Servizio di Staff e di Supporto Amministrativo	Mara Ferroni	Vedi allegato censimento trattamenti	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa

Area	Responsabile del trattamento	Settore/Servizio	Responsabile di settore/servizio P.O.	Trattamenti operati dalla struttura	Compiti della struttura
Area Servizi alla Persona	Elisabetta Scoccati	Servizi Educativi e Scolatici	Giovanni Amodio	Vedi allegato censimento trattamenti	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Servizi alla Persona	Elisabetta Scoccati	Servizi sportivi e Socio Territoriali	Maria Paola Bignami	Vedi allegato censimento trattamenti	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Servizi alla Persona	Elisabetta Scoccati	Istituzione Casalecchio delle Culture	Davide Montanari	Vedi allegato censimento trattamenti	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Comunicazione e Rapporti con il cittadino	Gian Paolo Cavina	Semplice Polifunzionale Sportello	Massimo Farnè	Vedi allegato censimento trattamenti	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Comunicazione e Rapporti con il cittadino	Gian Paolo Cavina	Servizi Demografici	Massimo Farnè	Vedi allegato censimento trattamenti	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Comunicazione e Rapporti con il cittadino	Gian Paolo Cavina	Servizio Sistemi Informativi	Gian Paolo Cavina	Vedi allegato censimento trattamenti	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa

Area	Responsabile del trattamento	Settore/Servizio	Responsabile di settore/servizio P.O.	Trattamenti operati dalla struttura	Compiti della struttura
Area Comunicazione e Rapporti con il cittadino	Gian Paolo Cavina	Comunicazione	Gian Paolo Cavina	Vedi allegato censimento trattamenti	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa

**Data di aggiornamento: 15/03/2010**

## ***L'accesso alle strutture fisiche dell'ente***

Vogliamo ora mettere in evidenza chi ha le “chiavi” per poter accedere alle strutture dell'ente: lo facciamo con la seguente tabella riepilogativa. Ricordiamo che tutto lo stabile è protetto da chiave e sistema di allarme

*Tavola 9.: assegnazione delle chiavi di accesso ai locali dell'ente*

<b>COGNOME E NOME</b>	<b>SERVIZIO/FUNZIONE</b>	<b>Struttura di cui si possiede la chiave di accesso</b>	<b>EVENTUALI NOTE</b>
Regazzi Maria Teresa	Ambiente / addetto amministrativo	Ex Magazzino Comunale	Oggi proprietà di ADOPERA
Passerini Andrea	Ambiente e sostenibilità/responsabile di servizio	Ex Magazzino Comunale	Oggi proprietà di ADOPERA
Zanasi Sergio	Ambiente / Tecnico	Ex Magazzino Comunale	Oggi proprietà di ADOPERA
Cerolini Cristina	LL.PP. / Tecnico	Ex Magazzino Comunale	Oggi proprietà di ADOPERA
Marchi Marco	LL.PP. / Tecnico	Ex Magazzino Comunale	Oggi proprietà di ADOPERA
Giordano Arianna	Diritti Animali	Ex Magazzino Comunale	Oggi proprietà di ADOPERA
Cinzia Amanti	Legale	Uff. 89 e 90	
Antonella Trentini	Legale	Uff. 89 e 90	
Incaricato Manutencoop	pulizie	Uff. 89 e 90	
Massimo Zimperi	Semplice (Commessi)	Municipio	
Renzo Pallotti	Semplice (Commessi)	Municipio	
Emanuele Bolelli	Semplice (Commessi)	Municipio	
Silvana Lietz	Semplice (Commessi)	Municipio	
Antonio Vespia	Semplice (Commessi)	Municipio	
Lucia Giacobino	Semplice (Commessi)	Municipio	

<b>COGNOME E NOME</b>	<b>SERVIZIO/FUNZIONE</b>	<b>Struttura di cui si possiede la chiave di accesso</b>	<b>EVENTUALI NOTE</b>
BATTAGLIA LILIA	SERVIZIO BIBLIOTECA	CHIAVI STRUTTURA CASA DELLA CONOSCENZA	Possiede una copia della chiave di un accesso, le altre sono depositate presso la struttura.
BONI MANUELA	SERVIZIO BIBLIOTECA	CHIAVI STRUTTURA CASA DELLA CONOSCENZA	Possiede una copia della chiave di un accesso, le altre sono depositate presso la struttura.
CINQUE MICHELE	SERVIZIO BIBLIOTECA	CHIAVI STRUTTURA CASA DELLA CONOSCENZA	Possiede una copia della chiave di un accesso, le altre sono depositate presso la struttura.
DE MARTINO FIORINA	SERVIZIO BIBLIOTECA	CHIAVI STRUTTURA CASA DELLA CONOSCENZA	Possiede una copia della chiave di un accesso, le altre sono depositate presso la struttura.
LONGHI NICOLA	SERVIZIO BIBLIOTECA	CHIAVI STRUTTURA CASA DELLA CONOSCENZA	Possiede una copia della chiave di un accesso, le altre sono depositate presso la struttura.
NERI MASSIMILIANO	SERVIZIO BIBLIOTECA	CHIAVI STRUTTURA CASA DELLA CONOSCENZA	Possiede una copia della chiave di un accesso, le altre sono depositate presso la struttura.
PATRIZI MIRELLA	SERVIZIO BIBLIOTECA	CHIAVI STRUTTURA CASA DELLA CONOSCENZA	Possiede una copia della chiave di un accesso, le altre sono depositate presso la struttura.
STEFANINI VIRGINIA	SERVIZIO BIBLIOTECA	CHIAVI STRUTTURA CASA DELLA CONOSCENZA	Possiede una copia della chiave di un accesso, le altre sono depositate presso la struttura.

COGNOME E NOME	SERVIZIO/FUNZIONE	Struttura di cui si possiede la chiave di accesso	EVENTUALI NOTE
MASCAGNI FEDERICA	SERVIZIO BIBLIOTECA	CHIAVI STRUTTURA CASA DELLA CONOSCENZA	Non ancora in servizio. Come gli altri, possiederà una copia della chiave di un accesso, le altre sono depositate presso la struttura.
ROPA LUCIANA	SERVIZIO BIBLIOTECA	CHIAVI STRUTTURA CASA DELLA CONOSCENZA	Possiede una copia della chiave di un accesso, le altre sono depositate presso la struttura.
MONTANARI DAVIDE	ISTITUZIONE CASALECCHIO DELLE CULTURE	Chiave accesso uffici Istituzione via Marconi 14, chiavi struttura Casa della conoscenza, chiavi Centro giovanile, Rifugio della Chiusa, chiave di emergenza Teatro.	Possiede solo una copia della chiave di un accesso alla Casa della Conoscenza e agli uffici di Via Marconi 14; presso questi ultimi depositate le altre chiavi.
LOLLI PAOLA	ISTITUZIONE CASALECCHIO DELLE CULTURE	Chiave accesso uffici Istituzione via Marconi 14, chiavi struttura Casa della conoscenza, chiavi Centro giovanile, Rifugio della Chiusa, chiave di emergenza Teatro.	Non ancora in servizio. Come gli altri possiederà solo una copia della chiave di un accesso alla Casa della Conoscenza e agli uffici di Via Marconi 14; presso questi ultimi depositate le altre chiavi.
PATETTA NICOLA	ISTITUZIONE CASALECCHIO DELLE CULTURE	Chiave accesso uffici Istituzione via Marconi 14, chiavi struttura Casa della conoscenza, chiavi Centro giovanile, Rifugio della Chiusa, chiave di emergenza Teatro.	Possiede solo una copia della chiave di un accesso alla Casa della Conoscenza e agli uffici di Via Marconi 14; presso questi ultimi depositate le altre chiavi.

COGNOME E NOME	SERVIZIO/FUNZIONE	Struttura di cui si possiede la chiave di accesso	EVENTUALI NOTE
ZANETTI JENNIFER	ISTITUZIONE CASALECCHIO DELLE CULTURE	Chiave accesso uffici Istituzione via Marconi 14, chiavi struttura Casa della conoscenza, chiavi Centro giovanile, Rifugio della Chiusa, chiave di emergenza Teatro.	Possiede solo una copia della chiave di un accesso alla Casa della Conoscenza e agli uffici di Via Marconi 14; presso questi ultimi depositate le altre chiavi.
PANIERI MANUELA	ISTITUZIONE CASALECCHIO DELLE CULTURE	Chiave accesso uffici Istituzione via Marconi 14, chiavi struttura Casa della conoscenza, chiavi Centro giovanile, Rifugio della Chiusa, chiave di emergenza Teatro.	Possiede solo una copia della chiave di un accesso alla Casa della Conoscenza e agli uffici di Via Marconi 14; presso questi ultimi depositate le altre chiavi.
RUBBI MASSIMILIANO	ISTITUZIONE CASALECCHIO DELLE CULTURE	Chiave accesso uffici Istituzione via Marconi 14, chiavi struttura Casa della conoscenza, chiavi Centro giovanile, Rifugio della Chiusa, chiave di emergenza Teatro.	Possiede solo una copia della chiave di un accesso alla Casa della Conoscenza e agli uffici di Via Marconi 14; presso questi ultimi depositate le altre chiavi.
TROTTA MAURIZIO	ISTITUZIONE CASALECCHIO DELLE CULTURE	Chiave accesso uffici Istituzione via Marconi 14, chiavi struttura Casa della conoscenza, chiavi Centro giovanile, Rifugio della Chiusa, chiave di emergenza Teatro.	Possiede solo una copia della chiave di un accesso alla Casa della Conoscenza e agli uffici di Via Marconi 14; presso questi ultimi depositate le altre chiavi.

COGNOME E NOME	SERVIZIO/FUNZIONE	Struttura di cui si possiede la chiave di accesso	EVENTUALI NOTE
MANUTENCOOP	SOGGETTO ESTERNO CHE EFFETTUA LA PULIZIA DI CASA DELLA CONOSCECENZA E UFFICI VIA MARCONI 14	Chiave accesso uffici Istituzione via Marconi 14, chiavi struttura Casa della conoscenza, chiavi Centro giovanile, Rifugio della Chiusa, chiave di emergenza Teatro.	Possiede solo una copia della chiave di un accesso alla Casa della Conoscenza e agli uffici di Via Marconi 14; presso di essi depositate le altre chiavi.
EMILIA ROMAGNA TEATRO FONDAZIONE	SOGGETTO CHE EFFETTUA LA GESTIONE DEL TEATRO COMUNALE A. TESTONI	CHIAVI STRUTTURA TEATRO COMUNALE A. TESTONI	
COOP. LE MACCHINE CELIBI	SOGGETTO CHE EFFETTUA LA GESTIONE DEL CENTRO GIOVANILE	CHIAVI STRUTTURA CENTRO GIOVANILE BLOGOS	
ASSOCIAZIONE MICROMACCHINA	SOGGETTO ESTERNO CHE COORDINA LA WEB-RADIO E WEB-TV PRESSO IL CENTRO GIOVANILE	CHIAVE ACCESSO CENTRO GIOVANILE BLOGOS	
Bolognesi Stefano	Comandante	Locali P.M.	
Fantini Maurizio	Ispettore Capo	Locali P.M.	
Fabbri Fabio	Ispettore Capo	Locali P.M.	
Pacchioni Riccardo	Agente	Locali P.M.	
Mignani Monica	Vice Ispettore	Locali P.M.	
Toffaloni Paolo	Agente	Locali P.M.	
Florenzano Fausto	Assistente	Locali P.M.	
Maccanti Paola	Ispettore	Locali P.M.	
Boldrini Matteo	Agente	Locali P.M.	
Sperli Laura	Agente	Locali P.M.	
Ventura Andrea	Vice Ispettore	Locali P.M.	
Casadei Manuela	Agente	Locali P.M.	

COGNOME E NOME	SERVIZIO/FUNZIONE	Struttura di cui si possiede la chiave di accesso	EVENTUALI NOTE
Pace Emilia	Agente scelto	Locali P.M.	
Sandri Luca	Ispettore	Locali P.M.	
Fantini Giovanni	Agente	Locali P.M.	
Mora Valentina	Agente	Locali P.M.	
Fontana Roberta	Agente	Locali P.M.	
Dobboletta Maurizio	Vice Ispettore	Locali P.M.	
Evangelisti Daniele	Agente scelto	Locali P.M.	
Parrella Cristian	Agente	Locali P.M.	
Serafini Micaela	Vice Ispettore	Locali P.M.	
Gamberini Federica	Agente	Locali P.M.	
Mondello Vincenzo	Agente	Locali P.M.	
Migliorini Alessia	Agente scelto	Locali P.M.	
Bernardi Emma	Agente scelto	Locali P.M.	
Urbinati Lucia	Agente scelto	Locali P.M.	
COBIANCHI ALBERTO	SCUOLA/AMMINISTRATIVO D1	<p>ASILI NIDO: DON FORNASINI, MERIDIANA, FRANCO CENTRO, VIGHI, PICCOLE MAGIE, ZEBRI.</p> <p>SCUOLE DELL'INFANZIA: DOZZA, ARCOBALENO, RUBINI, LIDO, DON MILANI, CARAVAGGIO, VIGNONI, ESPERANTO.</p> <p>SCUOLE PRIMARIE: TOVOLI, CIARI, XXV APRILE, GARIBALDI, CARDUCCI.</p> <p>SCUOLA SECONDARIA DI PRIMO GRADO MORUZZI.</p> <p>CHIAVI DELLA BACHECA DELLE CHIAVI DEL MUNICIPIO.</p>	
GAMBERINI IRENE	NIDO/CUOCO B3	ASILO NIDO FRANCO CENTRO	
ZANOTTI MONICA	NIDO/OPERATORE B1	ASILO NIDO FRANCO CENTRO	

<b>COGNOME E NOME</b>	<b>SERVIZIO/FUNZIONE</b>	<b>Struttura di cui si possiede la chiave di accesso</b>	<b>EVENTUALI NOTE</b>
SABATTINI PATRIZIA	NIDO/OPERATORE B1	ASILO NIDO FRANCO CENTRO	
CAPODIFERRO MONICA	NIDO/OPERATORE B1	ASILO NIDO FRANCO CENTRO	
VIGHI ANNA MARIA	NIDO/EDUCATORE C1	ASILO NIDO FRANCO CENTRO	
SCAMANDRI BARBARA	NIDO/EDUCATORE C1	ASILO NIDO FRANCO CENTRO	
CARBOTTI ANTONIA	NIDO/EDUCATORE C1	ASILO NIDO FRANCO CENTRO	
STASI MARIELLA	NIDO/EDUCATORE C1	ASILI NIDO: MERIDIANA, PICCOLE MAGIE	
NOTO ROSALBA	NIDO/OPERATORE B1	ASILI NIDO: MERIDIANA, PICCOLE MAGIE	
MINGARELLI RITA	NIDO/OPERATORE B1	ASILO NIDO MERIDIANA	
MAESTRAMI SANDRA	NIDO/OPERATORE B1	ASILO NIDO MERIDIANA	
MARI ANGELA	NIDO/EDUCATORE C1	ASILO NIDO MERIDIANA	
DEGLI ESPOSTI PATRIZIA	NIDO/EDUCATORE C1	ASILO NIDO MERIDIANA	
MARSAN MANUELA	NIDO/EDUCATORE C1	ASILO NIDO MERIDIANA	
GRAGNOLINI ADELE	NIDO/EDUCATORE C1	ASILO NIDO MERIDIANA	
VENTURA LINA	NIDO/EDUCATORE C1	ASILI NIDO: MERIDIANA, PICCOLE MAGIE	
FANCHINI INES	NIDO/EDUCATORE C1	ASILO NIDO MERIDIANA	
DRAGONE DARIO	NIDO/OPERATORE B1	ASILO NIDO ZEBRI	
BERTONCELLI CRISTINA	NIDO/OPERATORE B1	ASILO NIDO ZEBRI	
ALBERI RITA	NIDO/OPERATORE B1	ASILO NIDO ZEBRI	
STANZANI MARISA	NIDO/CUOCO B3	ASILO NIDO ZEBRI	
MAMMARELLA ALFREDINA	NIDO/OPERATORE B1	ASILO NIDO ZEBRI	
TOMESANI ELISABETTA	NIDO/EDUCATORE C1	ASILO NIDO ZEBRI	
ARMIENTO LUISA	NIDO/EDUCATORE C1	ASILO NIDO ZEBRI	
BARONI PATRIZIA	NIDO/EDUCATORE C1	ASILO NIDO ZEBRI	

<b>COGNOME E NOME</b>	<b>SERVIZIO/FUNZIONE</b>	<b>Struttura di cui si possiede la chiave di accesso</b>	<b>EVENTUALI NOTE</b>
PEZZOLI PATRIZIA	NIDO/EDUCATORE C1	ASILO NIDO ZEBRI	
FANTI ANTONELLA	NIDO/EDUCATORE C1	ASILO NIDO ZEBRI	
MELOTTI GRAZIELLA	NIDO/EDUCATORE C1	ASILO NIDO ZEBRI	
PORCACCIO PATRIZIA	NIDO/OPERATORE B1	ASILO NIDO ZEBRI	
CAVICCHIOLI VALERIA	NIDO/EDUCATORE C1	ASILO NIDO ZEBRI	
BALESTRI SUSANNA	NIDO/EDUCATORE C1	ASILO NIDO PICCOLE MAGIE	
VIGNI NADIA	NIDO/EDUCATORE C1	ASILO NIDO PICCOLE MAGIE	
MARCHI RITA	NIDO/EDUCATORE C1	ASILO NIDO PICCOLE MAGIE	
FERO VALERIA	NIDO/OPERATORE B1	ASILO NIDO PICCOLE MAGIE	
COMERCI FONTINA	NIDO/OPERATORE B1	ASILO NIDO PICCOLE MAGIE	
PAVIGNANI PAOLA	NIDO/AUSILIARIO A1	ASILO NIDO PICCOLE MAGIE	
DEGLI ESPOSTI MANUELA	NIDO/EDUCATORE C1	ASILO NIDO PICCOLE MAGIE	
DONATI SIMONA	NIDO/CUOCO B3	ASILO NIDO DON FORNASINI	
CAPALDO ASSUNTA	NIDO/OPERATORE B1	ASILO NIDO DON FORNASINI	
SCHINELLI MARIA ROSA	NIDO/OPERATORE B1	ASILO NIDO DON FORNASINI	
GINNETTI CARMELINA	NIDO/EDUCATORE C1	ASILO NIDO DON FORNASINI	
ZANARDI ANNAMARIA	NIDO/OPERATORE B1	ASILO NIDO DON FORNASINI	
PICCININI NADIA	NIDO/EDUCATORE C1	ASILO NIDO DON FORNASINI	
NOTO ELENA	NIDO/OPERATORE B1	ASILO NIDO DON FORNASINI	
MONTOLLI MARIA KATIA	NIDO/EDUCATORE C1	ASILO NIDO DON FORNASINI	
ROMANO CONCETTINA	NIDO/OPERATORE B1	ASILO NIDO DON FORNASINI	
VENTURI LAURA	NIDO/OPERATORE B1	ASILO NIDO DON FORNASINI	
ALTINAR LIVIA RAMONA	NIDO/AUSILIARIO A1	ASILO NIDO DON FORNASINI	
MUSIANI ALESSIO	NIDO/EDUCATORE C1	ASILO NIDO DON FORNASINI	
LORENZANO MARIA	NIDO/EDUCATORE C1	ASILO NIDO DON FORNASINI	

COGNOME E NOME	SERVIZIO/FUNZIONE	Struttura di cui si possiede la chiave di accesso	EVENTUALI NOTE
PATRIZI ANTONELLA	NIDO/OPERATORE B1	ASILO NIDO VIGHI	
CALVARUSO GIUSEPPA	NIDO/OPERATORE B1	ASILO NIDO VIGHI	
LIDAKI ANNA	NIDO/OPERATORE B1	ASILO NIDO VIGHI	
GUIDORENI MARILENA	NIDO/EDUCATORE C1	ASILO NIDO VIGHI	
GAMBERINI PAOLA	NIDO/EDUCATORE C1	ASILO NIDO VIGHI	
ANDRISANI ANGELA	NIDO/EDUCATORE C1	ASILO NIDO VIGHI	
BELLONI FABIANA	NIDO/EDUCATORE C1	ASILO NIDO VIGHI	
BETELLI MARINA	NIDO/OPERATORE B1	ASILO NIDO VIGHI	
CIVALE ANTONIO	NIDO/OPERATORE B1	ASILO NIDO VIGHI	
CUSMA' PICCIONE SILVANA	NIDO/EDUCATORE C1	ASILO NIDO VIGHI	
RUGGERI NADIA	NIDO/EDUCATORE C1	ASILO NIDO VIGHI	
MARESCA GABRIELLA	NIDO/EDUCATORE C1	ASILO NIDO VIGHI	
MARCHI MARIA CHIARA	NIDO/EDUCATORE C1	ASILO NIDO VIGHI	
VASSALLO MARIA VALERIA	NIDO/EDUCATORE C1	ASILO NIDO VIGHI	
SCIANNA CATERINA	NIDO/EDUCATORE C1	ASILO NIDO VIGHI	
AMENTA VIRGINIA	NIDO/AUSILIARIO A1	ASILO NIDO VIGHI	
ISTITUTO DI VIGILANZA LA PATRIA	VIGILANZA	MUNICIPIO	
COFATECH	MANUTENIZIONE IMPIANTI DI CONDIZIONAMENTO E RISCALDAMENTO	MUNICIPIO E SEDI ESTERNE	
<b>Data di aggiornamento: 24/03/2010</b>			

## Analisi tecnologica dei dati elettronici

Presentiamo il disegno sintetico della rete del Comune di Casalecchio di Reno avente lo scopo di rappresentare a colpo d'occhio la rete dell'ente per capirne i punti critici e porre in essere le analisi successive.

### Lo schema generale della rete

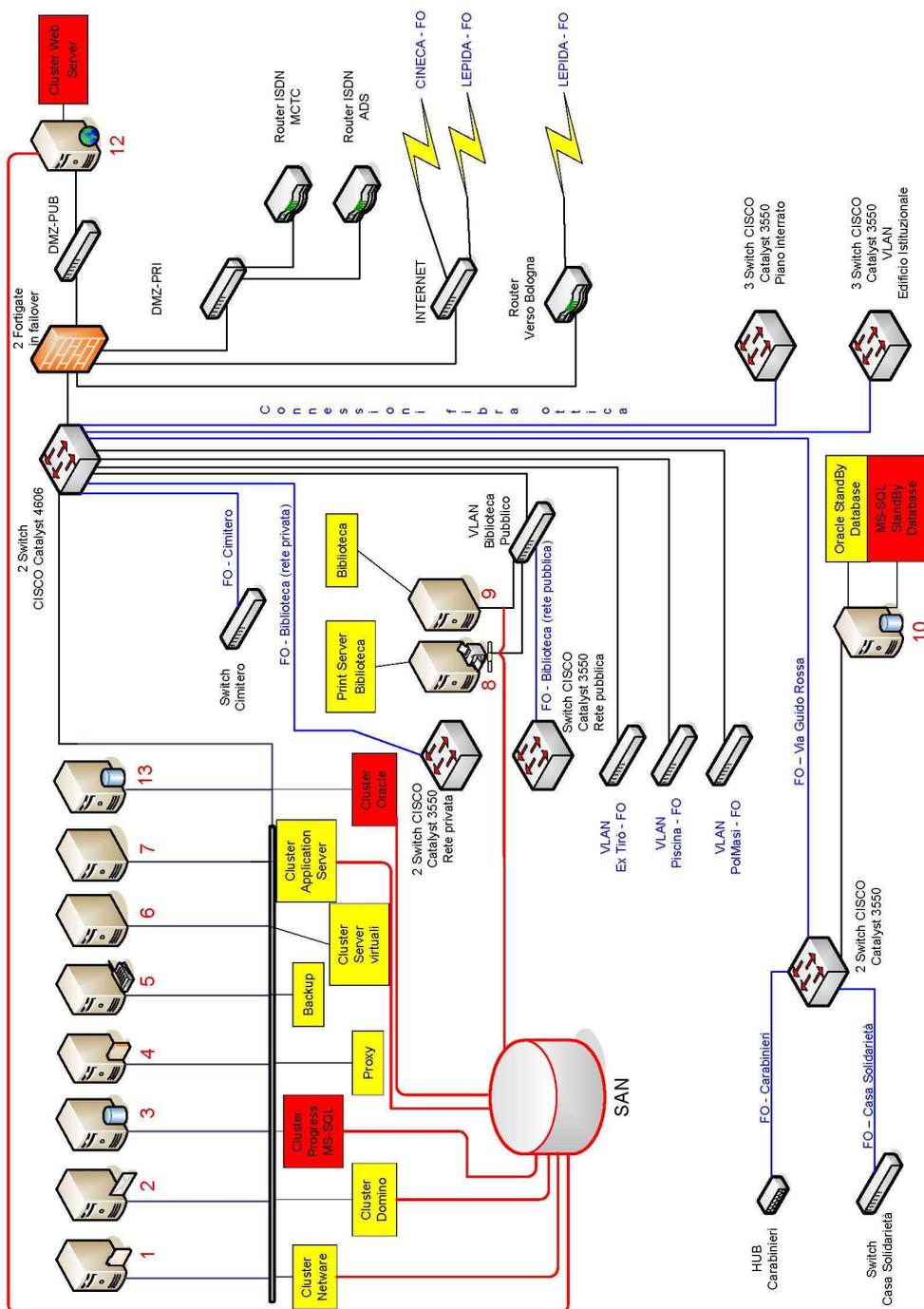


Figura 2: Il CED del Comune di Casalecchio di Reno



Dal punto di vista tecnologico il censimento dei beni da proteggere si identifica in un'attenta analisi della struttura informativa nel suo complesso partendo dal mezzo fisico per arrivare al trasporto ed allo stoccaggio dei dati. L'analisi sarà ripartita in sei aree di intervento:

- ✓ Analisi ambientale.
- ✓ Analisi del sistema di cablaggio.
- ✓ Analisi dell'architettura LAN e WAN.
- ✓ Analisi delle vulnerabilità interne e dell'accesso ai dati.
- ✓ Analisi delle applicazioni.
- ✓ Analisi delle comunicazioni verso Internet.
- ✓ Analisi dei servizi pubblicati sulla rete Internet.

### ***Analisi ambientale***

Obiettivo di questa sezione è l'analisi dello stato dei dati informatizzati, con particolare riguardo all'ambiente di ricovero degli stessi.

I dati sono tutti archiviati su server e nessuno di essi è presente sulle stazioni di lavoro PC dei singoli incaricati, se si eccettuano quelli dei posti di lavoro non in rete con il municipio ed i portatili. Tutti i server sono, a loro volta, custoditi nell'area CED.

L'area CED è ad accesso regolamentato e le persone autorizzate hanno accesso alla chiave della porta del CED stesso, chiave custodita dagli incaricati nominati nel gruppo "sistemi informativi" (Andrea Ventura, Alessandro Marchetti, Bruno Trebbi, Lisa Fini, Elisa Neretti, Barbara Buselli); una copia della stessa è custodita presso l'ufficio commessi.

I locali CED, come tutto l'edificio comunale, sono protetti da sistema anti-intrusione.

Per prevenire fenomeni di autocombustioni o autospegnimento il locale in cui è situato il CED è condizionato da un impianto in grado di raffreddare il locale in modalità ridondata. È programmata una temperatura fissa di 19 gradi massimi all'interno dello stesso locale. Il sistema di condizionamento è ridonato, ed in caso di superamento della



*segue*

temperatura programmata si attiva il combinatore telefonico che avvisa Ventura, Marchetti e Fini.

Infine l'impianto elettrico del CED è a norma, ed è protetto da un gruppo di continuità ridondato in grado di assicurare una autonomia complessiva all'impianto server di circa 25 minuti: non è previsto un sistemi di spegnimento automatico dei server. Non è presente un gruppo elettrogeno.

*Casi particolari: i posti di lavoro degli asili nido e del centro famiglie*

In queste sedi esistono dei PC locali con back-up autonomi gestiti dagli utenti

### ***Analisi del sistema di cablaggio***

Tutto il cablaggio è stato realizzato durante la costruzione dello stabile. e certificato in categoria 5 ed è in manutenzione alla società in house Adopera.

Gli armadi di cablaggio installati sono:

- tre armadi di cablaggio centrale nel Municipio collegati in fibra tra loro;
- un armadio di cablaggio presso ciascuna delle sedi remote

Tutti i sistemi di cablaggio sono mantenuti dalla società Adopera.

### ***Analisi dell'architettura LAN/WAN***

La scelta di analizzare in dettaglio le due architetture può sembrare, a prima vista, superflua, data la possibilità di desumerle dal disegno complessivo del sistema informativo dell'Ente. È utile, però, una scheda di sintesi.

#### *LAN*

L'architettura di LAN della sede del Municipio è basata su di una backbone Gigabit Ethernet, alla quale sono connessi i server e gli switch di piano, realizzata attraverso uno switch che offre anche la connettività fast ethernet verso:

- gli armadi remoti;
- gli switch di secondo livello che collegano tutta la periferia di personal computer e stampanti;

La struttura è comunque piuttosto semplice e provvedono alla sua manutenzione i seguenti fornitori:

1. ATS S.r.l. per tutta la parte di apparecchiature attive;
2. il personale dei servizi informativi con switch di ricambio disponibili nei locali del CED per le sedi interessate dal progetto.

Le fibre ottiche collegano la sede del Municipio con le altre sedi del comune. Tutte le fibre in oggetto sono state



*segue*

collaudate e certificate, e vengono mantenute da:

1. CINECA – collegamento Municipio-Cineca
2. AZIENDA INTERPELLATA ALL'OCCORRENZA – tutti gli altri collegamenti

WAN

Provvedono alla manutenzione della WAN i seguenti fornitori:

1. Tiscali per la connettività al Cineca con collegamento in fibra ottica, linee per le quali è fissato uno SLA (Service Level Agreement) di quattro ore massime per l'intervento;
2. Lepida per la connettività alla rete regionale delle Pubbliche Amministrazioni.
3. Acantho per la parte Hyperlan che collega alcuni asili nido con il municipio tranne la sede dell'ufficio cultura con la biblioteca che è in manutenzione ad Adopera stessa: per queste connessioni è fissato uno SLA (Service Level Agreement) di 16 ore lavorative massime per l'intervento;
4. 3CiME Technology Sistemi per gli apparati di interconnessione di tipo firewall, per i quali è fissato uno SLA (Service Level Agreement) di 4 ore lavorative massime per l'intervento;

### ***Analisi delle vulnerabilità interne e dell'accesso ai dati***

Specifichiamo ancora che in questa fase stiamo analizzando i dati archiviati su supporto informatico ed elettronico, mentre per quelli di tipo cartaceo rimandiamo l'analisi ad un paragrafo successivo.

Come in precedenza sottolineato, tutti i dati gestiti dall'ente sono archiviati su server, anche le caselle di posta elettronica dei singoli utenti, se si eccettuano i computer portatili: solo in modo transitorio possono lasciare traccia su di un posto di lavoro, ma devono, una volta utilizzati, e comunque a fine mansione, essere ritrasferiti sul server e cancellati dal posto di lavoro, pena l'assunzione da parte dell'operatore di tutte le responsabilità civili e penali derivanti dalla normativa.

Diverso è il discorso per le sedi distaccate, nelle quali non è presente un server, nelle quali non sono presenti, come detto precedentemente, alcun dato.

É importante qui sottolineare le regole di accesso ai dati da parte del personale dell'ente, che possono essere così riepilogate:

1. ogni incaricato ha diritto di accedere solamente ai dati che sono necessari per lo svolgimento delle proprie mansioni;
2. tutti i personal computer dell'ente hanno sistema operativo Windows 7, Windows XP o Windows 2000;



*segue*

3. ogni dipendente ha uno username, valido finché ha rapporti con l'ente, per l'accesso alla rete dell'ente stesso: lo username permette l'accesso alla rete Novell/Windows 200X, che è la base per l'accesso ai dati, e fornisce le credenziali anche per l'accesso ai file server. I server basati su altri sistemi operativi, o le specifiche applicazioni, come la posta elettronica o il software gestionale, richiedono di ridigitare specifici username e password. Viceversa l'accesso ad Internet non è regolamentato da uno username specifico in quanto integrato con il dominio Microsoft;
4. ad ogni username è associata una password per l'accesso ai server la cui scadenza è fissata in 90 giorni. I server Windows hanno la password a scadenza, mentre per le singole applicazioni deve essere il singolo utente che provvede in autonomia al cambio della password ogni 90 giorni;
5. in caso di assenza dell'utente, se è necessario accendere la sua stazione di lavoro per condividere la stampante collegata, basta accendere la macchina, la quale viene poi lasciata al Ctrl/Alt/Canc, stato sufficiente per la condivisione della stampante.

Da quanto riassunto si può quindi evincere che l'ente si è dotato di un sistema che offre un buon livello di sicurezza nell'accesso ai dati. È fatto comunque divieto a chiunque di portare all'esterno dati gestiti dal proprio servizio di appartenenza, sotto una qualunque forma, ad eccezione dei casi autorizzati previsti dal manuale di istruzione degli incaricati.

I Consiglieri Comunali e il gruppo del Consiglio Comunale hanno a disposizione un PC per ogni gruppo consigliere che usufruisce del collegamento ad Internet della rete del Municipio; detti utenti non hanno accesso al Dominio eDirectory dell'Amministrazione con diritti propri.

Gli Assessori ed il Presidente del Consiglio Comunale hanno invece anche accesso al dominio di rete.

La rete pubblica della Biblioteca è dotata di un proprio accesso ad Internet fisicamente indipendente dalla rete del Municipio.

I log di navigazione degli utenti secondo il decreto Pisanu sono storicizzati per sei mesi.

Alla Lan così separata della biblioteca potranno accedere anche:

- i cittadini utenti della biblioteca

### ***Analisi delle applicazioni: regola 19.8 dell'Allegato B al Codice***

Chi redige il documento ha approfondito lo stato dell'arte delle applicazioni gestionali installate nel comune e, anche a seguito di un confronto avuto con l'Avvocato Stefano Orlandi, in team con il quale viene redatto questo documento, esperto ed autore di pubblicazioni sull'argomento specifico, dobbiamo fare le seguenti considerazioni che valgono per le applicazioni software presenti nell'ente.

Tali applicazioni infatti paiono conformi ai seguenti punti del d.lgs. 196/2003 denominato "Codice sulla tutela dei dati



*segue*

personali”, anche in relazione a quanto dichiarato dai fornitori stessi:

1. Titolo III Art. 22 comma 6 recita: “I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.
2. Titolo III Art. 22 comma 7 recita: “I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici.

Il software, inoltre, pare conforme alle seguenti regole delle misure minime, anche secondo quanto dichiarato dai fornitori stessi (allegato B del d.lgs. in oggetto):

1. Art. 16 recita: I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-*quinquies* del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
2. Art. 17 recita: Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale

Tutti i dati comunali sono infatti protetti da sistema antivirus. L'amministratore ha predisposto un sistema antivirus sia sui client e sui server, sistema che dovrebbe ridurre al minimo tale rischio, ma che non può eliminarlo totalmente.



segue

Presentiamo di seguito un elenco di dettaglio dei software installati presso l'Ente

Tavola 10.riepilogativa del censimento dei software applicativi che rientrano nel piano di sicurezza dell'ente

<b>Prog.</b>	<b>Denominazione</b>	<b>Descrizione</b>	<b>Device o DB Server</b>
1.	Sinfecon	Pratiche delle attività produttive	dati sui server SQL
2.	Anagrafe del Comune di Bologna	Demografici (anagrafe, stato civile, saia, elettorale)	dati c/o Comune di Bologna
3.	Sebina	Biblioteca	Dati c/o CIB
4.	CG4	Controllo di gestione	dati sui server Oracle
5.	Babylon	Inventario	dati sui server SQL
6.	STR	Pratiche dei lavori pubblici	dati sui server SQL
7.	Mosaico	Contabilità lavori pubblici	dati sui server Progress
8.	Nettare	Gestione interventi lavori pubblici	dati sui server Oracle
9.	Serpico	Gestione giuridico-economica del personale – Contabilità - Cassa economale	dati sui server Progress
10.	JobTime	Gestione di timbrature e cartellini	dati sui server Oracle
11.	Polcity	Pratiche di polizia municipale	dati su Advantage Db Server
12.	Saturn	Gestione turni personale polizia municipale	con dati sui Db Access
13.	GS4PR	Protocollo	dati sui server Oracle
14.	GS4DE	Delibere e determine	dati sui server Oracle
15.	Sosia	Gestione rette scolastiche e servizi sociali	dati sui server Oracle
16.	Garsia	Servizi socio-sanitari	dati sui server Oracle
17.	Gradus	Graduatorie alloggi	con dati sui Db Access
18.	Tebit	Tributi e fiscalità locale	dati sui server Oracle



segue

<b>Prog.</b>	<b>Denominazione</b>	<b>Descrizione</b>	<b>Device o DB Server</b>
19.	Anagrafe Canina	Anagrafe canina	dati c/o la Regione Emilia Romagna
20.	Conedil	Pratiche dell'edilizia privata	dati su server Domino
21.	Articolo 12	Gestione cessione fabbricate	dati sui server Oracle
22.	Argo	Gestione accessi sportello polifunzionale	dati sui server SQL
23.	Surf	Gestione pratiche Sportello polizunfionale	dati sui server Oracle
24.	Amsefc	Gestione contratti cimiteriali	dati sui server Progress
25.	Utenze	Gestione utenze	dati su server Domino
26.	Carburanti	Gestione veicoli	dati su server Domino
27.	Oggetti Smarriti	Gestione oggetti smarriti	dati su server Domino
28.	Contratti	Gestione gare di acquisto e relativi contratti	dati su server Domino
29.	Sinistri Assicurativi	Gestione pratiche di risarcimento danni	dati su server Domino
30.	Entratel	Invio comunicazioni INPDAP all'Agenzia delle Entrate	Procedura stand-alone
31.	Sare	Invio comunicazioni assunzioni e cessazioni al centro per l'impiego	Procedura stand-alone
32.	GE770	Invio 770 all'Agenzia delle Entrate	Procedura stand-alone
33.	F24	Invio F24 all'Agenzia delle Entrate	Procedura stand-alone
34.	Programma pensioni		
35.	Extrafax	Gestione fax server integrato	dati su server Domino
36.	Sophos	Antivirus	
37.	Termthalc	Acquisizione marcature marcatempo	
38.	Time Navigator	Backup	



*segue*

<b>Prog.</b>	<b>Denominazione</b>	<b>Descrizione</b>	<b>Device o DB Server</b>
39.	Lotus Domino	Posta elettronica, bacheche, diari	Server Domino
	<b>Data di aggiornamento: 26/03/2010</b>		



segue

## ***Analisi delle comunicazioni verso Internet***

Tutte le comunicazioni verso Internet passano attraverso il collegamento con il provider Tiscali e la rete regionale LEPIDA: tale connessione è basata su tecnologia in fibra ottica a 100 MBit nominali presente nella sede del Municipio. L'ente si è dotato di tutta la strumentazione necessaria per ridurre al minimo i rischi di intrusione nonché di fuoriuscite di dati non autorizzate verso la rete.

Per prima cosa è opportuno presentare sinteticamente la struttura di comunicazione, meglio descritta dall'immagine presentata in precedenza:

- il server di posta elettronica è interno e completamente gestito dai Servizi Informativi;
- tutti gli utenti autorizzati possono navigare in Internet;
- la rete interna è divisa dalla rete pubblica da un firewall cauterizzato (Fortigate ridondato), che gestisce anche i log di connessione degli utenti (della cui esistenza gli utenti sono informati nel manuale di formazione utente), attraverso l'appliance Fortianlyzer, nel quale sono fissate le seguenti regole:
  - porte aperte in uscita: http, https, smtp, pop3, ftp, ed altre porte di servizio;
  - porte aperte in ingresso: http, https, pop3, (posta in relay), ftp verso un'area specifica, siti web in reverse proxy e web mail + altre porte di servizio per problematiche specifiche

E' necessario ora riepilogare i servizi attivi:

- tutti gli utenti dotati di personal computer hanno la posta elettronica, con possibilità di inviare/ricevere allegati con la dimensione massima di 5 MB: questo servizio è funzionale allo svolgimento della propria mansione, secondo quanto stabilito nel disciplinare Internet;
- navigazione in Internet secondo quanto detto nello specifico disciplinare Internet redatto nel primo trimestre del 2008 ed aggiornato annualmente;

Una parte consistente di quanto sopra riportato è riaffermato nella "Politica di sicurezza dell'ente", che sarà illustrata successivamente.

## ***Analisi dei servizi pubblicati sulla rete Internet***

I servizi pubblicati sulla rete Internet sono numericamente ristretti, ma vale ugualmente la pena citarli per meglio comprendere il loro impatto sulla sicurezza dei dati:

1. Il primo servizio pubblicato, ma di scarsa importanza ai fini della sicurezza, è dato dalle pagine web di presentazione dell'ente, raggiungibili al link [www.comune.casalecchio.bo.it](http://www.comune.casalecchio.bo.it).



*segue*

2. Portale degli atti amministrativi
3. Albo pretorio
4. Iscrizione dei fornitori
5. Portale Istituzionale
6. Portale dei tributi
7. Extranet per accesso remoto alle applicazioni dell'ente
8. Web-mail
9. Garsia.We invece è un servizio di FTP, verso la ASL Città di Bologna via Internet, di dati: i dati sono aggiornati dagli operatori del comuni ed il sistema provvede ad aggiornarli nella sede dell'ASL. I dati sono oggetto di back-up sia all'interno dell'ente che all'interno dell'ASL
10. Portale delle Associazioni di Volontariato e Gruppi Consiliari
11. Portale della rete WI-FI
12. Sportello Edilizia Privata

Non sono presenti altri servizi applicativi pubblicati.



## **Analisi dei dati cartacei**

### ***Analisi ambientale***

Le operazioni di trattamento dei dati cartacei avvengono negli uffici e/o reparti dove lavorano gli incaricati. Ogni ufficio è dotato di contenitori muniti di chiave nei quali riporre i dati personali sensibili e giudiziari, come indicato dal manuale di istruzioni fornito agli incaricati.

Ogni ufficio è ad accesso regolamentato, nel senso che le porte della sede di riferimento si aprono solo grazie al “via libera” fornito dalla chiave in possesso del incaricati.

Nella tabella chiavi successivamente riportata successivamente invece sono evidenziati quegli incaricati che hanno accesso alle sedi in modalità autonoma. I singoli incaricati possono anche accedere, dietro autorizzazione del responsabile di reparto/ufficio, in ambienti diversi da quelli di lavoro ordinario.

### ***Analisi delle vulnerabilità interne e dell'accesso dei dati***

I rischi a cui sono soggetti i dati cartacei trattati dall'ente sono quelli tradizionali:

- sottrazione di documenti da parte del personale
- mancata reposizione dei dati trattati sotto chiave, quindi la mancata osservazione delle istruzioni impartite agli incaricati.



## Le criticità dei beni informatici preposti al trattamento dei dati elettronici

L'analisi della criticità dei beni riguarda esclusivamente la dotazione informatica preposta al trattamento dei dati elettronici.

Occorre precisare che l'analisi è indirizzata a misurare la criticità della disponibilità dei dati, di conseguenza oggetto di analisi sono i beni informatici in quanto consentono la disponibilità dei dati stessi.

Tale analisi è effettuata sotto due punti di vista:

- il *fault tolerance*: questa analisi, che nel presente lavoro sarà particolarmente approfondita, si può desumere implicitamente dalla lettura dell'Allegato B del d.lgs n. 196/03 "Codice in materia di protezione dei dati personali" dove si sancisce la necessità di garantire la "disponibilità dei dati";
- il *disaster recovery*: questa seconda analisi rientra tra le misure minime dell'Allegato B del d.lgs n.196/03 "Codice in materia di protezione dei dati personali".

### ***Il fault tolerance***

La strategia di *fault tolerance* è data da tutti quegli accorgimenti che permettono di garantire la continuità del servizio informatico. Tale strategia assume notevole rilevanza nel trattamento dei dati dell'ente e soprattutto nelle necessità di garantire la continuità del servizio. Il Comune di Casalecchio di Reno è infatti una realtà che offre un pubblico servizio. Di conseguenza tutti i fattori volti a garantire al massimo la continuità di lavoro, rivestono una importanza decisiva o, addirittura, vitale.

Per procedere a questa prima analisi occorre innanzitutto definire il livello di criticità di ciascun bene informatico (da ora in poi denominato *device*), per poterlo poi classificare e successivamente definire le azioni da intraprendere per affrontare i possibili fermi macchina.

E' possibile ipotizzare una scala di criticità che va da 1 a 4 così definita:

1. *minimo*: i device possono stare fermi anche una settimana senza che si riscontrino problemi all'intero sistema informativo;
2. *intermedia*: il device può stare fermo per una settimana senza problemi all'intero sistema informativo, tranne che in periodi critici di eccesso di lavoro, nel quale le possibilità di fermo si riducono a 8 ore lavorative;
3. *alta*: il device non può, in qualunque situazione stare fermo per più di 8 ore lavorative (24 ore solari);
4. *critica*: il device non può stare fermo per più di 4 ore lavorative.

Occorre, in primo luogo, definire la criticità di tutti i device sotto elencati per elaborare una strategia di intervento efficace a coprire le esigenze di *fault tolerance*.



segue

Tavola 11.: Tabella riepilogativa dei device presenti nell'ente: censimento dei beni informatici

Servizi funzionali										
Device	File server	Altri server	DB Server gestionale	E-mail	Apps gestionali	Servizi di gestione	Router o switch	Marca	S.O	F.T.
<b>Municipio Via dei Mille, 9</b>										
Cluster6-n1				3				HP	Windows Server 2003	Cluster Domino
Cluster6-n2				2				HP	Windows Server 2003	Cluster Domino
Cluster4-n1	4					E-directory		HP	Novell Netware 6.5	Cluster Netware
Cluster4-n2	2					E-directory		HP	Novell Netware 6.5	Cluster Netware
NwPrint						4 Printer Server - Identity Manager		HP	Novell Netware 6.5	Cluster Netware
Cluster5-n1			4					HP	Linux RedHat + Oracle	Cluster Linux
Cluster5-n2			2					HP	Linux RedHat + Oracle	Cluster Linux
Cluster8-n1			4					HP	Windows Server 2003 + Ms-Sql DB	Cluster Microsoft
Cluster8-n2			4					HP	Windows 2000 Server + Progress DB	Cluster Microsoft
Cluster7-n1		4						HP	Windows Server 2003	Cluster Microsoft + IIS + Apache web server
Cluster7-n2		2						HP	Windows Server 2003	Cluster Microsoft + IIS + Apache web server
WebLab						3 Reverse Proxy		HP	Windows Server 2003	Raid 5
Webapp01					3			HP	Linux	Raid 5



segue

Servizi funzionali										
Device	File server	Altri server	DB Server gestionale	E-mail	Apps gestionali	Servizi di gestione	Router o switch	Marca	S.O	F.T.
Webapp02					3			HP	Linux	Raid 5
Castor						4 PDC - DNS - DHCP		HP	Windows Server 2003	Macchina Citrix XenServer
Pollux						2 PDC - DNS - DHCP		Server virtuale	Windows Server 2003	HA e Motion Citrix XenServer
Patch						3 WSUS		Server virtuale	Windows Server 2003	HA e Motion Citrix XenServer
Perseus						3 Backup Server		HP	Windows Server 2003	Raid 5
Titano						3 PDC - DNS - DHCP biblioteca		HP	Windows Server 2003	Raid 5
Hiperstream						2 Deduplica backup		Server virtuale	Windows Server 2003	HA e Motion Citrix XenServer
Winwkf						2		Server virtuale	Windows Server 2003	HA e Motion Citrix XenServer
Centralino		4						Server virtuale	Fedora	HA e Motion Citrix XenServer
TestLab			2 Oracle - SIT					HP	Windows Server 2003	Raid 5
Gespage						2 Printer Server Biblioteca		HP	Linux Fedora	Raid 5
Server		2						HP	Windows Server 2003	Raid 1
Fortigate 01						4 Firewall		Fortinet	N.a.	Cluster
Fortigate 02						2 Firewall		Fortinet	N.a.	Cluster
FortiAnalyzer						2 Log di navigazione		Fortine	N.a.	Nessuno
Router vari							4	CISCO	CISCO IOS	/
Apparecchiature rete HyperLan							4	Varie		/
Switch vari							4	CISCO	CISCO IOS	/



segue

Servizi funzionali										
Device	File server	Altri server	DB Server gestionale	E-mail	Apps gestionali	Servizi di gestione	Router o switch	Marca	S.O	F.T.
<b>Magazzino – Via Guido Rossa, 1-3</b>										
OraStdb			2					HP	Linux RedHat + Oracle	Oracle Standby DB
Cluster8-stdb			2					HP	Windows Server 2003	Microsoft MS-Sql Standby DB
Switch vari	☹	☹	☹	☹	☹	☹	4	Vari	n.a.	
<b>Altre sedi</b>										
Router							4	CISCO	CISCO IOS	/
Apparecchiature rete HyperLan							4	Varie		/
Switch vari							4	Vari	n.a.	Nessuno
<b>Data di aggiornamento: 15/03/2010</b>										

#### Legenda

I numeri indicati nelle celle evidenziate in giallo indicano il fattore di criticità riepilogato sede per sede (i numeri sono assegnati sulla base della scala di criticità prima esplicitata).

F.T. sta per Fault Tolerance

Con i simboli rossi è indicato, invece, l'impatto che un eventuale fault del device può avere sui servizi in ordinata.

#### Il disaster recovery

Analizzare le problematiche di disaster recovery è molto più complesso in quanto i problemi da affrontare sono molteplici:

Innanzitutto bisogna rifare un'analisi di criticità orientata specificamente ai server, ed una orientata alle linee di comunicazione, in quanto i termini sono differenti da quelli usati per lo studio precedente: possiamo però rifarci all'elenco sopra riportato per un censimento dei server e dei collegamenti WAN.

Occorre, innanzitutto, definire i fattori di criticità relativi alle problematiche di disaster recovery allo scopo di stabilire una scala di importanza dei dati/applicazioni/conessioni, in quanto non è possibile pensare di assegnare lo stesso fattore di importanza a tutti i servizi. Anche in questo caso è congeniale ipotizzare una scala di criticità che proceda da 1 a 2 così definita:

1. *minimo*: questi server/link non contengono dati d'importanza vitale per l'ente, o, in altre parole, contengono dati per i quali è possibile aspettare le normali operazioni di *restore*, dai nastri di back-up che saranno



segue

depositati “al sicuro” con periodicità da definire, o di *ripristino* da normali operazioni di assistenza;

2. *critica*: questi server/link contengono dati d’importanza vitale per l’attività produttiva dell’ente e devono essere ripristinati immediatamente in una locazione diversa da quella che ha subito il disastro, con uno switch il più possibile automatizzato;

Occorre quindi definire la criticità di tutti i device sotto elencati per elaborare una strategia di intervento efficace a coprire le esigenze di disaster recovery.

Tavola 12.: Tabella riepilogativa dei fattori di criticità per il servizio di disaster recovery

Servizi funzionali										
Device	File server	Altri server	DB Server gestionale	E-mail	Apps gestionali	Servizi di gestione	Router o switch	Marca	S.O	F.T.
<b>Municipio Via dei Mille, 9</b>										
Cluster6-n1				2				HP	Windows Server 2003	Cluster Domino
Cluster6-n2				1				HP	Windows Server 2003	Cluster Domino
Cluster4-n1	2		☺☺	☺☺		E-directory		HP	Novell Netware 6.5	Cluster Netware
Cluster4-n2	1		☺☺	☺☺		E-directory		HP	Novell Netware 6.5	Cluster Netware
NwPrint						2 Printer Server - Identity Manager		HP	Novell Netware 6.5	Cluster Netware
Cluster5-n1			2					HP	Linux RedHat + Oracle	Cluster Linux
Cluster5-n2			1					HP	Linux RedHat + Oracle	Cluster Linux
Cluster8-n1			2					HP	Windows Server 2003 + Ms-Sql DB	Cluster Microsoft
Cluster8-n2			2					HP	Windows 2000 Server + Progress DB	Cluster Microsoft
Cluster7-n1		2						HP	Windows Server 2003	Cluster Microsoft + IIS + Apache web server



segue

Servizi funzionali										
Device	File server	Altri server	DB Server gestionale	E-mail	Apps gestionali	Servizi di gestione	Router o switch	Marca	S.O	F.T.
Cluster7-n2		1						HP	Windows Server 2003	Cluster Microsoft + IIS + Apache web server
WebLab				☺☺☺		2 Reverse Proxy		HP	Windows Server 2003	Raid 5
Webapp01					2			HP	Linux	Raid 5
Webapp02					1			HP	Linux	Raid 5
Castor	☺☺☺	☺☺☺	☺☺☺	☺☺☺	☺☺☺	2 PDC - DNS - DHCP		HP	Windows Server 2003	Macchina Citrix XenServer
Pollux						1 PDC - DNS - DHCP		Server virtuale	Windows Server 2003	HA e Motion Citrix XenServer
Patch						2 WSUS		Server virtuale	Windows Server 2003	HA e Motion Citrix XenServer
Perseus	☺☺☺	☺☺☺	☺☺☺	☺☺☺	☺☺☺	2 Backup Server		HP	Windows Server 2003	Raid 5
Titano						1 PDC - DNS - DHCP biblioteca		HP	Windows Server 2003	Raid 5
Hiperstream						1 Deduplica backup		Server virtuale	Windows Server 2003	HA e Motion Citrix XenServer
Winwkf						1		Server virtuale	Windows Server 2003	HA e Motion Citrix XenServer
Centralino		2						Server virtuale	Fedora	HA e Motion Citrix XenServer
TestLab			1 Oracle - SIT					HP	Windows Server 2003	Raid 5
Gespage						1 Printer Server Biblioteca		HP	Linux Fedora	Raid 5
Server		1						HP	Windows Server 2003	Raid 1
Fortigate 01				☺☺☺		2 Firewall		Fortinet	N.a.	Cluster



segue

Servizi funzionali										
Device	File server	Altri server	DB Server gestionale	E-mail	Apps gestionali	Servizi di gestione	Router o switch	Marca	S.O	F.T.
Fortigate 02				☺☺		1 Firewall		Fortinet	N.a.	Cluster
FortiAnalyzer						1 Log di navigazione		Fortinet	N.a.	Nessuno
Router vari							2	CISCO	CISCO IOS	/
Apparecchiature rete HyperLan							2	Varie		/
Switch vari	☺☺	☺☺	☺☺	☺☺	☺☺	☺☺	2	CISCO	CISCO IOS	/
<b>Magazzino – Via Guido Rossa, 1-3</b>										
OraStdb			1					HP	Linux RedHat + Oracle	Oracle Standby DB
Cluster8-stdb			1					HP	Windows Server 2003	Microsoft MS-Sql Standby DB
Switch vari	☺☺	☺☺	☺☺	☺☺	☺☺	☺☺	2	Vari	n.a.	
<b>Altre sedi</b>										
Router							2	CISCO	CISCO IOS	/
Apparecchiature rete HyperLan							2	Varie		/
Switch vari							2	Vari	n.a.	Nessuno
<b>Data di aggiornamento: 15/03/2010</b>										

*Legenda*

I numeri indicati nelle celle evidenziate in giallo indicano il fattore di criticità riepilogato sede per sede (i numeri sono assegnati sulla base della scala di criticità prima esplicitata).

F.T. sta per Fault Tolerance

Con i simboli blu è indicato, invece, l'impatto che una mancanza del device può avere sui servizi in ordinata.



## **L'analisi dei rischi a cui possono essere soggetti i dati elettronici e i dati cartacei: regola 19.3 dell'Allegato B al Codice**

In linea con l'art. 35, Capo I, Titolo V del d.lgs. n. 196/2003 che “*impone di ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta*” si procede analizzando i rischi a cui sono soggetti i dati informatici ed i dati cartacei trattati dagli incaricati dell'ente.

Per ciò che concerne le azioni intraprese per fronteggiare tali rischi si rimanda al capitolo relativo al *Documento Programmatico per la sicurezza dei dati*.

### ***Analisi dei rischi dei dati elettronici***

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

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



segue

Presentazione sintetica dei rischi a cui sono soggetti i dati elettronici trattati dal Comune di Casalecchio di Reno.

Tavola 13.: I rischi a cui sono soggetti i dati elettronici trattati dal Comune di Casalecchio di Reno sono di seguito riepilogati:

Rischio	Dettaglio	Gravità stimata	Probabilità di accadimento
<u>Accesso indebito alle risorse da parte di utenti interni all'ente</u>	<ul style="list-style-type: none"><li>• Accesso alle banche dati non autorizzato.</li><li>• Copie non autorizzate dei dati per il trasporto all'esterno dell'ente</li></ul>	<ul style="list-style-type: none"><li>○ Alta</li><li>○ Alta</li></ul>	<ul style="list-style-type: none"><li>○ Bassa</li><li>○ Media</li></ul>
<u>Comportamenti degli operatori</u>	<ul style="list-style-type: none"><li>• Furto di credenziali di autenticazione</li><li>• carenza di consapevolezza, disattenzione o incuria</li><li>• comportamenti sleali o fraudolenti</li><li>• errore materiale</li></ul>	<ul style="list-style-type: none"><li>○ Alta</li><li>○ Alta</li><li>○ Alta</li><li>○ Media</li></ul>	<ul style="list-style-type: none"><li>○ Bassa</li><li>○ Bassa</li><li>○ Bassa</li><li>○ Bassa</li></ul>
<u>Eventi relativi agli strumenti</u>	<ul style="list-style-type: none"><li>• azione di <i>virus</i> informatici o di codici malefici</li><li>• spamming o altre tecniche di sabotaggio</li><li>• malfunzionamento, indisponibilità o degrado degli strumenti</li></ul>	<ul style="list-style-type: none"><li>○ Alta</li><li>○ Alta</li><li>○ Media</li></ul>	<ul style="list-style-type: none"><li>○ Media</li><li>○ Media</li><li>○ Media</li></ul>
<u>Eventi relativi al contesto</u>	<ul style="list-style-type: none"><li>• accessi non autorizzati a locali/reparti ad accesso ristretto</li><li>• Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ...)</li></ul>	<ul style="list-style-type: none"><li>○ Media</li><li>○ Alta</li></ul>	<ul style="list-style-type: none"><li>○ Bassa</li><li>○ Media</li></ul>



segue

<b>Rischio</b>	<b>Dettaglio</b>	<b>Gravità stimata</b>	<b>Probabilità di accadimento</b>
<u>Sicurezza nelle trasmissioni</u> dei dati	<ul style="list-style-type: none"><li>• Tentativi di carpire i dati che vengono inviati all'ente da parte di pirati esterni.</li><li>• Tentativi di carpire i dati che vengono spediti dal Comune di Casalecchio di Reno da parte di pirati esterni.</li><li>• Rischio di invio dati a destinatari sbagliati.</li><li>• Tentativi di intrusione nella rete interna dell'ente, dall'esterno, da Internet, da sedi di comuni collegati via linee telefoniche all'ente e da parte di pirati esterni.</li></ul>	<ul style="list-style-type: none"><li>○ Alta</li><li>○ Alta</li><li>○ Bassa</li><li>○ Alta</li></ul>	<ul style="list-style-type: none"><li>○ Media</li><li>○ Media</li><li>○ Bassa</li><li>○ Media</li></ul>
<u>Rischi circa l'integrità fisica</u> dei dati	<ul style="list-style-type: none"><li>• Cancellazione involontaria/accidentale dei dati.</li><li>• Servizi di back-up non andati a buon fine.</li></ul>	<ul style="list-style-type: none"><li>○ Bassa</li><li>○ Bassa</li></ul>	<ul style="list-style-type: none"><li>○ Bassa</li><li>○ Bassa</li></ul>
<u>Rischi circa l'integrità logica</u> dei dati	<ul style="list-style-type: none"><li>• Incongruenze fra i dati.</li><li>• Le applicazioni software in uso che creano disallineamenti.</li></ul>	<ul style="list-style-type: none"><li>○ Bassa</li><li>○ Bassa</li></ul>	<ul style="list-style-type: none"><li>○ Bassa</li><li>○ Bassa</li></ul>
Rischi <u>manomissioni o furti o azioni dolose</u>	<ul style="list-style-type: none"><li>• Manomissioni del CED.</li><li>• Furti di dati sia dagli elaboratori, che degli elaboratori stessi.</li></ul>	<ul style="list-style-type: none"><li>○ Alta</li><li>○ Alta</li></ul>	<ul style="list-style-type: none"><li>○ Bassa</li><li>○ Bassa</li></ul>
<u>Eventi dannosi o disastrosi</u>	<ul style="list-style-type: none"><li>• Incendio.</li><li>• Terremoti, alluvioni ed ogni altro evento non prevedibile.</li></ul>	<ul style="list-style-type: none"><li>○ Alta</li><li>○ Impredicibile</li></ul>	<ul style="list-style-type: none"><li>○ Media</li><li>○ Alta</li></ul>



segue

## Analisi dei rischi dei dati cartacei

I rischi ai quali possono essere soggetti i dati cartacei presenti nell'ente sono i seguenti:

- Accesso indebito alle risorse sia da parte di personale interno non autorizzato.
- Rischi connessi alla trasmissione dei dati.
- Perdita dei dati e quindi perdita della loro integrità fisica.
- Furti e azioni dolose.
- Eventi dannosi o disastrosi.
- Rischi connessi alla procedura di eliminazione di dati erroneamente stampati.

*Presentazione sintetica dei rischi a cui possono essere soggetti i dati cartacei trattati dall'ente*

*Tavola 14.: I rischi a cui possono essere soggetti i dati cartacei trattati dall'ente possono essere così riepilogati:*

<b>Rischio</b>	<b>Dettaglio</b>	<b>Gravità stimata</b>	<b>Probabilità di accadimento</b>
<u>Accesso indebito alle risorse da parte di utenti interni</u> all'ente	<ul style="list-style-type: none"> <li>• Accesso alle banche dati non autorizzato.</li> <li>• Copie non autorizzate dei dati per il trasporto all'esterno dell'ente</li> </ul>	<ul style="list-style-type: none"> <li>○ Alta</li> <li>○ Alta</li> </ul>	<ul style="list-style-type: none"> <li>○ Bassa</li> <li>○ Media</li> </ul>
<u>Comportamenti degli operatori</u>	<ul style="list-style-type: none"> <li>• Carenza di consapevolezza, disattenzione o incuria</li> <li>• comportamenti sleali o fraudolenti</li> <li>• errore materiale</li> </ul>	<ul style="list-style-type: none"> <li>○ Alta</li> <li>○ Alta</li> <li>○ Media</li> </ul>	<ul style="list-style-type: none"> <li>○ Bassa</li> <li>○ Bassa</li> <li>○ Bassa</li> </ul>
<u>Eventi relativi al contesto</u>	<ul style="list-style-type: none"> <li>• accessi non autorizzati a locali/reparti ad accesso ristretto</li> <li>• Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ...)</li> </ul>	<ul style="list-style-type: none"> <li>○ Media</li> <li>○ Alta</li> </ul>	<ul style="list-style-type: none"> <li>○ Bassa</li> <li>○ Media</li> </ul>



segue

<b>Rischio</b>	<b>Dettaglio</b>	<b>Gravità stimata</b>	<b>Probabilità di accadimento</b>
<u>Sicurezza nelle trasmissioni</u> dei dati	<ul style="list-style-type: none"><li>• Rischio di invio dati a destinatari sbagliati.</li></ul>	<input type="radio"/> Bassa	<input type="radio"/> Bassa
<u>Rischi circa l'integrità fisica</u> dei dati	<ul style="list-style-type: none"><li>• Cancellazione involontaria/accidentale dei dati</li></ul>	<input type="radio"/> Bassa	<input type="radio"/> Bassa
<u>Eventi dannosi o disastrosi</u>	<ul style="list-style-type: none"><li>• Incendio.</li><li>• Terremoti, alluvioni ed ogni altro evento non prevedibile.</li></ul>	<input type="radio"/> Alta <input type="radio"/> Impredicibile	<input type="radio"/> Media <input type="radio"/> Alta
<u>Rischi connessi alla procedura di eliminazione di dati erroneamente stampati</u>	<ul style="list-style-type: none"><li>• Mancata distruzione dei dati erroneamente stampati dagli incaricati</li></ul>	<input type="radio"/> Alta	<input type="radio"/> Bassa

## L'analisi dei sistemi di videosorveglianza

In linea con quanto previsto dal Garante per la protezione dei dati personali, nonché dalla Convenzione europea sui diritti dell'uomo, il trattamento dei dati attraverso sistemi di videosorveglianza avviene rispettando i seguenti principi legislativi, sanciti anche dal regolamento interno:

- principio di liceità: non sono ammissibili interferenze illecite nella vita privata, di tutela della dignità, dell'immagine, del domicilio e di tutti gli altri luoghi ai quali è riconosciuta analoga tutela (tali limitazioni si aggiungono a quelle già previste dal c.p. in materia di intercettazioni di comunicazioni e di conversazioni);
- principio di necessità: un sistema di videosorveglianza introduce un vincolo per il cittadino in termini di limitazioni o condizionamenti, di conseguenza si deve escludere ogni uso superfluo o eccessivo;
- principio di proporzionalità: l'ente o l'impresa deve valutare innanzitutto il grado di rischio in cui può incorrere e adottare un sistema di videosorveglianza solo quando le altre misure si rivelano insufficienti; la soluzione che porta all'adozione di un sistema di videosorveglianza non deve rispondere a meri criteri di risparmio o di semplicità;
- principio di finalità: con l'introduzione di sistemi di videosorveglianza possono essere perseguite solo finalità trasparenti e portate opportunamente a conoscenza del pubblico mediante comunicazioni o cartelli, escludendo qualsiasi finalità generiche o indeterminate.

Tavola 15.: Tabella riepilogativa dei sistemi di videosorveglianza

Progressivo	Dislocazione e scopo	Registrazione
1.	Municipio (4 telecamere)	Collegate con Istituto di Vigilanza "La Patria"
2.	Stazione Garibaldi	Registrazione su server in Municipio
3.	Piazza del Popolo	Registrazione su server in Municipio
4.	Parco della Chiusa - Montagnola di Mezzo (2 telecamere)	Registrazione su server in Municipio
Data di aggiornamento: 25/03/2010		



*segue*

## ***Adempimenti ottemperati adottati nel regolamento interno***

### ***DOVERE DI INFORMAZIONE***

Gli interessati sono informati con formule sintetiche, ma chiare e senza ambiguità, che stanno per accedere o che si trovano in una zona videosorvegliata e dell'eventuale registrazione anche se si tratta di eventi, di spettacoli pubblici o di attività pubblicitarie.

### ***MISURE DI SICUREZZA***

Quando i dati vengono conservati sono previsti, all'interno della struttura, diversi livelli di accesso al sistema e di utilizzo delle informazioni, avendo riguardo anche agli interventi ordinari e straordinari di manutenzione. La risposta adottata al rischio che si verifichino abusi è stata l'introduzione di una "doppia chiave" fisica o logica che consente un'immediata ed integrale visione delle immagini solo in caso di necessità.

Sono previste iniziative periodiche di formazione degli incaricati sui doveri, sulle garanzie e sulle responsabilità, sia nel momento dell'introduzione del sistema di videosorveglianza, sia in sede di modifica dello stesso.

Le misure di sicurezza riducono al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta.

### ***DURATA DELL'EVENTUALE CONSERVAZIONE***

In linea con il principio di proporzionalità anche l'eventuale conservazione temporanea è commisurata al grado di indispensabilità e per il solo tempo necessario a raggiungere la finalità perseguita.

La conservazione è a poche ore o, al massimo, alle 24 ore successive alla rilevazione, fatte salve speciali esigenze in relazione a festività o chiusura di uffici, a richieste dell'autorità giudiziaria, a speciali esigenze tecniche o per la particolare rischiosità dell'attività svolta dal titolare. In quest'ultimo caso il termine più ampio di conservazione dei dati non può comunque superare la settimana.



segue

## La definizione della politica di sicurezza dell'ente

È la fase organizzativa più importante e delicata da affrontare, che vede coinvolti il redattore del presente progetto con il responsabile di progetto incaricato dal Comune di Casalecchio di Reno.

Occorre precisare che per quanto riguarda la gestione dei dati sensibili e giudiziari su supporto cartaceo vale la regola generale, condivisa dall'intera organizzazione ed opportunamente esplicitata nel manuale di istruzione dei diversi incaricati, in base alla quale alla fine di ciascun trattamento autorizzato devono essere riposti sotto chiave nei relativi archivi.

Si procede invece all'analisi dei dati elettronici che si articola in 4 punti:

1. *Chi-fa-cosa dentro*, ovvero chi, all'interno dell'organizzazione ha diritto di accedere a dati (digitali o cartacei), in che orari, con che diritti, che server ha diritto di utilizzare, quali applicazioni, ecc.
2. *Chi-fa-cosa fuori*, ovvero chi ha diritto di uscire verso Internet, verso i clienti, partners, fornitori, che ha diritto di usare un modem, chi ha diritto di fare qualunque cosa che, nell'esercizio delle proprie funzioni, entri in relazione con il mondo esterno.
3. *Chi, interno, fa cosa da fuori* ovvero chi, membro dell'organizzazione, ha necessità di accedere dall'esterno alla rete dell'ente con che diritti e per fare cosa.
4. *Chi, esterno, può fare cosa da fuori*, ovvero chi esterno all'organizzazione, come un fornitore o un partner, può fare cosa nel momento in cui accede ai sistemi informativi, digitali o cartacei, della organizzazione.
  - a. Rapporti con aziende esterne all'organizzazione assimilabili a titolari del trattamento.

### *Chi-fa-cosa dentro*

In questa fase si analizza chi, all'interno dell'organizzazione ha diritto di accedere a dati elettronici, in che orari, con che diritti, che server ha diritto di utilizzare, quali applicazioni, ecc..

*Legenda:* R sta per **read** (diritto di lettura) e W sta per **write** (diritto di scrittura).

Tavola 16.: *chi-fa-cosa dentro*

Gruppi	Server	Diritti	Orari
Direzione Generale	File Server	R/W per la directory di area (sia per le cartelle di dati comuni che per quelle con dati sensibili) e nessuno per le altre	Nessuna limitazione



segue

<b>Gruppi</b>	<b>Server</b>	<b>Diritti</b>	<b>Orari</b>
	Altri server	R	Nessuna limitazione
	DB Server gestionale	R/W	Nessuna limitazione
	E-Mail server	R/W	Nessuna limitazione
	Applicazioni gestionali	R/W	Nessuna limitazione
	Servizi di gestione	Nessuno	Nessuna limitazione
Ufficio Staff del Sindaco	File Server	R/W per la directory di area (sia per le cartelle di dati comuni che per quelle con dati sensibili) e nessuno per le altre	Nessuna limitazione
	Altri server	R	Nessuna limitazione
	DB Server gestionale	R/W	Nessuna limitazione
	E-Mail server	R/W	Nessuna limitazione
	Applicazioni gestionali	R/W	Nessuna limitazione
	Servizi di gestione	Nessuno	Nessuna limitazione
Avvocatura	File Server	R/W per la directory di area (sia per le cartelle di dati comuni che per quelle con dati sensibili) e nessuno per le altre	Nessuna limitazione
	Altri server	R	Nessuna limitazione
	DB Server gestionale	R/W	Nessuna limitazione
	E-Mail server	R/W	Nessuna limitazione
	Applicazioni gestionali	R/W	Nessuna limitazione
	Servizi di gestione	Nessuno	Nessuna limitazione



segue

<b>Gruppi</b>	<b>Server</b>	<b>Diritti</b>	<b>Orari</b>
Area Risorse	File Server	R/W per la directory di area (sia per le cartelle di dati comuni che per quelle con dati sensibili) e nessuno per le altre	Nessuna limitazione
	Altri server	R	Nessuna limitazione
	DB Server gestionale	R/W	Nessuna limitazione
	E-Mail server	R/W	Nessuna limitazione
	Applicazioni gestionali	R/W	Nessuna limitazione
	Servizi di gestione	Nessuno	Nessuna limitazione
Area Servizi al Territorio	File Server	R/W per la directory di area (sia per le cartelle di dati comuni che per quelle con dati sensibili) e nessuno per le altre	Nessuna limitazione
	Altri server	R	Nessuna limitazione
	DB Server gestionale	R/W	Nessuna limitazione
	E-Mail server	R/W	Nessuna limitazione
	Applicazioni gestionali	R/W	Nessuna limitazione
	Servizi di gestione	Nessuno	Nessuna limitazione
Area Servizi alla Persona	File Server	R/W per la directory di area (sia per le cartelle di dati comuni che per quelle con dati sensibili) e nessuno per le altre	Nessuna limitazione
	Altri server	R	Nessuna limitazione



segue

<b>Gruppi</b>	<b>Server</b>	<b>Diritti</b>	<b>Orari</b>
	DB Server gestionale	R/W	Nessuna limitazione
	E-Mail server	R/W	Nessuna limitazione
	Applicazioni gestionali	R/W	Nessuna limitazione
	Servizi di gestione	Nessuno	Nessuna limitazione
Area Comunicazione e Rapporti con il cittadino	File Server	R/W per la directory di area (sia per le cartelle di dati comuni che per quelle con dati sensibili) e nessuno per le altre. Tutti per gli incaricati dei sistemi informativi	Nessuna limitazione
	Altri server	R – R/W per gli incaricati dei sistemi informativi	Nessuna limitazione
	DB Server gestionale	R/W	Nessuna limitazione
	E-Mail server	R/W	Nessuna limitazione
	Applicazioni gestionali	R/W	Nessuna limitazione
	Servizi di gestione	Nessuno per tutti tranne – R/W per gli incaricati dei sistemi informativi	Nessuna limitazione



segue

## Chi-fa-cosa fuori

In questa fase ci si sofferma su chi ha diritto di uscire verso Internet, verso i clienti, partners, fornitori, che ha diritto di usare un modem, chi a diritto di fare qualunque cosa che, nell'esercizio delle proprie funzioni entri in relazione con il mondo esterno.

Tavola 17.: chi-fa-cosa fuori

Gruppi	Servizi	Diritti	Orari
Direzione Generale	Posta	R/W	Nessuna limitazione
	Navigazione	Nessuna limitazione	Nessuna limitazione
	FTP	R/W	Nessuna limitazione
Ufficio Staff del Sindaco	Posta	R/W	Nessuna limitazione
	Navigazione	Nessuna limitazione	Nessuna limitazione
	FTP	R/W	Nessuna limitazione
Avvocatura	Posta	R/W	Nessuna limitazione
	Navigazione	Nessuna limitazione	Nessuna limitazione
	FTP	R/W	Nessuna limitazione
Area Risorse	Posta	R/W	Nessuna limitazione
	Navigazione	Nessuna limitazione	Nessuna limitazione
	FTP	R/W	Nessuna limitazione
Area Servizi al Territorio	Posta	R/W	Nessuna limitazione
	Navigazione	Nessuna limitazione	Nessuna limitazione
	FTP	R/W	Nessuna limitazione
Area Servizi alla Persona	Posta	R/W	Nessuna limitazione
	Navigazione	Nessuna limitazione	Nessuna limitazione



segue

Gruppi	Servizi	Diritti	Orari
	FTP	R/W	Nessuna limitazione
Area Comunicazione e Rapporti con il cittadino	Posta	R/W	Nessuna limitazione
	Navigazione	Nessuna limitazione	Nessuna limitazione
	FTP	R/W	Nessuna limitazione

Il servizio FTP nei gruppi può essere attivato, su richiesta per alcuni utenti

### ***Chi, interno, fa cosa da fuori***

Oggetto dell'analisi è chi, membro dell'organizzazione, ha necessità di accedere dall'esterno alla rete dell'ente allo scopo di definire i diritti e per fare cosa.

*Tavola 18.: chi, interno, fa-cosa da fuori*

Gruppi	Persone	Diritti
Direzione Generale	Tutti	La WebMail per tutti, nessuno per il resto dei servizi
Ufficio Staff del Sindaco	Tutti	La WebMail per tutti, nessuno per il resto dei servizi
Avvocatura	Tutti	La WebMail per tutti, nessuno per il resto dei servizi
Area Risorse	Tutti	La WebMail per tutti, nessuno per il resto dei servizi
Area Servizi al Territorio	Tutti	La WebMail per tutti, nessuno per il resto dei servizi
Area Servizi alla Persona	Tutti	La WebMail per tutti, nessuno per il resto dei servizi



*segue*

<b>Gruppi</b>	<b>Persone</b>	<b>Diritti</b>
Area Comunicazione e Rapporti con il cittadino	Tutti - Ventura e Marchetti hanno accesso in VPN con gli stessi diritti di amministrazione presenti in locale	La WebMail per tutti, nessuno per il resto dei servizi. Ventura e Marchetti hanno accesso in VPN con gli stessi diritti di amministrazione presenti in locale
Dirigenti, consiglieri e gruppo consiliari	Tutti	La WebMail per tutti, nessuno per il resto dei servizi

Occorre ricordare che gli utenti eventualmente autorizzati entrano con gli stessi diritti di quando lavorano in LAN, ovvero dal proprio posto di lavoro interno.



segue

### **Chi, esterno, può fare cosa da fuori o, in casi definiti, da dentro**

Infine analizziamo chi esterno all'organizzazione, come un fornitore o un partner, può fare cosa nel momento in cui accede ai sistemi informativi interni all'organizzazione.

*Tavola 19.: chi, esterno, può fare-cosa da fuori o, in casi definiti, da dentro*

<b>Azienda</b>	<b>Server o apparecchiatura o servizio</b>	<b>Diritti</b>	<b>Orari</b>
3CiME Technology Srl	Accesso a tutti i server ed al sistema di storage in fase di installazione	R/W Amministrazione	Via VPN site to site sempre attiva
ACER	Accesso ad alcuni dati dell'Anagrafe	R	Nessuna limitazione
EQUITALIA POLIS S.p.a.	Accesso ad alcuni dati dell'Anagrafe	R	Nessuna limitazione
INPDAP	Accesso ad alcuni dati dell'Anagrafe	R	Nessuna limitazione
S.A.T.	Accesso ad alcuni dati dell'Anagrafe	R	Nessuna limitazione
Corte d'appello	Accesso ad alcuni dati dell'Anagrafe	R	Nessuna limitazione
Carabinieri	Accesso all'anagrafe	R	Nessuna limitazione
INPS	Accesso all'Anagrafe	R	Nessuna limitazione
QUESTURA	Accesso all'Anagrafe	R	Nessuna limitazione
Manutencoop	Potenzialmente a tutti i dati cartacei	Nessuno	Orari previsti dal contratto
Data Management S.p.A.	Serpico gestione giuridica/economica e gestione finanziaria	Consulta e modifica dati	In accordo con i servizi informatici e servizi che utilizzano il data base



segue

<b>Azienda</b>	<b>Server o apparecchiatura o servizio</b>	<b>Diritti</b>	<b>Orari</b>
ADS	Software dei contratti, Albo informatizzato dei fornitori	Consulta e modifica dati	In accordo con il servizio
ETonelli.com	Software vari piattaforma notes	Consulta e modifica dati	In accordo con il servizio
VideoArts	Portale degli ordini	Consulta e modifica dati	In accordo con il servizio
ACER Bologna	Gradus	Consulta e modifica dati	In accordo con il servizio
Gies	Inventario: Babilon e Samsah	Consulta e modifica dati	In accordo con il servizio
CORE Soluzioni Informatiche	DB pratiche edilizie - sw su Notes	tutto	Nessuna limitazione
SELEC	DB Sinfecon Attività Produttive - Archivio SQL Server	tutto	Nessuna limitazione
Coop Le Pagine	Archivio utenti e archivio documenti.	R/W Amministrazione	Orari previsti dal contratto
DEDAX S.r.L.	Lavori Pubblici - per conto di Adopera SRL	R/W Amministrazione	Nessuna limitazione
Emisfera Sistemi S.r.l.	Infrastruttura Hyperlan	R/W Amministrazione	Nessuna limitazione
Engineering Ingegneria Informatica S.P.A.	Portale Autenticazione - Pagamenti On-Line - Tributi	R/W Amministrazione	Nessuna limitazione
InfoLine Servizi Informatici S.r.L.	Gestione Presenze del Personale	R/W Amministrazione	Nessuna limitazione
Longwave S.p.A.	Centralino analogico	R/W Amministrazione	Nessuna limitazione



segue

<b>Azienda</b>	<b>Server o apparecchiatura o servizio</b>	<b>Diritti</b>	<b>Orari</b>
Open Software S.r.L.	Manutenzione SW Visual Polcity	R/W Amministrazione	Nessuna limitazione
Progetti di Impresa S.r.l.	Portale Istituzionale	R/W Amministrazione	Nessuna limitazione
SofTech S.r.l.	Gestionali Servizi Sociali e Scolastici	R/W Amministrazione	Nessuna limitazione
TRAFFIC TECHNOLOGY	Vistared	R/W Amministrazione	Nessuna limitazione
Centro Computer	Assistenza hardware personal computer e server	R/W Amministrazione	Nessuna limitazione
Make IT	Assistenza e manutenzione su struttura MS-SQL	Solo in locale	Nessuna limitazione
Adopera SRL	Ha accesso alla sala macchine remota di via Guido Rossa	R/W Amministrazione	Nessuna limitazione
Verbatel	Manutenzione SW centrale radio	R/W Amministrazione	In accordo col CED



segue

## ***Rapporti con aziende esterne all'organizzazione assimilabili a titolari del trattamento: regola 19.7 dell'Allegato B al Codice***

Allo scopo di assicurare un servizio di manutenzione ordinaria gestito in outsourcing è necessario che alcune società esterne possano intervenire sui sistemi informativi dell'ente o presso le sedi fisiche. Dette società prestano l'assistenza dovuta al fine di garantire la continuità del servizio, il ripristino dei sistemi in caso di fault, blocco o disastro, in altri casi servizi necessari per il corretto funzionamento delle strutture.

Per l'elenco delle suddette società è possibile fare riferimento al piano di sicurezza dell'ente al paragrafo precedente dal titolo: *“Chi esterno fa cosa da fuori”*.

In questo paragrafo si intende, invece, sottolineare che i rapporti con queste strutture sono regolati da un apposito accordo che le nomina *“responsabili esterni all'organizzazione”* ai sensi dell'art. 29 del d.lgs n. 196/2003.

Nell'accordo si fa presente che le società esterne che intervengono sul sistema informativo dell'ente avendo, di regola, diritti di amministratore, in teoria possono fare tutto. In ragione di ciò è imposto loro di intervenire solo con atti necessari alla prestazione dei servizi oggetto di contratto. È fatto loro esplicito divieto di consultare, copiare, cancellare e fare qualunque operazione sui dati oggetto di trattamento, a meno di diversa autorizzazione scritta da parte del responsabile del trattamento dei dati. È fatto inoltre divieto, salvo diversa autorizzazione scritta da parte dell'amministratore dei sistemi, di cancellare i log riportanti *“chi ha fatto cosa”* sui dati.

Resta anche inteso che qualunque intervento prestato dai tecnici di dette ditte andrà preventivamente richiesto all'amministratore di sistema (ad una delle figure nominate), anche via e-mail, ma sempre in modalità scritta.

Il titolare si deve riservare di fare controlli sull'operato del responsabile esterno in qualunque momento e con qualunque mezzo consentito dalla legge.

Il soggetto cui le attività sono affidate deve dichiarare:

1. di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali;
2. di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali;
3. di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere;
4. di tenere traccia, in un proprio registro, del chi ha fatto cosa, data e ora, in ogni intervento di amministrazione fatto dai suoi operatori;
5. di impegnarsi a relazionare annualmente, se richiesto dal committente, sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze;
6. di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

## Securelaw

### Securelaw: verifica degli adempimenti formali

#### *Dati residenti su elaboratori elettronici*

Tavola 20.: riepilogo adempimenti formali per dati residenti su elaboratori elettronici

Adempimenti formali	Persona fisica o giuridica interessata	Modalità/conseguenze
Censimento delle banche dati.	Il gruppo di lavoro di progetto.	Espletata con il presente documento.
Notifica al garante		Non necessaria in quanto l'ente non gestisce alcun dato di quelli previsti all'art 37 comma 1 del D.lgs. 196/2003
Identificazione del titolare del trattamento dei dati.	Il Comune di Casalecchio di Reno nella persona del legale rappresentante, Sig. <b>Simone Gamberini</b> , affiancato dagli organi dell'ente, siano essi la Giunta ed il Consiglio Comunale	
Identificazione del/dei responsabili del trattamento dei dati (colui che è preposto al trattamento dei dati e che è soggetto alla vigilanza del titolare).	Nominati i seguenti dirigenti: Raffaella Galliani - prot. n. 5443 Fabiana Battistini - prot. n. 5444 Vittorio Emanuele Bianchi - prot. n. 5445 Gian Paolo Cavina - prot. n. 5446 Aida Gaggioli - prot.n. 5447 Davide Montanari - prot. n. 5448 Stefano Bolognesi - prot. n. 5449 del 3 marzo 2010  La loro nomina è confermata con il presente atto	Nomina per iscritto riconfermata con il presente atto.



segue

<b>Adempimenti formali</b>	<b>Persona fisica o giuridica interessata</b>	<b>Modalità/conseguenze</b>
Amministratore di sistema (è il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione).	Tutti coloro che verranno nominati nell'atto di incarico specifico che è redatto entro i termini previsti dal provvedimento del garante	Nominato per iscritto riconfermato con il presente atto.
Il custode delle chiavi - o password (persona fisica che opera in costante contatto con gli incaricati e che ha il compito di custodire la password da essi stabilita ed annotata in busta chiusa conservata in armadio sotto chiave).	Non è previsto	
Identificazione degli incaricati (persona fisica che provvede quotidianamente al trattamento).	Tutti gli utenti definiti nel presente documento.	È tenuto ad operare secondo le istruzioni e le direttive impartite in forma scritta dal titolare e dal responsabile.
Interessato (è la persona fisica o giuridica alla quale si riferiscono i dati)	Tutti coloro che vengono in contatto diretto con l'ente	Deve dare l'assenso al trattamento dei propri dati per iscritto



## Securelaw: verifica degli adempimenti sostanziali

Occorre innanzitutto ribadire la regola generale che vige all'interno dell'ente per ciò che concerne i dati elettronici, che consiste nella comunicazione, avvenuta anche attraverso i corsi di formazione istituiti, a tutti gli incaricati del divieto di archiviare alcun tipo di dato sul proprio posto di lavoro/personal computer, pena l'acquisizione della piena responsabilità del trattamento di quei dati e le relative conseguenze civili e penali in capo all'incaricato/responsabile in caso di perdita e trafugamento dei dati medesimi.

Nel d.lgs. n. 196/2003 il legislatore richiede di adottare misure idonee volte a garantire la sicurezza e l'integrità dei dati: è opinione corrente della giurisprudenza che si debba intendere che tali misure siano scelte in relazione alle conoscenze acquisite in base al progresso tecnologico. Di conseguenza, per rispettare la normativa in vigore, è necessario aggiornarsi continuamente alle più recenti misure di protezione degli archivi di dati che siano rese disponibili dal produttore o dal mercato nel suo complesso.

Il d.lgs. n. 196/2003, Allegato B richiede di adottare misure minime che non si limitano alla protezione in senso tecnico dei sistemi informatici, ma si estendono: alla predisposizione di impianti antincendio che prevengano la distruzione di archivi, alla trasmissione degli stessi a società specializzate per l'archiviazione in armadi protetti, alla pianificazione di regole interne per la disciplina del comportamento degli incaricati (es. non attaccare memo di carta riportanti la password sul monitor del PC), ecc.

Si prende atto che l'ente dichiara di essere in linea con quanto previsto dalla normativa: di seguito si riepilogano le azioni poste in essere.



segue

## Adempimenti sostanziali dati elettronici

Tavola 21.: riepilogo adempimenti sostanziali per dati residenti su elaboratori elettronici

<b>Adempimenti sostanziali</b>
a) Password per l'accesso ai dati con dovere per l'utente di cambiarla.
b) Sono stati nominati amministratori di sistema tutti coloro che sono stati indicati nell'atto di incarico specifico redatto entro i termini previsti dal provvedimento del garante
c) Uno user-id per ogni incaricato, user-id che deve essere cancellato entro sei mesi dal termine dell'incarico.
d) Programma antivirus sia lato server che lato personal computer che è aggiornato ogni volta che il produttore rilascia la disponibilità di un aggiornamento. Il prodotto adottato è dato dalla suite della Sophos per tutti i server ed i client, nonché un prodotto integrato nel firewall Fortigate sul perimetro (server di posta e navigazione).
e) Sistema di sicurezza che prevenga l'azione degli hackers (pirati informatici), anti intrusione e volto ad evitare accessi non autorizzati.
f) Redazione del documento programmatico sulla sicurezza dei dati.
g) È stato redatto un manuale contenente le istruzioni per gli incaricati che comprende: <ol style="list-style-type: none"><li>1. L'elencazione specifica degli incaricati (rimanda allo specifico atto di nomina).</li><li>2. La descrizione del profilo assegnato nell'ambito dello svolgimento delle mansioni previste dall'incarico, con riferimento al trattamento dei dati personali (rimanda allo specifico data base).</li><li>3. L'elencazione dei dati a cui possono avere accesso e delle eventuali restrizioni (autorizzazione che deve essere limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento) (rimanda allo specifico atto di nomina ed allo specifico data base).</li><li>4. Il comportamento da assumere in caso di malfunzionamento del sistema (può anche essere semplicemente l'indicazione di richiedere l'intervento dell'assistenza tecnica).</li><li>5. Le istruzioni per l'utilizzo dei supporti magnetici.</li><li>6. Elenco ed ubicazione degli elaboratori abilitati alla connessione verso l'esterno.</li><li>7. Altre eventuali specifiche istruzioni.</li></ol>
h) Almeno una volta all'anno il titolare, o se designato, il responsabile, devono verificare la correttezza di tali informazioni e, se necessario, provvedere alla loro modifica



segue

## Securelaw: verifica degli adempimenti formali

### *Dati residenti su archivi cartacei*

Tavola 22.: riepilogo adempimenti formali per dati residenti su archivi cartacei

<b>Adempimenti formali</b>	<b>Persona fisica o giuridica interessata</b>	<b>Modalità/conseguenze</b>
Censimento delle banche dati.	Gruppo di lavoro di progetto	Espletata con il presente documento.
Notifica al garante		Non necessaria.
Identificazione del titolare del trattamento dei dati.	Il Comune di Casalecchio di Reno nella persona del legale rappresentante, Sig. <b>Simone Gamberini</b> , affiancato dagli organi dell'ente, siano essi la Giunta ed il Consiglio Comunale	
Identificazione del/dei responsabili del trattamento dei dati (colui che è preposto al trattamento dei dati e che è soggetto alla vigilanza del titolare).	Nominati i seguenti dirigenti: Raffaella Galliani - prot. n. 5443 Fabiana Battistini - prot. n. 5444 Vittorio Emanuele Bianchi - prot. n. 5445 Gian Paolo Cavina - prot. n. 5446 Aida Gaggioli - prot.n. 5447 Davide Montanari - prot. n. 5448 Stefano Bolognesi - prot. n. 5449 del 3 marzo 2010  La loro nomina è confermata con il presente atto	Nomina per iscritto riconfermata con il presente atto.
Identificazione degli incaricati (persona fisica che provvede quotidianamente al trattamento).	Tutti gli utenti definiti nel presente documento.	È tenuto ad operare secondo le istruzioni e le direttive impartite in forma scritta dal titolare e dal responsabile.



*segue*

<b>Adempimenti formali</b>	<b>Persona fisica o giuridica interessata</b>	<b>Modalità/conseguenze</b>
Interessato (è la persona fisica o giuridica alla quale si riferiscono i dati)	Tutti coloro che vengono in contatto diretto con l'ente	Deve dare l'assenso al trattamento dei propri dati per iscritto



segue

## **Adempimenti sostanziali dati cartacei**

Tavola 23.: riepilogo adempimenti sostanziali per dati residenti su archivi cartacei

<b>Adempimenti sostanziali</b>
a) È stato redatto un manuale contenente le istruzioni per gli incaricati che comprende: <ol style="list-style-type: none"><li>1. L'elencazione specifica degli incaricati (rimanda allo specifico atto di nomina).</li><li>1. Il piano di formazione degli incaricati.</li><li>2. L'identificazione del gruppo di appartenenza ai fine del trattamento dei dati personali.</li><li>3. L'elencazione dei dati a cui gli incaricati possono avere accesso e delle eventuali restrizioni (autorizzazione che deve essere limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento).</li><li>4. Il comportamento da assumere in caso di necessità di distruzione di documenti erroneamente stampati.</li><li>5. Altre eventuali specifiche istruzioni.</li></ol>
b) Definizione dei rapporti con i soggetti esterni che si configurano come responsabili del trattamento dei dati.
c) Almeno una volta all'anno il titolare, o se designato, il responsabile, devono verificare la correttezza di tali informazioni e, se necessario, provvedere alla loro modifica.



## **Securelaw: piano formativo degli incaricati: regola 19.6 dell'Allegato B al Codice**

In ottemperanza all'Allegato B del "Codice in materia di protezione dei dati" sono previsti *interventi formativi degli incaricati del trattamento per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare*. La formazione è prevista a partire dal primo ingresso nell'ente e procede per l'intera vita lavorativa, divenendo particolarmente significativa in occasioni di mutamenti di mansione e di introduzione di nuovi significativi strumenti ai fini del trattamento dei dati.

Può non essere superfluo ricordare che un mirato e programmato processo di formazione favorisce una condivisione di regole e valori che permettono all'ente di operare in condizioni di efficacia ed efficienza.

Il piano di formazione degli incaricati può riguardare tre diverse tipologie di utenti:

- Utenti in pianta organica.
- Neoassunti.
- Utenti in revisione di incarico.

### ***Utenti in pianta organica.***

Per questa prima tipologia di utenti sono previsti due livelli di attività formativa:

1. una sessione iniziale volta a far apprendere le seguenti conoscenze:
  - lo spirito e i contenuti della legge;
  - le istruzioni impartite nel manuale degli incaricati;
  - le informazioni specifiche inerenti il trinomio incarico/profilo/unità-organizzativa o gruppo.
2. una sessione periodica di aggiornamento volta a spiegare:
  - le eventuali novità di legge;
  - le novità tecnologiche introdotte volte ad aumentare il livello di sicurezza secondo lo spirito di "adeguamento tecnologico" suggerito dalla normativa.

### ***Utenti neoassunti.***

Per questa seconda tipologia di utenti sono previsti due livelli di attività formativa:



*segue*

1. una sessione iniziale prevista all'interno del percorso formativo del dipendente e da tenersi sotto la responsabilità del dirigente di settore al quale afferisce il neoincaricato volta a far apprendere:
  - lo spirito e i contenuti della legge;
  - le istruzioni impartite nel manuale degli incaricati;
  - le informazioni specifiche inerenti il trinomio incarico/profilo/unità-organizzativa o gruppo.
2. la partecipazione alle sessioni periodiche di aggiornamento (come sopra indicato).

### ***Utenti in revisione di incarico***

Per questa ultima tipologia di utenti sono previsti due livelli di attività formativa:

1. una sessione iniziale prevista all'interno del percorso formativo del dipendente e da tenersi sotto la responsabilità del dirigente di settore al quale afferisce il neoincaricato volta a far apprendere:
  - le differenze nella gestione dei dati relative al nuovo incarico, rispetto al precedente;
  - istruzioni impartite nel manuale degli incaricati.
2. la partecipazione alle sessioni periodiche di aggiornamento (come sopra indicato).

Le modalità di erogazione dell'attività formativa possono avvenire attraverso lezioni frontali o dialogate in aula, nonché attraverso le più moderne tecnologie di e-learning. Nel caso si scegliesse quest'ultima modalità, si consiglia di prevedere una fase di verifica dell'apprendimento delle conoscenze e competenze oggetto del percorso formativo.



segue

Tavola 24.: piano di formazione degli utenti

Corso di formazione	Descrizione sintetica	Classi di incarico interessate	Numero di incaricati interessati	Numero di incaricati già formati/ da formare	Calendario
Il nuovo Codice sulla Tutela dei dati personali ed il manuale utente	Riassunto legislativo e spiegazione del manuale degli incaricati in aula per i dirigenti ed in e-learning per gli incaricati	Tutti i gruppi	Tutti	Tutti	Formazione di tutto il personale in aula o in e-learning nel corso del 2006.  Inoltre tutti gli anni viene data informazione al titolare ed ai responsabili del trattamento dei dati del Comune di Casalecchio di Reno, dell'atto di dazione del DPS, nonché, limitatamente ad alcuni allegati, a tutti gli incaricati al trattamento dei dati mediante invio a mezzo posta elettronica e pubblicazione sul portale intranet dell'Ente

**Data aggiornamento: 15/03/2010**



# DPS Documento Programmatico sulla Sicurezza dei dati: le azioni

## Dati residenti su supporto cartaceo

### *Analisi dei rischi*

I rischi ai quali sono soggetti i dati residenti su supporto cartaceo presenti nell'ente sono molto minori, ma comunque possiamo così elencarli:

- Accesso indebito alle risorse sia da parte di personale interno non autorizzato.
- Rischi connessi alla trasmissione dei dati.
- Perdita dei dati e quindi perdita della loro integrità fisica.
- Furti e azioni dolose.
- Eventi dannosi o disastrosi.
- Rischi connessi alla procedura di eliminazione di dati erroneamente stampati.

### *Analisi dei rischi e delle azioni intraprese per cautela relativamente al trattamento dei dati cartacei: regola 19.4 dell'Allegato B al Codice*

Le soluzioni individuate per la protezione dei dati residenti su elaboratori sono diverse e sono di seguito elencate.

*Tavola 25.: riepilogo dei rischi e delle azioni legate al trattamento dei dati cartacei*

Rischio	Azione
• Criteri e procedure per evitare <u>l'accesso indebito alle risorse da parte di utenti interni</u> all'ente	<ul style="list-style-type: none"><li>• Ogni utente autorizzato ha le chiavi dell'ente o degli uffici di propria pertinenza (si veda tabella relativa). È fatto divieto assoluto agli incaricati di recarsi in locali per i quali l'accesso non è autorizzato e fuori dall'orario di lavoro, qualora non espressamente autorizzati.</li></ul>
• Criteri e procedure per disciplinare il <u>comportamenti degli operatori</u>	<ul style="list-style-type: none"><li>• Formazione periodica di tutti gli incaricati</li><li>• Controlli periodici circa l'operato degli utenti</li><li>• Controlli degli accessi, sia fisici che informatici</li></ul>



segue

<b>Rischio</b>	<b>Azione</b>
Criteria e procedure per disciplinare gli <u>eventi relativi al contesto</u>	<ul style="list-style-type: none"><li>• Tutti i locali sono ad accesso controllato</li></ul>
Criteria e procedure per assicurare la <u>sicurezza nelle trasmissioni</u> dei dati	<ul style="list-style-type: none"><li>• I dati su supporto cartaceo sono consegnati solo a corriere postale o ad un corriere privato o ad altro operatore autorizzato</li></ul>
Criteria e procedure per assicurare l' <u>integrità fisica</u> dei dati	<ul style="list-style-type: none"><li>• Tutti i locali sono protetti da un sistema antincendio a norma 626.</li></ul>
Criteria tecnici ed organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché individuazione delle procedure per controllare l'accesso delle persone autorizzate ai locali medesimi: ciò al fine di evitare al massimo <u>manomissioni o furti o azioni dolose</u>	<ul style="list-style-type: none"><li>• Ogni utente autorizzato ha le chiavi dell'ente o degli uffici di propria pertinenza (si veda tabella relativa). È fatto divieto assoluto agli incaricati di recarsi in locali per i quali l'accesso non è autorizzato e fuori dall'orario di lavoro.</li></ul>
<u>Eventi dannosi o disastrosi</u>	<ul style="list-style-type: none"><li>• Tutti i dati su supporto cartaceo prodotti dall'ente possono comunque riprodotti in ogni momento partendo dagli archivi elettronici.</li><li>• I dati ricevuti, in futuro, saranno oggetto di digitalizzazione</li></ul>
<u>Rischi connessi alla procedura di eliminazione di dati erroneamente stampati.</u>	<ul style="list-style-type: none"><li>• Tutti i supporti cartacei che devono essere distrutti finiscono in alcuni raccoglitori solo dopo essere stati stracciati</li></ul>
Elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni	<ul style="list-style-type: none"><li>• Ogni volta che si presenta la necessità vengono tenute delle sessioni di aggiornamento, anche nell'ambito della formazione all'utilizzo dei nuovi strumenti informatici, volte ad assicurare tale conoscenza e l'aggiornamento della stessa</li></ul>
Controlli periodici	<ul style="list-style-type: none"><li>• Il responsabile effettua controlli periodici annuali circa l'applicazione delle regole suddette</li></ul>



segue

## Dati residenti su elaboratori elettronici

### Analisi dei rischi

Come evidenziato sopra, i rischi ai quali sono soggetti i dati residenti sugli elaboratori presenti nell'ente, già precedentemente elencati, sono i seguenti:

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

### Analisi dei rischi e delle azioni intraprese per cautela: regola 19.4 dell'Allegato B al Codice

Le soluzioni individuate per la protezione dei dati residenti su elaboratori sono diverse e sono di seguito elencate.

Tavola 26.: analisi dei rischi e azioni intraprese per i dati residenti su supporto elettronico

Rischio	Azione
<p>Criteria e procedure per evitare <u>l'accesso indebito alle risorse da parte di utenti interni</u> all'ente</p>	<ul style="list-style-type: none"> <li>• Ogni utente ha un codice identificativo ed una password che lo abilitano ad entrare nel sistema di rete limitatamente ai dati necessari per lo svolgimento delle proprie mansioni. La password è a scadenza secondo i requisiti normativi</li> <li>• Ogni utente ha un codice identificativo ed una password che lo abilitano ad entrare nel sistema applicativo limitatamente ai dati necessari per lo svolgimento delle proprie mansioni. La password è a scadenza, ove possibile, secondo i requisiti normativi</li> </ul>
<p>Criteria e procedure per disciplinare il <u>comportamenti degli</u></p>	<ul style="list-style-type: none"> <li>• Formazione periodica di tutti gli incaricati</li> </ul>



segue

<b>Rischio</b>	<b>Azione</b>
<u>operatori</u>	<ul style="list-style-type: none"><li>• Controlli periodici circa l'operato degli utenti</li><li>• Controlli degli accessi, sia fisici che informatici</li></ul>
Criteri e procedure per disciplinare gli <u>eventi relativi agli strumenti</u>	<ul style="list-style-type: none"><li>• Aggiornamento e potenziamento periodico dei sistemi antivirus installati</li><li>• Azioni specifiche previste per il fault tolerance (vedi tabelle successive)</li></ul>
Criteri e procedure per disciplinare gli <u>eventi relativi al contesto</u>	<ul style="list-style-type: none"><li>• Tutti i locali sono ad accesso controllato</li><li>• I sistemi di condizionamento del CED sono a tolleranza di guasto, ovvero in caso di guasto è pronta ad intervenire la società che ne ha in gestione la manutenzione</li></ul>
Criteri e procedure per assicurare la <u>sicurezza nelle trasmissioni</u> dei dati	<ul style="list-style-type: none"><li>• L'accesso alla rete pubblica degli utenti è regolamentato da strumenti tecnici (firewall) che consentono l'accesso al servizio solo agli incaricati che ne hanno necessità e registrano le attività fatte</li><li>• I suddetti sistemi proteggono la rete locale da accessi indebiti alle risorse da parte di "pirati" esterni</li><li>• La comunicazione con alcuni fornitori avviene tramite router specifico via VPN, associati ai relativi username e password</li><li>• È fissato un piano di controllo giornaliero le cui responsabilità ed oneri sono descritti nella tabella di cui sotto</li></ul>
Criteri e procedure per assicurare <u>l'integrità fisica</u> dei dati	<ul style="list-style-type: none"><li>• Servizi di back-up le cui responsabilità ed oneri sono descritti nella tabella di cui sotto</li><li>• I nastri di back-up sono normalmente archiviati in armadio sotto chiave presente all'interno della sede del CED, tranne i mensili che finiscono nella cassaforte del Municipio stesso.</li></ul>



segue

Rischio	Azione
	<ul style="list-style-type: none"><li>• Gli altri strumenti di back-up delle sedi remote e non collegate, sono archiviati, sotto chiave, nelle singole sedi</li><li>• È installato un sistema antivirus. Il prodotto adottato è dato dalla suite della Sophos per tutti i server ed i client. Il firewall ha un antivirus. I server di posta domino sono sotto firewall</li></ul>
Criteria e procedure per assicurare <u>l'integrità logica</u> dei dati	<ul style="list-style-type: none"><li>• Le applicazioni software in uso coprono l'ente da tale rischio</li></ul>
Criteria tecnici ed organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché individuazione delle procedure per controllare l'accesso delle persone autorizzate ai locali medesimi: ciò al fine di evitare al massimo <u>manomissioni o furti o azioni dolose</u>	<ul style="list-style-type: none"><li>• I server di rete sono localizzati in un ambiente – CED ad accesso controllato, la cui chiave è nelle mani esclusive dei membri del Servizio Informatico e delle altre persone autorizzate</li></ul>
Criteria tecnici ed organizzativi per limitare al massimo gli effetti di <u>eventi dannosi o disastrosi</u>	<ul style="list-style-type: none"><li>• I dati vengono ricoverati tutti i giorni in armadio sotto chiave</li><li>• Il piano di disaster recovery è definito</li></ul>
Elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni	<ul style="list-style-type: none"><li>• Ogni volta che si presenta la necessità vengono tenute delle sessioni di aggiornamento, anche nell'ambito della formazione all'utilizzo dei nuovi strumenti informatici, volte ad assicurare tale conoscenza e l'aggiornamento della stessa</li></ul>
Controlli periodici	<ul style="list-style-type: none"><li>• Il responsabile e l'amministratore di sistema effettuano controlli periodici annuali circa l'applicazione delle regole suddette</li></ul>

Descriviamo ora di seguito in modo dettagliato le attività più importanti intraprese per affrontare i rischi sopra riportati



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

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

Il sistema di back-up dei dati dei server è separato per ogni server e centralizzato nelle responsabilità: è basato sul software Time Navigator 4.2 che pilota una library con doppio driver LTO3.

Il back-up è quotidiano differenziale e full durante il week-end.

I differenziali vengono tenuti per una storia di 15 giorni

Per ogni full back-up si tiene una storia di un anno dell'ultimo full mensile.

Il back-up mensile viene archiviato nella cassaforte ignifuga del Municipio

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

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

*Tavola 27.: riepilogo delle operazioni di salvataggio dei dati*

1. eseguire giornalmente il back-up dei dati (Lisa Fini)
2. archiviare i nastri dei back-up sotto chiave (Lisa Fini)
3. controllare che le versioni del software di back-up siano allineate alle ultime versioni disponibili (Lisa Fini)
4. eseguire trimestralmente una prova di restore parziale dei dati (Lisa Fini)
5. eseguire settimanalmente un back-up intero dei dati (Lisa Fini)
6. eseguire annualmente una prova di restore dei dati ai fini di disaster (Lisa Fini)
7. archiviare provvedere a centralizzare in luogo definito, CD ROM dei sistemi operativi e dei software di sistema, in modo da averli sempre a disposizione in caso di bisogno (Lisa Fini)
8. provvedere a centralizzare in luogo definito e sicuro (Cassaforte del Municipio), copie dei back-up, in modo da averli sempre a disposizione in caso di bisogno (Lisa Fini)



*segue*

## **I controlli anti-intrusione dall'esterno**

Presentiamo di seguito il piano di sicurezza relativo ai controlli anti-intrusione: anche in questo caso elencheremo le operazioni previste, che fungono da manuale di istruzioni per gli incaricati addetti, ed il responsabile della esecuzione di tali operazioni. Tali operazioni verranno eseguite dopo la installazione del firewall.

*Tavola 28.: riepilogo delle operazioni di controlli anti-intrusione dall'esterno*

1. tenere aperto il monitor relativo ai tentativi di intrusione che il firewall offre (Andrea Ventura)
2. eseguire giornalmente il controllo del log relativo ai tentativi di intrusione (Andrea Ventura)
3. avvisare l'amministratore di sistema dei dati di eventuali attacchi (Andrea Ventura)
4. attivare azioni correttive (Andrea Ventura)
5. chiedere consulenza al fornitore dell'assistenza sistemistica su altre precauzioni da adottare (Andrea Ventura)



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

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

Server Novell NT/2000

Server Windows 2003

Server di data base Linux - Oracle

Server di data base SQL Server

Server di posta Lotus Domino

Switch

Firewall

Router

Linee Hyperlan o in fibra di collegamento con le sedi remote

Analizziamo ora le azioni adottate per ciascun elemento, ricordando che sono presenti alcuni sistemi SAN che permettono di gestire l'alta affidabilità dei sistemi, sia a livello di cluster, che a livello di macchine virtuali.

### Server Novell Netware

Per questo tipo di server il fattore di criticità sono tutti al livello 4. Le soluzioni adottate sono diverse. Vediamole una per una.

<b>Server Novell in categoria 4</b>
-------------------------------------

In questa categoria abbiamo la coppia dei file server. I servizi su questi server sono critici, ma esistono già dei sistemi di fault tolerance sui dischi (Raid5); e sulle memorie RAM. I server inoltre sono configurati in cluster, per cui la caduta di un server è gestita dalla configurazione in alta affidabilità. Inoltre, come per tutti i server, la macchina è coperta da 3 anni di garanzia e dopo il terzo anno è previsto il servizio indicato nel contratto di manutenzione o ne viene prevista la sostituzione. Le operazioni sopra riportate sono eseguite dal responsabile della rete interna (Andrea Ventura). In caso di assenza del responsabile di rete l'operazione può essere fatta da uno qualunque dei membri del Servizio Informatico..



segue

## Server Windows Server 200X

Per questo tipo di server il fattore di criticità varia dal livello 2 al livello 4. Anche in questo caso le soluzioni adottate sono diverse. Vediamole una per una.

### Server 200X/NT in categoria 4

In questa categoria abbiamo la coppia dei file server. I servizi su questi server sono critici, ma esistono già dei sistemi di fault tolerance sui dischi (Raid5); e sulle memorie RAM. I server inoltre sono configurati in cluster, per cui la caduta di un server è gestita dalla configurazione in alta affidabilità. Inoltre, come per tutti i server, la macchina è coperta da 3 anni di garanzia e dopo il terzo anno è previsto il servizio indicato nel contratto di manutenzione o ne viene prevista la sostituzione. Le operazioni sopra riportate sono eseguite dal responsabile della rete interna (Andrea Ventura). In caso di assenza del responsabile di rete l'operazione può essere fatta da uno qualunque dei membri del Servizio Informatico..

I servizi di PDC sono coperti a caldo da quelli del server BDC

### SQL Server

Per detto server il fattore criticità è sempre a livello 4, in quanto senza tale server gli utenti non possono lavorare sulle applicazioni gestionali ed accedere ai propri archivi. I servizi su questi server sono critici, ed anche in questo caso è configurato un cluster. Inoltre esistono dei sistemi di fault tolerance sui dischi della SAN. Per quello che riguarda il server è presente un secondo server denominato StandyDB che riceve copia asincrona dei dati dal principale e che ne offre una copia a caldo. Le operazioni sopra riportate sono eseguite dal responsabile della rete interna (Andrea Ventura). In caso di assenza del responsabile di rete l'operazione può essere fatta da uno qualunque dei membri del Servizio Informatico.

### Server 200X in categoria 3 e 2

In questa categoria abbiamo il server Domino principale e di back-up e numerosi server di applicazioni minori. I servizi su questi server sono decisamente meno critici, ma esistono comunque sistemi di fault tolerance sui dischi, mentre le memorie RAM attive sono a correzione di errore. In particolare comunque, i server Domino hanno una configurazione cluster gestita da Domino stesso. Come per tutti i server, le macchine sono coperta da 3 anni di garanzia e dopo il terzo anno non è previsto alcun contratto di manutenzione, in quanto si provvede alla sostituzione del server stesso nel corso del quarto anno di vita. Le operazioni sopra riportate sono eseguite dal responsabile della rete interna (Andrea Ventura). In caso di assenza del responsabile di rete l'operazione può essere fatta da uno qualunque dei membri del Servizio Informatico.

## Server Linux Red Hat Enterprise - Oracle

Per questo tipo di server il fattore di criticità è fisso al livello 4. Anche in questo caso le soluzioni adottate sono:



segue

#### **Server Linux Red Hat Enterprise - Oracle in categoria 4**

In questa categoria abbiamo il server Oracle che funge anche da Data Base di molte tra le più importanti applicazioni gestionali del comune). I servizi su questi server sono critici, e la configurazione è clusterizzata su due macchine fisiche. Esistono inoltre dei sistemi di fault tolerance sui dischi (Raid1); e sulle memorie RAM. Nonostante ciò è stato attivato un servizio di clustering per coprire gli eventuali failover del server. È inoltre configurato uno StandbyDB server che interviene in caso di fault del server principale, permettendo la continuazione dei servizi di accesso a dati ed applicazioni.

Il server è inoltre coperto da 3 anni di garanzia viene messo successivamente sotto contratto di manutenzione o sostituito.

#### **Server Linux in categoria 4**

In questa categoria abbiamo il server del centralino. Per l'affidabilità di questi server si è scelto di percorrere la strada della virtualizzazione. Esistono quindi copie di ogni macchina, archiviate sul sistema di Storage ed aggiornate giornalmente. In caso di fault della macchina fisica o virtuale si possono sfruttare le possibilità dell'ambiente XenServer per spostare tali macchine su altri device sì da garantire le funzionalità e la continuità del servizio. Le macchine hardware sulle quali si appoggiano hanno comunque sistemi di fault tolerance sui dischi, mentre le memorie RAM attive sono a correzione di errore. Come per tutti i server, la macchina è coperta da 3 anni di garanzia e dopo il terzo anno non è previsto alcun contratto di manutenzione, in quanto si provvede alla sostituzione del server stesso nel corso del quarto anno di vita. Le operazioni sopra riportate sono eseguite dal responsabile della rete interna (Andrea Ventura). In caso di assenza del responsabile di rete l'operazione può essere fatta da uno qualunque dei membri del Servizio Informatico.

#### **Server Linux in categoria 2**

In questa categoria abbiamo diversi server. I servizi su questi server sono decisamente meno critici, e tendono ad essere gestiti su macchine virtuali, per cui si beneficia delle caratteristiche di quell'ambiente ed esistono comunque sistemi di fault tolerance sui dischi, mentre le memorie RAM attive sono a correzione di errore. Come per tutti i server, la macchina è coperta da 3 anni di garanzia e dopo il terzo anno non è previsto alcun contratto di manutenzione, in quanto si provvede alla sostituzione del server stesso nel corso del quarto anno di vita. Le operazioni sopra riportate sono eseguite dal responsabile della rete interna (Andrea Ventura). In caso di assenza del responsabile di rete l'operazione può essere fatta da uno qualunque dei membri del Servizio Informatico.

## **Switch**

Attualmente nel Comune di Casalecchio di Reno risultano installati diversi switch sui quali si basano tutta l'architettura di rete delle sedi interessate dal progetto ed hanno chiaramente un fattore di criticità che variano dal livello 4 al livello 3.



*segue*

In caso di fault gli switch possono essere sostituiti, temporaneamente e con l'obiettivo di far ripartire un servizio, anche se ridotto, da un vecchio modello, disponibile a magazzino, oppure da un hub di scorta. A.T.S. in ogni caso ha un contratto per intervento entro le 8 ore dalla chiamata. La rete ripartirà comunque anche se con velocità ridotte. Le operazioni sopra riportate sono eseguite dal responsabile della rete interna (Andrea Ventura). In caso di assenza del responsabile di rete l'operazione può essere fatta da uno qualunque dei membri del Servizio Informatico.

## **Firewall e Router**

I router sono classificati in fascia 4 in quanto costituiscono la portante delle comunicazioni dell'ente verso il mondo esterno. I router sono apparecchiature sulle quali non è sempre possibile prevedere un back-up a caldo e d'altronde non è possibile pensare di tenere una macchina di questo tipo di scorta in magazzino. Le precauzioni intraprese sono due:

1. Il router che connette l'ente ad Internet tramite la rete a Larga Banda LEPIDA è in gestione e manutenzione alla Acantho, mentre quello che connette al Cineca (Tiscali) è in gestione al provider stesso. Con entrambi i provider è sottoscritto un contratto di assistenza che garantisce tempi di intervento di 4 ore lavorative.
2. Per le connessioni HyperLan le apparecchiature sono a noleggio e sono assistite da Emisfera Sistemi S.r.l., la quale assicura dei livelli di SLA Service Level Agreement in grado di assicurare tempi di intervento dell'ordine delle 8 ore dalla segnalazione di guasto o del problema.

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

Il firewall Fortigate è in configurazione cluster ed è assistito direttamente in gestione e manutenzione alla 3CiME Technology.

Il firewall Fortigate accorpa la banda sia della connessione Tiscali che della connessione Lepida, così da cautelare il Comune di Casalecchio dal fault di una delle due linee.

Le connessioni XDSL e ISDN sono invece in assistenza Telecomitalia che garantisce tempi di intervento entro le 8 ore lavorative



segue

## Procedure da seguire in caso di fault

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

### Server

#### Interventi validi per tutti i server installati

##### *Fault di disco*

Diversi i server sono al livello 4 della scala di criticità: tutti i server sono quindi coperti da un servizio di fault tolerance di tipo cluster e Raid sui dischi che è in grado di intervenire senza operatore. In caso di fault quindi gli utenti non subiranno interruzioni di lavoro, ed il responsabile del CED dell'ente si attiverà per aprire una chiamata al centro di assistenza hardware del modello interessato (qualora il server sia ancora in garanzia o sotto contratto di manutenzione), il quale interverrà per sostituire il disco. È opportuno controllare i tempi di intervento dell'assistenza. Contemporaneamente è necessario attivare la società di assistenza sistemistica 3CiME Technology per affrontare eventuali operazioni di riconfigurazione che si dovessero eventualmente rendere necessarie.

##### *Altro tipo di fault*

Il responsabile del CED dell'ente si attiverà per aprire una chiamata al centro di assistenza hardware del modello interessato (qualora il server sia ancora in garanzia o sotto contratto di manutenzione), il quale interverrà per sostituire il pezzo difettoso. È opportuno controllare i tempi di intervento dell'assistenza. Contemporaneamente è necessario attivare la società di assistenza sistemistica 3CiME Technology per affrontare eventuali operazioni di riconfigurazione che si dovessero eventualmente rendere necessarie.

### Server Novell

Tutti questi server reggono i più importanti servizi applicativi dell'ente. Le macchine quindi devono funzionare sempre. In caso di fault di un server le operazioni che il responsabile dei Servizi Informativi dell'ente devono fare sono tre:

1. aprire immediatamente una chiamata al centro di assistenza del produttore hardware per segnalare il guasto;
2. aprire immediatamente una chiamata alla società che offre assistenza sistemistica 3CiME Technology per segnalare il problema e ricevere il supporto necessario;

**Il numero dell'assistenza tecnica da contattare in caso di bisogno è  
Il venditore della macchina per i primi 3 anni di garanzia**



segue

**Centro Computer per le macchine fuori garanzia 051/6837999**

**ADS 051/ 6307411**

**3CiME Technology 051/4070383**

## **Server Windows 200X**

Tutti questi server reggono i più importanti servizi applicativi dell'ente. Le macchine quindi devono funzionare sempre. In caso di fault di un server le operazioni che il responsabile dei Servizi Informativi dell'ente devono fare sono tre:

1. aprire immediatamente una chiamata al centro di assistenza del produttore hardware per segnalare il guasto;
2. aprire immediatamente una chiamata alla società che offre assistenza sistemistica 3CiME Technology per segnalare il problema e ricevere il supporto necessario;

**Il numero dell'assistenza tecnica da contattare in caso di bisogno è**

**Il venditore della macchina per i primi 3 anni di garanzia**

**Centro Computer per le macchine fuori garanzia 051/6837999**

**ADS 051/ 6307411**

**3CiME Technology 051/4070383**

Successivamente alla riparazione sarà necessario:

1. riconfigurare il server danneggiato;

## **Server Linx - Oracle**

Tutti questi server reggono i più importanti servizi applicativi dell'ente. Le macchine quindi devono funzionare sempre. In caso di fault di un server le operazioni che il responsabile del CED dell'ente devono fare sono tre:

1. aprire immediatamente una chiamata al centro di assistenza di ADS per segnalare il guasto;
2. aprire immediatamente una chiamata alla società che offre assistenza sistemistica ADS o 3CiME Technology per segnalare il problema e ricevere il supporto necessario;

**Il numero dell'assistenza tecnica da contattare in caso di bisogno è**

**Il venditore della macchina per i primi 3 anni di garanzia**

**Centro Computer per le macchine fuori garanzia**

**ADS 051/6307411**

**3CiME Technology 051/4070383**

Successivamente alla riparazione sarà necessario:

1. riconfigurare il server danneggiato;



*segue*

## **Server Windows 200X – SQL Server**

Questi server regge un servizio applicativo che tra i più importanti dell'ente. Le macchine quindi devono funzionare con regolarità. In caso di fault di un server le operazioni che il responsabile del CED dell'ente devono fare sono tre:

1. aprire immediatamente una chiamata al centro di assistenza di Make IT o 3CiME Technology per segnalare il guasto;
2. aprire immediatamente una chiamata alla società che offre assistenza sistemistica Make IT o 3CiME Technology per segnalare il problema e ricevere il supporto necessario;

**Il numero dell'assistenza tecnica da contattare in caso di bisogno è**

**Il venditore della macchina per i primi 3 anni di garanzia**

**Centro Computer per le macchine fuori garanzia**

**Make IT 051/220726**

**3CiME Technology 051/4070383**

Successivamente alla riparazione sarà necessario:

3. riconfigurare il server danneggiato;

## **Sistema di SAN Storage Area Network**

Questo sistema regge tutti i servizi cluster e tutti gli ambienti virtualizzati, ed è il cuore dei dati dell'ente. Le macchine quindi devono funzionare sempre. In caso di fault di un server le operazioni che il responsabile del CED dell'ente devono fare sono tre:

1. aprire immediatamente una chiamata al centro di assistenza hardware del fornitore per segnalare il guasto;
2. aprire immediatamente una chiamata alla società che offre assistenza sistemistica 3CiME Technology per segnalare il problema e ricevere il supporto necessario;

**Il numero dell'assistenza tecnica da contattare in caso di bisogno è**

**Il venditore della macchina per i primi 3 anni di garanzia**

**3CiME Technology 051/4070383**

Successivamente alla riparazione sarà necessario:

3. riconfigurare i cluste eventualmente danneggiati;

## **Switch**

Tutti gli switch garantiscono il lavoro di tutti gli utenti e quindi devono funzionare sempre. In caso di fault di uno



segue

switch le operazioni che il responsabile del CED dell'ente devono fare sono due:

1. accedere immediatamente al magazzino e recuperare uno switch o un hub di scorta;
2. provvedere alla sostituzione dello switch danneggiato con uno di scorta: gli utenti potranno così ricominciare a lavorare anche se con prestazioni ridotte;

**In caso di fault di detti router l'operazione che il responsabile di rete dell'ente deve fare è:**

1. aprire immediatamente una chiamata presso il centro di supporto ATS., il quale provvederà risolvere il problema entro le ore fissate dal contratto;

**Il numero dell'assistenza tecnica da contattare in caso di bisogno è**

ATS S.p.A. 059/821332

## Firewall e connessione ad Internet

I router di fascia alta installati sono tutti al livello 3 della scala di criticità: è chiaro che, essendo il cuore di tutta la comunicazione, devono essere soggetti al minimo numero di interruzioni possibili.

**In caso di fault di detti router o firewall l'operazione che il responsabile di rete dell'ente deve fare è:**

1. aprire immediatamente una chiamata presso la ditta ACANTHO o Tiscali la quale provvederà gestire il guasto (che potrebbe essere anche sulla linea dati) entro le ore fissate dal contratto ed a riconfigurare il servizio; contattare 3CiME Technology sistemi anche per problematiche al firewall.

**Il numero dell'assistenza tecnica da contattare in caso di bisogno è**

**3CiME Technology 051/4070383**

**Tiscali Numero Verde Servizio Clienti: 192-130**

**Acantho Numero Verde Servizio Clienti: 800-055800**

## Router e connessioni WAN

I router di fascia alta installati sono tutti al livello 3 della scala di criticità: è chiaro che, essendo il cuore di tutta la WAN, devono essere soggetti al minimo numero di interruzioni possibili

**In caso di fault di detti router l'operazione che il responsabile di rete dell'ente deve fare è:**

2. aprire immediatamente una chiamata presso il centro di supporto Telecomitalia, per le connessioni XDSL/ISDN, il quale provvederà risolvere il problema entro le ore fissate dal contratto;



**Il numero dell'assistenza tecnica da contattare in caso di bisogno è  
Telecomitalia 191**

## **Linee di collegamento in fibra ottica**

Le linee di connessione installate fra le varie sedi dell'ente sono tutte al livello 4 della scala di criticità. In caso di indisponibilità di dette linee le operazioni che il responsabile di rete deve fare sono due:

1. aprire immediatamente una chiamata presso il centro di supporto Adopera, per le linee in fibra ottica, il quale provvederà risolvere il problema entro le ore fissate dal contratto;

**Il numero dell'assistenza tecnica da contattare in caso di bisogno è  
Cineca per la fibra Municipio-Cineca  
Altra Azienda del settore per le altre fibre**



segue

## Azioni da intraprendere per il disaster recovery

Dobbiamo innanzi tutto definire quali sono le sedi interessate allo studio di disaster recovery. Stabiliamo dunque che le sedi in oggetto sono due e sono costituite dalla sede principale dell'ente e dalla sede di disaster che è individuata presso la sede del Magazzino Comunale in Via Guido Rossa. Chiameremo dunque A la sede principale e B la sede di disaster.

*A: Sede principale Via dei Mille, n.9 40068 Casalecchio di Reno (BO)*

*B: Sede di disaster recovery: c/o Magazzino Comunale via Guido Rossi 1/3 - Cap 40033 Casalecchio di Reno (Bo)*

*C: Sede di archiviazione dei dati c/o Magazzino Comunale dove sono già presenti una copia dello StandBy DB di Oracle e l'analogo per i dati SQL Server*

### Regole valide per tutti i Server

Per i server i discorsi sono molteplici

1. In primo luogo prendiamo atto che nella sede C di archiviazione dei dati sono già presenti in modo automatico copie dei data base gestionali Oracle e Microsoft
2. Abbiamo definito ed attivato una procedura che permette di avere periodicamente i dati dei file system ricoverati in un luogo sicuro, nel nostro caso la sede di "archiviazione dei dati di back-up-disaster". Nel nostro caso dunque ogni giorno una copia incrementale dei back-up definita "disaster copy" viene effettuata dalla sede A alla sede di archiviazione dei dati C di copia dei dati, pronta per essere trasferita nella sede B in caso di disastro.
3. In secondo luogo si ricorda che giornalmente si eseguono e si controllano i back-up ordinari

### Server in categoria 2

1. Per i server basati su sistema operativo di tipo Windows NT/200X o Linux –Oracle sono disponibili, secondo le modalità sopra indicate, le immagini delle configurazioni, dalle quali è possibile ricostruire i server.
2. Per poter fare in modo che questa cautela produca, in caso di bisogno, i suoi effetti, abbiamo previsto che il nella sede di disaster sono disponibili alcuni server pronti per essere configurati ed installati presso la sede B, necessari per accogliere la restore dei dati.



segue

### Server in categoria 1

1. Anche in questo caso per ogni sistema operativo presente si utilizzano i servizi garantiti dal software di backup: i dati verranno restaurati, in un momento successivo alla ripartenza, su nuovi server che verranno man mano resi disponibili.

### WAN Link

Il primo problema riguarda la disponibilità di un accesso ad Internet, dal quale gli utenti potranno ripartire a lavorare sul server e sui dati messi a disposizione nella sede di disaster.

La sede dell'ente, come più volte evidenziato, è collegata ad Internet attraverso una connessione in fibra, con router in comodato di Acantho o di Tiscali.

In caso di disastro bisognerà richiedere l'attivazione, normalmente garantita entro 7 giorni dalla richiesta, di una connessione ADSL o HDSL con router a noleggio presso una delle sedi dell'ente verso la sede B di disaster. Una volta ottenuta, il fornitore di assistenza sistemistica provvederà alla riconfigurazione dei server e delle postazioni di lavoro per la ripartenza dei servizi.

### Firewall

Nel caso del Comune di Casalecchio di Reno la riconfigurazione del server comporta anche la riconfigurazione e, di conseguenza, la ripartenza dei servizi di firewall le cui operazioni saranno a carico del CED dell'ente.

## Procedure da seguire per affrontare una situazione di disaster recovery

La procedura da seguire, che cercheremo di definire passo a passo, è strettamente legata alle soluzioni tecniche adottate.

### Server

#### *Procedure da eseguire per i server di cui è presente il servizio di disaster recovery sul software di back-up dei dati*

Si cerca di riassumere in modo sintetico e semplice le attività da eseguire

*Tavola 29.: riepilogo procedure di disaster recovery per la sede del Municipio di Casalecchio di Reno legate ai dati*

#### **Per la sede del Municipio: attività a preventivo**

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



*segue*

### **Attività da espletare in caso di disastro**

1. controllare la disponibilità dei server “disaster” sui quali far ripartire il servizio, server che, come da accordi devono essere resi disponibili nella sede di disaster entro 3 giorni
2. avvertire del disastro il partner 3CiME Technology perché si tenga pronto ad intervenire (responsabile è Andrea Ventura)
3. definire gli utenti che dovranno ripartire nella sede di disaster (responsabile è Andrea Ventura)
4. provvedere alla reinstallazione dei server Netware/Windows 200X e Linux (responsabile è Andrea Ventura)
5. restaurare i dati sui server Netware/Windows 200X e Linux (responsabile è Andrea Ventura)
6. installare le postazioni client per detti utenti o permettergli di lavorare da postazioni esistenti (responsabile è Andrea Ventura)
7. ridefinire le stampanti (responsabile è Andrea Ventura)
8. riattivare il sistema di back-up sul nuovo server (responsabile è Andrea Ventura)



segue

## Router e Wan Link

Essendo la sede di disaster non collegata direttamente ad Internet, in caso di disastro sarà necessario provvedere ad espletare tutte quelle attività che sono necessarie per collegare ad Internet la sede di disaster. Le attività da fare sono le seguenti:

*Tavola 30.: riepilogo procedure di disaster recovery per la sede di Casalecchio di Reno legate ai Wan Link*

### Attività da espletare in caso di disastro

1. avvertire del disastro i partner Lepida e Tiscali perché si tengano ad intervenire (responsabile è Andrea Ventura)
2. avvertire del disastro il partner 3CiME Technology perché si tenga ad intervenire (responsabile è Andrea Ventura)
3. ordinare una nuova connessione ADSL/HDSL Internet verso la sede di disaster a Telecomitalia (responsabile è Andrea Ventura)
4. avvisare il fornitore dei servizi di assistenza sistemistica (ADS e 3CiME Technology) perché provveda alla riconfigurazione dei servizi HDSL di connessione (responsabile è Andrea Ventura)
5. provvedere alla riconfigurazione dei servizi firewall (responsabile è Andrea Ventura)
6. avvisare il fornitore dei servizi di disaster (3CiME Technology) perché provveda alla riconfigurazione dei server (responsabile è Andrea Ventura)
7. avvisare il fornitore della parte Oracle dei dati (ADS) perché provveda alla riconfigurazione dei server (responsabile è Andrea Ventura)
8. avvisare il fornitore della parte SQL Server dei dati (Make-it) perché provveda alla riconfigurazione dei server (responsabile è Andrea Ventura)
9. avvisare il fornitore del servizio di disaster della necessità di riconfigurare i servizi di back-up sulla nuova sede temporaneamente attivata (responsabile è Andrea Ventura)
10. Riconfigurare i posti di lavoro per quanto concerne le attività Internet (responsabile è Andrea Ventura)



## Documenti aggiuntivi: disciplinare Internet

Nel corso di questi anni il Garante per la protezione dei dati personali, ha emesso una serie di provvedimenti volti a rendere obbligatori alcuni adempimenti ulteriori rispetto al DPS. In particolare con delibera n. 13 del 1 marzo 2007, denominata “**le linee guida del Garante per posta elettronica e internet**” ha disposto che ogni organizzazione si doti di un “Disciplinare interno” che regoli la materia, da pubblicizzare adeguatamente (verso i singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori, ecc.) e da sottoporre ad aggiornamento periodico.

Tale disciplinare è stato redatto entro la data di scadenza annuale del DPS, ovvero entro il 31 marzo 2008. Il DPS recepisce quanto disposto da detto disciplinare in materia di gestione di Internet verso la rete interna e gli utenti. Ogni anno viene regolarmente aggiornato entro il 31 marzo.



## Amministratori di sistema

Il Garante per la protezione dei dati personali, ha emesso il provvedimento “**Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema**” - **27 novembre 2008**, nel quale ha chiesto la nomina ufficiale di coloro che svolgono tale funzione, e l’implementazione di accorgimenti tecnici volti a registrare alcuni eventi della attività degli amministratori di sistema stessi.

Il Comune di Casalecchio di Reno ha provveduto a nominare ufficialmente le persone interne del settore “Sistemi Informativi”, mentre per tutti coloro che svolgono tale attività presso ditte esterne, si è provveduto alla nomina di tali ditte come responsabili esterni al trattamento, ai sensi dell’art. 29 dlgs 196/2003, con obbligo per tali ditte di tenere traccia su proprio registro del “chi ha fatto cosa”.

Per ciò che concerne invece la registrazione dei log, fatto salvo l’applicazione del principio

1 utente amministratore = 1 user = 1 password

principio valido anche per le ditte esterne a livello aziendale (ovvero hanno un unico username e provvedono al loro interno alla registrazione di chi ha fatto tale attività), è installato un sistema di logging che trasferisce tali dati presso la società 3CiME Technology Srl, la quale mantiene inalterati tali dati per 1 anno solare dalla loro registrazione. Per l’attività di controllo, 3CiME Technology attiva, su richiesta del titolare o di persona da esso incaricata, un account per la consultazione web dei dati di logging.



## Relazione allegata al bilancio

Come da indicazione del Garante per la protezione dei dati personali, nella relazione accompagnatoria al bilancio consuntivo, è citata la redazione e l'aggiornamento del presente Documento Programmatico sulla Sicurezza.



## Conclusioni

Il presente documento redatto da AltaVia Consulting non esime il Cliente dalle sue responsabilità. Durante l'analisi si è preso atto delle informazioni che gli incaricati hanno fornito e si sono ordinate nel presente documento.

Sarà anche onere dell'ente tenere aggiornato il presente documento, almeno annualmente, sia affidando ancora l'incarico ad AltaVia Consulting che procedendo autonomamente.



segue

## Termini e definizioni

La terminologia relativa alla disciplina della gestione dei rischi di protezione può a volte essere di difficile comprensione. In alcuni casi, un termine noto può essere interpretato in modo diverso da persone diverse. Per questi motivi è importante comprendere le definizioni attribuite dagli autori di questa guida ai termini più importanti in essa contenuti. Molte delle definizioni elencate di seguito sono state originariamente utilizzate all'interno di documenti pubblicati da altre due organizzazioni: la International Standards Organization (ISO) e la Internet Engineering Task Force (IETF). Gli indirizzi dei siti Web di queste organizzazioni sono contenuti nella sezione "Ulteriori informazioni" più avanti in questo capitolo. Nell'elenco riportato di seguito sono illustrati i componenti principali della gestione dei rischi di protezione.

<ul style="list-style-type: none"><li>• <b>Previsione di perdita annua</b> — L'importo totale in denaro che l'organizzazione perderà in un anno se non viene presa alcuna iniziativa per ridurre un rischio.</li></ul>
<ul style="list-style-type: none"><li>• <b>Tasso di occorrenza annuo</b> — Il numero di volte che un rischio si potrebbe verificare nel corso di un anno.</li></ul>
<ul style="list-style-type: none"><li>• <b>Bene</b> — Tutto ciò che ha valore per un'organizzazione, come i componenti hardware e software, i dati, le persone e la documentazione.</li></ul>
<ul style="list-style-type: none"><li>• <b>Disponibilità</b> — La caratteristica di un sistema o di una risorsa di sistema che ne garantisce l'utilizzabilità da parte di un utente autorizzato che ne abbia fatto richiesta. La disponibilità è una delle caratteristiche fondamentali di un sistema sicuro.</li></ul>
<ul style="list-style-type: none"><li>• <b>CIA</b> — Acronimo di Confidentiality, Integrity, Availability (<i>Riservatezza, Integrità e Disponibilità</i>).</li></ul>
<ul style="list-style-type: none"><li>• <b>Riservatezza</b> — La caratteristica in base alla quale un'informazione non viene resa disponibile o divulgata a individui, entità o processi non autorizzati (ISO 7498-2).</li></ul>
<ul style="list-style-type: none"><li>• <b>Controllo</b> — Una modalità organizzativa, procedurale o tecnologica di gestione di un rischio; sinonimo di <i>misura di protezione o contromisura</i>.</li></ul>
<ul style="list-style-type: none"><li>• <b>Analisi costi-benefici</b> — Stima e confronto del valore relativo e del costo associati ai diversi controlli proposti al fine di implementare il controllo più efficace.</li></ul>
<ul style="list-style-type: none"><li>• <b>Supporto alle decisioni</b> — Definizione delle priorità dei rischi sulla base di un'analisi costi-benefici. Il costo sostenuto per la riduzione di un rischio mediante una soluzione di protezione viene confrontato con i benefici che la riduzione del rischio apporta all'azienda.</li></ul>
<ul style="list-style-type: none"><li>• <b>Difesa a più livelli</b> — L'approccio che prevede l'applicazione di più livelli di protezione nel caso in cui il livello di difesa di un singolo componente di protezione non sia sufficiente.</li></ul>



segue

<ul style="list-style-type: none"><li>• <b>Attacco</b> — Sfruttamento di una vulnerabilità al fine di danneggiare le attività o intaccare la protezione delle informazioni aziendali.</li></ul>
<ul style="list-style-type: none"><li>• <b>Esposizione</b> — La divulgazione dannosa e diretta di dati sensibili a un'entità non autorizzata (RFC 2828). Ai fini del processo di gestione dei rischi di protezione, con questa definizione si intende in particolare l'entità del danno a un bene aziendale.</li></ul>
<ul style="list-style-type: none"><li>• <b>Impatto</b> — La perdita di profitti complessiva prevista come conseguenza di un attacco ai danni di un bene.</li></ul>
<ul style="list-style-type: none"><li>• <b>Integrità</b> — La caratteristica dei dati che non hanno subito alterazioni o distruzioni in modo non autorizzato (ISO 7498-2).</li></ul>
<ul style="list-style-type: none"><li>• <b>Riduzione dei rischi</b> — Gestione dei rischi mediante specifiche azioni progettate per affrontare i pericoli ad essi associati.</li></ul>
<ul style="list-style-type: none"><li>• <b>Soluzione di riduzione dei rischi</b> — L'implementazione di un controllo organizzativo, procedurale o tecnologico al fine di gestire un rischio di protezione.</li></ul>
<ul style="list-style-type: none"><li>• <b>Probabilità</b> — La possibilità che un evento si verifichi.</li></ul>
<ul style="list-style-type: none"><li>• <b>Gestione dei rischi qualitativa</b> — Un approccio alla gestione dei rischi che prevede l'assegnazione di un valore relativo ai diversi beni, rischi, controlli e tipi di impatto.</li></ul>
<ul style="list-style-type: none"><li>• <b>Gestione dei rischi quantitativa</b> — Un approccio alla gestione dei rischi che prevede l'assegnazione di un valore numerico oggettivo (ad esempio un valore economico) ai diversi beni, rischi, controlli e tipi di impatto.</li></ul>
<ul style="list-style-type: none"><li>• <b>Reputazione</b> — L'opinione della gente nei riguardi di un'organizzazione; la reputazione di molte aziende ha un valore reale, anche se, essendo un concetto intangibile, è difficilmente quantificabile.</li></ul>
<ul style="list-style-type: none"><li>• <b>Ritorno sull'investimento nella protezione (ROSI)</b> — L'importo totale in denaro che un'organizzazione prevede di risparmiare in un anno grazie all'implementazione di un controllo di protezione.</li></ul>
<ul style="list-style-type: none"><li>• <b>Rischio</b> — La combinazione della probabilità che un evento si verifichi e delle conseguenze associate al verificarsi dell'evento (Guida ISO 73).</li></ul>
<ul style="list-style-type: none"><li>• <b>Valutazione dei rischi</b> — Il processo di identificazione dei rischi e di determinazione dell'impatto ad essi associato.</li></ul>
<ul style="list-style-type: none"><li>• <b>Gestione dei rischi</b> — Il processo che prevede la determinazione di un livello accettabile di rischio, la</li></ul>



*segue*

valutazione del livello attuale di rischio, l'adozione di azioni volte a ridurre il rischio a un livello accettabile e il mantenimento di questo livello di rischio.
• <b>Previsione di perdita singola (SLE)</b> — L'importo totale dei ricavi perduti in seguito a una singola occorrenza del rischio.
• <b>Pericolo</b> — Una causa potenziale di impatto indesiderato ai danni di un sistema o un'organizzazione (ISO 13335-1).
• <b>Vulnerabilità</b> — Qualsiasi punto debole, processo amministrativo, azione o esposizione fisica che rende un bene informatico suscettibile di attacco