REGIONE AUTONOMA
FRIULI VENEZIA GIULIA

Italian Cyber Security Report 2014

L'esperienza della R. A. Friuli – Venezia Giulia

Presidenza della Regione – Direzione Generale
Servizio Sistemi Informativi ed E-Government

1. Introduzione

1.1 Sistema Informativo Integrato Regionale (SIIR)

- Ente Regione, Enti locali, Aziende sanitarie, Enti strumentali
- Infrastrutture comuni di comunicazione di rete, di calcolo e applicative
- Servizi condivisi a vantaggio delle PA e di tutta la popolazione e delle imprese che agiscono sul territorio
- Gestione integrata della sicurezza
- CERT - raFVG

2. Contesto

2.1 Presentazione del Friuli-Venezia Giulia

- Regione Autonoma, istituita con la legge costituzionale n.1 del 31 gennaio 1963.
- Regione a statuto speciale, dispone di forme e condizioni particolari di autonomia sotto il profilo politico, legislativo, amministrativo e finanziario.
- Impegno primario nel settore ICT, funzionale all'attuazione del dettato legislativo di autonomia.
- Sistema Informativo Integrato Regionale, ex L.R. n. 9 del 14/7/2011, chiave di volta per poter garantire una gestione integrata e trasversale delle realtà e dei fenomeni che insistono sul proprio territorio.

3. Evoluzione dei servizi IT in RAFVG

3.1 Evoluzione giuridica

- Legge regionale 27 aprile 1972, n. 22 “Istituzione di un sistema informativo elettronico di interesse regionale…”), focus non solo all'Ente Regione ma esteso a tutte le PPAA del territorio regionale (trasversalità ed integrazione)
- Nascita di Insiel S.p.a. (Informatica Friuli-Venezia Giulia – 1972, assetto attuale con scorporo attività non in-house - 2009)
- Legge regionale 14 luglio 2011, n. 9 “Disciplina del sistema informativo integrato regionale del Friuli Venezia Giulia”

3. Evoluzione dei servizi IT in RAFVG

3.2.1 Ruolo e funzioni attuali dell'IT in Regione

- Ente Regione
  - Progettazione, organizzazione, sviluppo del sistema informativo e telematico regionale per le attività istituzionali
  - Coordinamento del SIIR per consentire interoperabilità, integrazione, miglioramento dei servizi, efficienza ed efficacia dei processi amministrativi
  - Monitoraggio della diffusione e dello sviluppo delle ICT sul territorio regionale e valutazione dei risultati raggiunti
  - Pianificazione, regolamentazione e monitoraggio dell'interoperabilità e della sicurezza dei sistemi e delle reti pubbliche

3. Evoluzione dei servizi IT in RAFVG

3.2.2 Ruolo e funzioni attuali dell'IT in Regione

- Insiel
  - Attività regolata dalla Legge Regionale 9/2011
  - Conduzione e Sviluppo del SIIR
  - Soggetto Responsabile del trattamento dei dati personali di cui la Regione è Titolare, ai sensi del D.Lgs. 196/2003
  - Soggetto attivo nell'adozione delle misure di sicurezza previste dal D.Lgs. 196/2003

3. Evoluzione dei servizi IT in RAFVG

3.3 Contesto infrastrutturale e applicativo attuale

- Portfolio di soluzioni applicative comuni a disposizione di Enti Locali e Aziende Sanitarie.
- Data center regionale per l'erogazione di servizi applicativi ed infrastrutturali in modalità "Cloud" per Ente Regione, Enti Locali e Aziende Sanitarie.
- Rete Pubblica Regionale in fibra ottica per il collegamento di tutte le PA del territorio, completata entro fine 2015 (Progetto ERMES).
- Infrastruttura centralizzata di cyber security per garantire il monitoraggio e la sicurezza di quanto indicato nei punti precedenti facendo rientrare nel perimetro di sicurezza regionale tutte le realtà che usufruiscono di detti servizi.

3. Evoluzione dei servizi IT in RAFVG

3.4 Azioni previste nel periodo 2014-2018

- Piano Strategico Regionale 2014-2018, approvato con deliberazione della Giunta regionale n. 1332 dell'11 luglio 2014:
  - Sviluppo di un Data Center a beneficio del territorio;
  - Completamento del programma Ermes per la costruzione della Rete Pubblica Regionale in fibra ottica;
  - Sviluppo di un sistema di gestione informatizzata delle procedure di acquisto per la nuova Centrale Unica di Committenza, al servizio delle PPAA regionali;
  - Coordinamento dello sviluppo dei sistemi informativi a livello locale e introduzione del nuovo sistema finanziario-contabile (a regime dal 2015);
  - Garanzia di accesso in banda larga a tutte le scuole per lo sviluppo della cultura digitale.

4. La gestione della sicurezza IT in RAFVG

4.1 Breve cronistoria

- Sistema nato e sviluppatosi a partire dagli anni '70, utilizzato da sempre per il trattamento di dati legati alle attività della PA, sia interne sia inerenti a cittadini e imprese, con forte attenzione alla sicurezza informatica.
- Nei primi anni sviluppo del sistema basato su un modello centrale con architettura mainframe con una rete ad estensione limitata e perimetro ben definito e controllato, concetto di sicurezza legato alla protezione del dato in termini di disponibilità delle risorse, integrità dei dati e sicurezza degli accessi fisici.
- Con l'evoluzione tecnologica verso sistemi dipartimentali e la maggiore disponibilità di connettività sono emerse ulteriori esigenze. La normativa sulla protezione dei dati personali ha ribadito la necessità di far evolvere il sistema di sicurezza per coprire maggiormente gli aspetti legati alla riservatezza delle informazioni e il controllo degli accessi, per minimizzare il rischio di accessi non autorizzati ai dati personali.
- Allo stato attuale, nel contesto dei servizi distribuiti e del Cloud, sono state introdotte contromisure quali i sistemi di accesso centralizzati, sistemi di controllo dei flussi di traffico, sistemi di protezione a più livelli, ma anche misure di formazione, sensibilizzazione e responsabilizzazione nei confronti degli operatori, il tutto nell'ottica di indirizzare in maniera coerente i rischi connessi con il trattamento delle informazioni stesse.

4. La gestione della sicurezza IT in RAFVG

4.2 Elementi caratteristici del modello IT Security RAFVG

- Portfolio di soluzioni applicative comuni messo a disposizione di Ente Regione, Enti Locali e Aziende Sanitarie (link: goo.gl/zj4cnR);
- Data center regionale, dal quale vengono erogati servizi applicativi ed infrastrutturali in modalità “Cloud” verso l'Ente Regione, gli Enti Locali e le Aziende Sanitarie ed Ospedaliere;
- Infrastruttura centralizzata di cyber security, che garantisce il monitoraggio e la sicurezza di quanto indicato nei punti precedenti facendo rientrare nel perimetro di sicurezza regionale tutte le realtà che usufruiscono di detti servizi quali:
  - Protezione antimalware, anche “cloud”;
  - Canale di navigazione Internet protetto;
  - Posta elettronica protetta;
- CERT (Computer Emergency Response Team) raFVG, punto di riferimento per le attività di sicurezza informatica in ambito regionale. I suoi servizi sono erogati da Insiel e sono una parte di quelli previsti dall’ "Handbook for CSIRTs" (Computer Security Incident Response Team).

4. Continuità operativa

4.1 Continuità operativa

- Aderenza Linee guida Agid
- Nuovo progetto Disaster Recovery 2014-2015
  - Adeguamento Data Center Primario
  - Utilizzo infrastrutture già esistenti, anche di altre PA, per garantire DR e CO

5. Cultura organizzativa della sicurezza ICT

5.2 CERT - raFVG

- Il CERT – ra FVG nasce nel 2005 come punto di riferimento per le attività di sicurezza informatica in ambito regionale. I servizi rientranti nell'ambito vengono erogati normalmente tramite Insiel S.p.A. e sono una parte di quelli previsti dall' "*Handbook for CSIRTs*" dove CSIRT sta per *Computer Security Incident Response Team*.
- In ottica evolutiva, le azioni di sviluppo previste per il Sistema Informativo Integrato Regionale volte a favorire l'integrazione e la centralizzazione dei servizi estenderanno naturalmente il perimetro delle attività quali la gestione degli incidenti e la disponibilità di misure tecnologiche da mettere a fattor comune a beneficio dei servizi erogati per gli Enti del territorio.

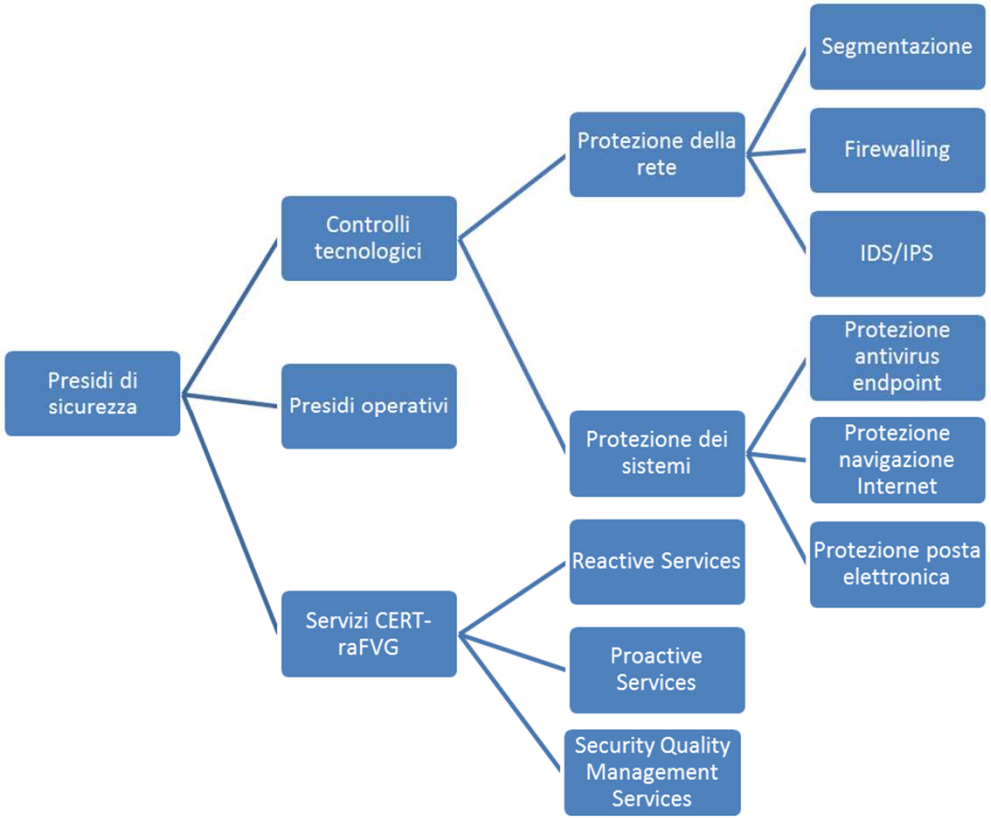
5. Cultura organizzativa della sicurezza ICT

5.3 Security Summit FVG

- Organizzato nel maggio 2013 in collaborazione con CLUSIT (Associazione italiana per la sicurezza informatica) con l'obiettivo di portare nelle amministrazioni locali della Regione Friuli-Venezia Giulia competenze e "best practice" per una corretta gestione della sicurezza delle informazioni
- Rivolto ad un pubblico di utenti, anche non specializzati, costituito principalmente da responsabili di enti ed amministrazioni locali, con l'obiettivo di:
  - Aumentare la conoscenza delle delicate problematiche tecnologiche, organizzative, legali e gestionali connesse alla sicurezza delle informazioni e quindi incrementare la cultura della sicurezza;
  - Diffondere i concetti di base e le "buone prassi" della Ict Security presso i dipendenti delle Pubbliche Amministrazioni locali, che per il loro ruolo utilizzano computer con applicazioni di tipo "office" e che hanno relazioni con l'interno e l'esterno della Pubblica Amministrazione attraverso email, navigazione siti, scambio file, utilizzo di nuovi dispositivi (smartphone, tablet) ecc…
  - Approfondire, anche a beneficio degli addetti ai sistemi IT e/o alla sicurezza ICT, alcuni temi specialistici di particolare interesse ed attualità.

6. IT security presso RAFVG

6.1 Presidi di sicurezza



6. IT security presso RAFVG

6.2 Presidi operativi Data Center Regionale

Attività proattive / reattive per l'identificazione dell'anomalia	Monitoraggio e controllo	Sono in uso tecnologie di monitoraggio dotate di appositi controlli che segnalano eventuali situazioni di attenzione o malfunzionamento. In base alle specifiche operative, il personale a presidio effettua le varie azioni per riportare alla normalità la situazione segnalata;
	Presidio telefonico	Sugli ambiti di servizio più critici viene garantito un presidio telefono h24 per ricevere eventuali segnalazioni di malfunzionamento o per eseguire qualsiasi operazione di supporto al personale Insiel per garantire la migliore operatività e i livelli di servizio;
Attività proattive / reattive per la risoluzione dell'anomalia	Interventi di primo livello	In base alle segnalazioni provenienti dai sistemi di monitoraggio, o da segnalazioni di altra natura (telefoniche o via e-mail) il personale a presidio provvede agli interventi di primo livello per correggere eventuali situazioni di malfunzionamento;
	Escalation	In caso di necessità il personale a presidio contatta il supporto specialistico per assistenza su eventuali malfunzionamenti. Il supporto specialistico viene garantito mediante presenza in sede durante il normale orario di lavoro o reperibilità, al di fuori di tale orario, relativamente ad un set definito di servizi.

6. IT security presso RAFVG

6.3 CERT - raFVG

Reactive Services	Proactive Services	Security Quality Management Services
Alerts and Warnings	Announcements	Risk Analysis
Incident Handling	**Technology Watch**	Business Continuity and Disaster Recovery Planning
Vulnerability Handling	**Security Audits or Assessments**	**Security Consulting**
Artifact Handling	Configuration and maintenance of Security Tools, Applications, and Infrastructures	**Awareness Building**
	Development of Security Tools	**Education/Training**
	Intrusion Detection Services	Product Evaluation or Certification
	Security-Related Information Dissemination	

fonte: www.cert.org

REGIONE AUTONOMA
FRIULI VENEZIA GIULIA

Riferimenti

Paolo PANONTIN
Assessore alla funzione pubblica, autonomie locali, coordinamento delle riforme, caccia e risorse ittiche, delegato alla protezione civile
assessorefunzionepubblica@regione.fvg.it

Antonina RISTAGNO
Direttore Ufficio Stampa – RAFVG
antonina.ristagno@regione.fvg.it

Luca MORATTO
Direttore Servizio SIEG – RAFVG
luca.moratto@regione.fvg.it

Paolo AGATI
paolo.agati@regione.fvg.it
Referente Cyber Security Report 2014 - RAFVG

Alessandro MASOLIN
alessandro.masolin@insiel.it
Resp. Area Data Center Services – Insiel S.p.a.

Diego MEZZINA
diego.mezzina@insiel.it
Referente Area IT Security – Insiel S.p.a.

Direzione centrale Funzione pubblica, autonomie locali e coordinamento delle riforme
Servizio Sistemi Informativi ed E-Government