



COMUNE DI CASALECCHIO DI RENO

Allegato n. 10

**PIANO DI SICUREZZA DEI DOCUMENTI
INFORMATICI**

PIANO DI SICUREZZA INFORMATICA

a cura

del Servizio Informatico Associato

Sommario:

Premessa: la gestione della sicurezza informatica

Identificazione del servizio da erogare

Descrizione delle infrastrutture tecnologiche

Schema rete logica VPN L3 dell'Unione Reno Lavino Samoggia

Server Fisici

Server virtuali

Descrizione dei sistemi informativi

Analisi dei rischi

Elenco dei rischi dei dati elettronici

Premessa: la gestione della sicurezza informatica

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

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

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

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

L'obiettivo è quindi quello di poter 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
- default di servizi
- eventi dannosi o disastrosi

offrendo al contempo garanzia di:

- autenticità e integrità delle registrazioni elettroniche

ed assicurando:

- possibilità di auditing

Per **accesso indebito alle risorse** si intende che dati, programmi, 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 sistema informativo da azioni particolari come modifica o copia di informazioni, file, programmi da parte di persone non autorizzate, uso non autorizzato dei privilegi di sistema, dirottamento o duplicazione di informazioni o uso di software non autorizzato, virus, trojan, ransomware, malware.

Per **protezioni degli errori operativi** s'intende che il sistema informativo deve essere progettato in modo tale 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 o la caduta di alcuni servizi**, 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, "caduto" in seguito a un guasti, problematiche 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 di condizionamento) o disastrosi (incendi, crolli, calamità naturali ecc..).

La **garanzia** che deve essere offerta del 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 sistema informativo è quello di garantire l'integrità logica (*coerenza e consistenza*) e fisica (*esistenza di copie e/o di salvataggi*) di tali dati.

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

Il presente documento viene redatto in forma minima e non esaustiva, tenendo conto della architettura centralizzata in via di svolgimento e compimento, del Servizio Informatico Associato dell'Unione dei Comuni Valli del Reno, Lavino Samoggia a cui le Amministrazioni dei Comuni di Comuni di Casalecchio di

Reno, Monte San Pietro, Sasso Marconi, Valsamoggia e Zola Predosa hanno conferito con apposita convenzione per la gestione delle funzioni informatiche.

Si specifica come il presente documento inerente nello specifico al Comune di Casalecchio di Reno la forma **minima e non esaustiva** essendo l'intero sistema informativo dell'ente in fase di transizione e di migrazione verso un Datacenter esterno della società in-house Lepida Spa. Tale migrazione è prevista ed esplicitata nel progetto "PROGETTO DI ADOZIONE DEI SERVIZI DI DATA CENTER & CLOUD DI LEPIDA SPA E MIGRAZIONE DEI DATACENTER LOCALI VERSO IL DATACENTER DI LEPIDA SPA" approvato dalla Giunta dell'Unione in data 01/02/2016

Tale fase transitoria verrà completata entro il primo quadrimestre dell'anno 2017 e al termine tale documento inizieranno le attività propedeutiche alla redazione e aggiornamento, in maniera completa ed esaustiva del presente documento riguardante l'intero sistema informativo dell'Unione Reno Lavino Samoggia.

Identificazione del servizio da erogare

I Comuni dell'Unione dell'Unione Reno Lavino Samoggia hanno conferito all'Unione la gestione associata dei servizi informatici e servizi informativi in piena armonia con la normativa nazionale e regionale in materia di gestioni associate.

Tale conferimento prevede lo svolgimento delle seguenti attività:

- la progettazione e gestione dell'infrastruttura tecnologica del servizio informativo prevista in un unico Datacenter esterno ai Comuni dell'Unione e di proprietà di Lepida SPA
- la progettazione e gestione delle reti dati dei singoli Comuni e di un'unica rete VPN che permetta l'interconnessione di tutte le reti locali dei Comuni le une con le altre
- l'assistenza informatica a seguito di aperture di ticket in un unico portale per tutta l'Unione
- l'installazione e configurazioni delle postazioni di lavoro
- la gestione unitaria dei contratti informatici
- l'omogenizzazione dei software di back office
- l'erogazione di servizi on line
- la sottoscrizione di accordi con altri enti in ambito ICT
- gestione dei sistemi e dei relativi hot spot wifi sul territorio

Descrizione delle infrastrutture tecnologiche

L'Unione Reno Lavino Samoggia usufruirà dei servizi di Datacenter di Lepida SPA e nella fattispecie usufruirà dei servizi del Datacenter ubicato a Ravenna.

Tutti i Comuni sono collegati alla rete in banda larga regionale Lepida e collegati logicamente tra di loro tramite la stessa banda larga tramite una rete VPN L3 realizzata e configurata dalla collaborazione tra SIA e Lepida SPA.

Lepida SPA per i servizi di Datacenter e banda larga dispone di un servizio di help desk attivo 24 ore per 365 giorni all'anno.

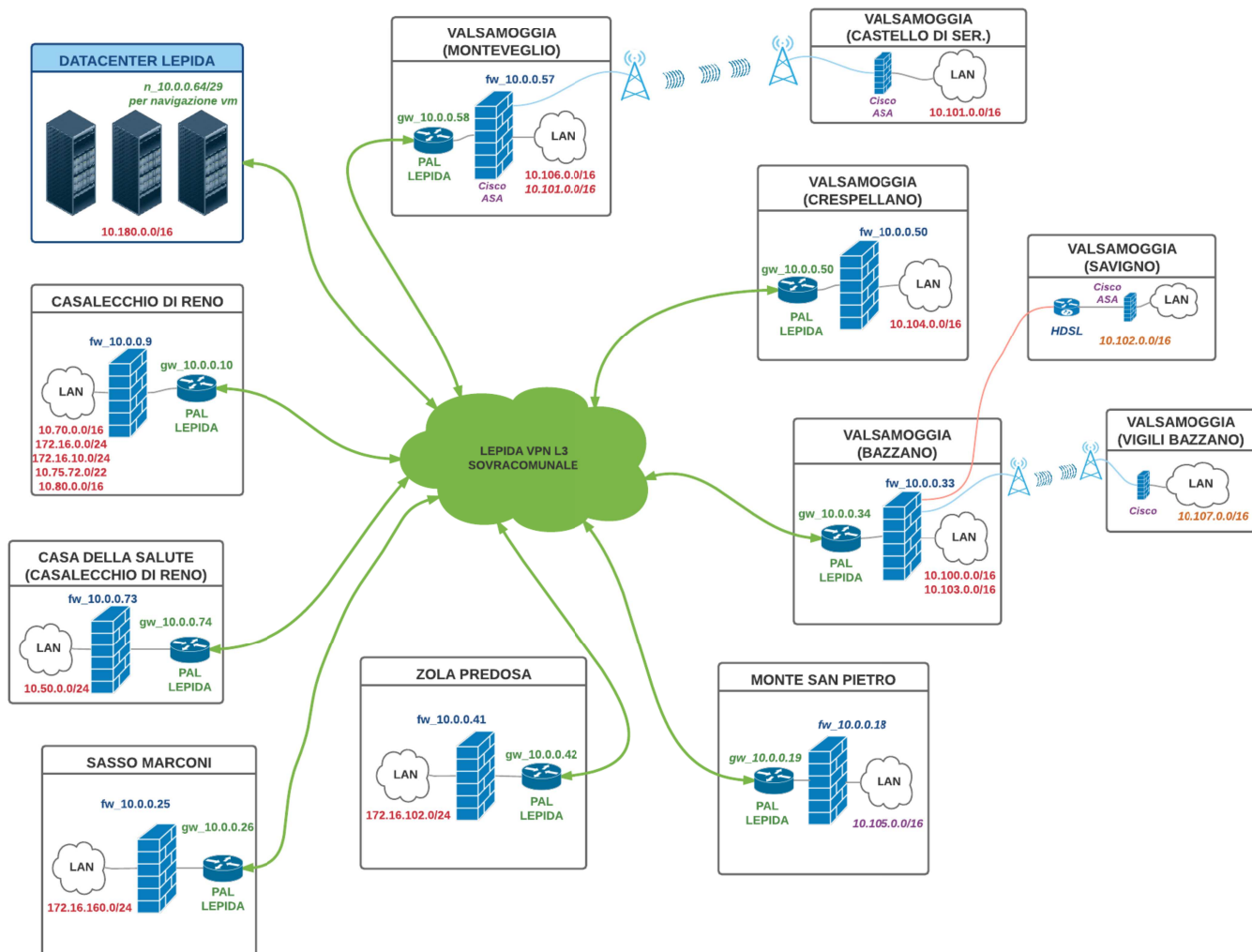
Il datacenter di Lepida è basato totalmente su un'architettura virtualizzata tramite tecnologia Microsoft Hyper-v e prossimamente VmWare.

In base agli enti e/o alle tipologie di applicazioni, le stesse applicazioni possono essere installate sulle postazioni di lavoro, oppure distribuite tramite tecnologie a terminale grafico Citrix o Remote Desktop Service.

Si incoraggia infine l'uso e l'adozione di applicazioni web richiedenti l'uso principalmente o esclusivamente di un browser web.

Schema rete logica VPN L3 dell'Unione Reno Lavino Samoggia

NETWORK SOVRACOMUNALE



Si procederà nelle pagine seguenti a riportare gli elenchi dei server fisici, server virtuali **solo** del Comune di Casalecchio. Tali elenchi “fotografano” la situazione ad oggi, che come esplicito nelle premessa non rappresenta la situazione a regime, a termine del progetto di migrazione, che prevede lo spegnimento dei server fisici e la ristrutturazione e installazione dei server virtuali su una nuova infrastruttura esterna.

Server Fisici

NOME	OS	MODELLO	NOTE
Pollux2k8	Windows Server 2008 R2	HP Proliant DL380	Domain controller, DNS, DHCP alternativo CDR
Datacore-1	Windows Server 2008 R2	HP Proliant DL380 G7	Gestione SAN
Datacore-2	Windows Server 2008 R2	HP Proliant DL380 G7	Gestione SAN
Cluster1-N1	Windows Server 2008 R2	HP Proliant DL380 G6	Fileserver CDR
Cluster1-N2	Windows Server 2008 R2	HP Proliant DL380 G6	Fileserver CDR
Xen 110	Citrix Xenserver Host 6.5	HP Proliant DL380 G5	Server per la Virtualizzazione
Xen 111	Citrix Xenserver Host 6.5	HP Proliant DL380 G5	Server per la Virtualizzazione
Xen 112	Citrix Xenserver Host 6.5	HP Proliant DL380 G5	Server per la Virtualizzazione
Xen 115	Citrix Xenserver Host 6.5	HP Proliant DL380 G6	Server per la Virtualizzazione
Xen 116	Citrix Xenserver Host 6.5	HP Proliant DL380 G6	Server per la Virtualizzazione
Xen 117	Citrix Xenserver Host 6.5	HP Proliant DL380 G6	Server per la Virtualizzazione
Xen 130	Citrix Xenserver Host 6.5	HP Proliant DL380 G7	Server per la Virtualizzazione
Xen 131	Citrix Xenserver Host 6.5	HP Proliant DL380 G7	Server per la Virtualizzazione
Xen 132	Citrix Xenserver Host 6.5	HP Proliant DL380 G7	Server per la Virtualizzazione
Srvrac1	Red Hat Linux	HP Proliant DL380 G8	Oracle
Srvrac2	Red Hat Linux	HP Proliant DL380 G8	Oracle
Cluster 8-N1	Windows Server 2003 R2	HP Proliant DL380	SQL e Progress
Cluster 8-N2	Windows Server 2003 R2	HP Proliant DL380	SQL e Progress
Hyperstream-1	Windows Server 2008 R2	HP Proliant DL380 G5	Backup
Hyperstream-2	Windows Server 2008 R2	HP Proliant DL380 G5	Backup
Allarmi	Linux	HP Proliant DL360 G7	gestione Allarmi SIA
Perseus	Windows Server 2008 R2	HP Proliant DL585	Backup
Teseo	Windows Server 2008 R2	HP Proliant DL585	Backup
Titano	Windows Server 2003 R2	HP Proliant DL380	Server Biblioteca
Sophos Email Appliance	OS Proprietario	Sophos ES 1100	Sophos Email Appliance
Centralino	OS Proprietario	Digium Switchbox 365	Centralino
Videosorveglianza	Linux	HP StorageWorks X1600 G2	Videosorveglianza PM
Mercurio	Windows Server 2008 R2	HP Proliant DL380	Fileserver

Server virtuali

NOME	OS	COMMENTI
Archiflow	Windows Server 2003 R2	
Arcmail	Debian 6	archivio posta Mdaemon
Pensioni 2	Windows XP Professional	Macchina per l'installazione di pensioni INPDAP
Webapp08	Windows Server 2008 R2	
Fax	Windows Server 2008 R2	Gestione Fax
Pensioni 3	Windows XP Professional	Macchina client programma Pensioni
Persone	Windows Server 2003 Standard	Applicativo Persone per il servizio Tributi
Plutone	Windows Server 2003 R2	Archivio di Posta Lotus Notes (Domino 7.04)
Webapp09	CentOS 6.6	Application Server gestione Rifiuti (R.U.S.C.O.), cfr Luca Pomi
Anacner	CentOS 6.3	Anacner
Segreteria	Windows 7 Professional	
SITECO	Windows Server 2003 R2	WebServices e MapServer
Srvman	Red Hat 6.4	
AldebaranBCK	Windows Server 2008 R2	Backup di Aldebaran (vecchio server posta Mdaemon)
Castor2k8	Windows Server 2008 R2	Domain controller, DNS, DHCP alternativo CDR
Kiwano	Windows Server 2003 R2	File Server ASC
Meucci	Windows Server 2003 R2	
NetscalerCDR	FreeBSD 8.4	
Pataia2k8	Windows Server 2008 R2	File Server ASC
Aldebaran	Windows Server 2008 R2	vecchio server posta Mdaemon
LicenzeAutocad_1	Windows XP Professional	server licenze vecchie Autocad 2006
Patch	Windows Server 2003 R2	server antivirus Sophos CDR
Webapp03	Red Hat 5	Server Tomcat per applicazioni SIT
Webapp04	CentOS 5.9	Tomcat per la gestione di applicativi atti e protocollo, pubblicazione atti, albo applicativo e pubblico, ad4web, Surf e Semplice, Fornitori. Il servizio si chiama tomcat7atti
Webapp07	CentOS 6.3	Tomcat per la gestione di Garsia Il servizio si chiamano jbossSOFTECH
Webserver01	Windows Server 2003 R2	sito web istituzionale Comune di Casalecchio
Webserver02	Windows Server 2003 R2	applicativi web vari CDR
Winwkf	Windows XP Professional	Windows Workflow ADS
Xenbiblio01	Windows Server 2003 R2	Distribuzione applicativi biblioteca via Citrix
Xenbiblio02	Windows Server 2003 R2	Distribuzione applicativi biblioteca via Citrix
Xenbiblio03	Windows Server 2003 R2	Distribuzione applicativi biblioteca via Citrix

Xenconsole	Windows Server 2003 R2	Distribuzione applicativi biblioteca via Citrix
Xenpvs02	Windows Server 2008 R2	Provisioning applicativi biblioteca via Citrix
LicenzeAutocad_2	Windows XP Professional	server licenze vecchie Autocad 2006
Nibiru	Windows Server 2003 R2	ex Perseus (Backup)
Printerserver	Windows Server 2008 R2	gestione stampanti di rete
Sitserver	Windows Server 2003 R2	gestione cartografia (cfr. Luca Pomi)
Webapp05	CentOS 5.9	Tomcat per la gestione di ASC: protocolloasc.cdr.local Tomcat ASC - Workflow ASC - Si4cs ASC - Http Il servizio si chiama tomADS
Webapp06	CentOS 5.9	Tomcat per la gestione del workflow e di si4cs I servizi si chiamano si4cs e workflow
Corsi2k8	Windows Server 2008 R2	Distribuzione applicativi macchine Corsi via Citrix
Ospiti	Windows Server 2008 R2	Programma Ospiti ASC
Durian2k8	Windows Server 2008 R2	Distribuzione applicativi ASC via Citrix
Acai2k8	Windows Server 2008 R2	Distribuzione applicativi ASC via Citrix
Pepino2k8	Windows Server 2008 R2	Distribuzione applicativi ASC via Citrix

Descrizione dei sistemi informativi

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

Il processo di omogeneizzazione dei software ha interessato in maniera prioritaria i servizi conferiti in maniera associata all'Unione, come per il Servizio Personale Associato che ha adottato un software unico per la gestione Giuridica ed un'altro unico per la gestione Economica.

Sempre nel processo di omogeneizzazione dei software nel corso del 2016 sono stati unificati i software:

- per la gestione della posta elettronica e di collaborazione e groupware
- antivirus

e nel corso del 2017 verrà adottato un software unico per tutti i Comuni dell'Unione per la gestione di SUE, SUAP.

Per tutte le altre tipologie di sistema informativo ogni Comune ad oggi ha conservato i propri. Di seguito vengono quindi riportati i sistemi informativi e le relative modalità di gestione e dispiegamento del solo Comune di Casalecchio di Reno.

Denominazione	Device o DB Server	Dati	Modalità di Dispiegamento	Fornitore
Sinfecon	Pratiche delle attività produttive	dati sui server SQL	Client/Server, autenticazione specifica	
Anagrafe del Comune di Bologna	Demografici (anagrafe, stato civile, saia, elettorale)	dati c/o Comune di Bologna	Client/Server, autenticazione specifica	Comune di Bologna
Sebina	Biblioteca	Dati c/o CIB	via Web	Università di Bologna
CG4	Controllo di gestione	dati sui server Oracle	Client/Server, autenticazione specifica	ADS
Babylon	Inventario	dati c/o ditta GIES		Gies
STR	Pratiche dei lavori pubblici	dati sui server SQL	Client/Server, autenticazione specifica	
Mosaico	Contabilità lavori pubblici	dati sui server Progress	Client/Server, autenticazione specifica	Data Management
Nettare	Gestione interventi lavori pubblici	dati sui server Oracle		

Serpico	Gestione giuridico-economica del personale – Contabilità - Cassa economale STORICO	dati sui server Progress	Client/Server, autenticazione specifica	Data Management
JobTime	Gestione di timbrature e cartellini	dati sui server Oracle	via Web, autenticazione specifica	Infoline
Polcity	Pratiche di polizia municipale	dati su Advantage Db Server	Client/Server, autenticazione specifica	Open Software
Saturn	Gestione turni personale polizia municipale	con dati sui Db Access		
Prisma	Protocollo	dati sui server Oracle	via Web, autenticazione LDAP	ADS
Sfera	Delibere e determine	dati sui server Oracle	via Web, autenticazione LDAP	ADS
Sosia	Gestione rette scolastiche e servizi sociali	dati sui server Oracle	Client/Server, autenticazione specifica	Softech
Garsia	Servizi socio-sanitari	dati sui server Oracle	via Web, autenticazione specifica	Softech
Gradus	Graduatorie alloggi	con dati sui Db Access	Client/Server, autenticazione specifica	Softech
Thebit	Tributi e fiscalità locale	dati sui server Oracle	Client/Server, autenticazione specifica	Engeneering
Anagrafe Canina	Anagrafe canina	dati c/o la Regione Emilia Romagna	Client/Server, autenticazione specifica	
Conedil	Pratiche dell'edilizia privata	dati su server Domino	tramite Lotus Notes	
Argo	Gestione accessi sportello polifunzionale	dati sui server SQL	via Web, autenticazione specifica	
Surf	Gestione pratiche Sportello polizunfionale	dati sui server Oracle	via Web, autenticazione specifica	
Amsefc	Gestione contratti cimiteriali	dati sui server Progress		
Utenze	Gestione utenze	dati su server Domino	tramite Lotus Notes	
Carburanti	Gestione veicoli	dati su server Domino	tramite Lotus Notes	

Oggetti Smarriti	Gestione oggetti smarriti	dati su server Domino	tramite Lotus Notes	
Contratti	Gestione gare di acquisto e relativi contratti	dati su server Domino	tramite Lotus Notes	
Sinistri Assicurativi	Gestione pratiche di risarcimento danni	dati su server Domino	tramite Lotus Notes	
Entratel	Invio comunicazioni INPDAP all'Agenzia delle Entrate	Procedura stand-alone	Client/Server, autenticazione specifica	
Sare	Invio comunicazioni assunzioni e cessazioni al centro per l'impiego	Procedura stand-alone	Client/Server, autenticazione specifica	
GE770	Invio 770 all'Agenzia delle Entrate	Procedura stand-alone	Client/Server, autenticazione specifica	
F24	Invio F24 all'Agenzia delle Entrate	Procedura stand-alone	Client/Server, autenticazione specifica	
Sophos	Antivirus		Server Web PATCH	
Termtalk	Acquisizione marcature marcatempo			Infoline
Time Navigator	Backup			
Google Apps	Posta elettronica, Drive, Calendari	dati c/o server Google	via Web, autenticazione specifica	
Sibak	Ragioneria	dati sui server Progress	via Web, autenticazione specifica	Data Management
Casa di Vetro	Trasparenza	dati sui server Oracle	via Web, autenticazione LDAP	ADS
Raccomandate	Gestione Raccomandate		via Web, autenticazione specifica	Istrice (Fabio Mosti)
Gestinfrazioni	Gestione Infrazioni PM		Client/Server, autenticazione specifica	Sapignoli
Tares	Servizio Tributi	dati su server Persone	via Web, autenticazione specifica	AdvancedSystem
IUC	Servizio Tributi	dati su server Persone	via Web, autenticazione specifica	AdvancedSystem
Gestimp	Servizio Tributi	dati su server Persone	via Web, autenticazione specifica	AdvancedSystem
Osap	Servizio Tributi	dati su server Persone	via Web, autenticazione specifica	AdvancedSystem
ORCART	Gestione Flotta Auto Comunale	dati su server ORCART	via Web, autenticazione specifica	ORCART

Analisi dei rischi

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 dovrà procedere ad elencare i rischi cui sono soggetti i dati informatici ed i dati cartacei trattati dagli incaricati degli enti.

Elenco dei rischi dei dati elettronici

I rischi cui possono essere soggetti i dati sono i seguenti:

- accesso indebito alle risorse sia da parte di personale interno non autorizzato, che da parte di soggetti esterni non autorizzati o malintenzionati
- rischi connessi alla trasmissione dati
- perdita dei dati o parte di essi e relativo intaccamento della loro integrità
- errori operativi volti a minare l'integrità logica dei dati
- azioni dolose
- manomissioni o furti
- eventi dannosi o disastrosi

Per ciò che concerne i rischi contestualizzati su ciascuna tipologia di dati e rischi e le azioni intraprese e da intraprendere ed i relativi strumenti per fronteggiare tali rischi si rimanda al termine della fase migrazione al Datacenter di Lepida, con un apposito nuovo piano di sicurezza informatica globale per tutta l'Unione.