CYBER SECURITY REPORT 2014

CASE STUDY 2: l'esperienza della regione Friuli Venezia Giulia

Indice dei Contenuti

1. **Executive Summary** ... 3

2. Introduzione ... 4

3. Contesto: presentazione della Regione Friuli Venezia Giulia ... 4

4. Breve storia dell'evoluzione dei servizi IT in Regione ... 5

4.a. Ruolo e funzioni attuali dell'IT in Regione ... 5

4.a.i. **Il contesto attuale** ... 5

4.a.ii. **Azioni previste nel quadriennio 2014-2018** ... 6

5. La gestione della sicurezza IT in Regione FVG ... 6

5.a. **Breve cronistoria** ... 6

5.b. **Organizzazione attuale** ... 7

5.b.i. **Identificazione elementi caratteristici del modello IT Security della Regione** ... 9

5.c. Continuità Operativa ... 9

5.c.i. **Premessa** ... 9

5.c.ii. **Affidabilità dei sistemi e gestione ordinaria** ... 10

5.c.iii. **Gestione delle attività di manutenzione programmata** ... 11

5.c.iv. **Gestione degli eventi straordinari** ... 11

5.c.v. **Tecnologie di riferimento** ... 12

6. **La cultura organizzativa della sicurezza ICT in Regione: policy di sicurezza, formazione, sensibilizzazione** 13

6.a. **CERT – raFVG** ... 13

6.b. **Organizzazione del Security Summit FVG** ... 14

7. Appendice: IT security presso la Regione Friuli Venezia Giulia ... 15

7.a. **Presidi di sicurezza** ... 15

7.a.i. **Presidi operativi Data Center Regionale** 16

7.a.ii. **Cert raFVG** 17

Specializzazione delle risorse umane 19

7.b. Strategie per la definizione di policy di sicurezza 20

7.b.i. **Accesso utente ai sistemi** 20

7.b.ii. **Accesso ad Internet** 20

7.b.iii. **Accesso ospiti** 21

7.c. **Application security** 21

7.d. **Information security (confidenzialità, integrità, autenticazione e non ripudio)** 21

7.d.i. **Gestione dei cambiamenti HW e SW** 21

7.d.ii. **Politica di backup** 22

7.d.iii. **Regole per l'installazione del software sulle postazioni di lavoro.** 22

1. Executive Summary

Scopo del presente documento è illustrare come vengono affrontate le problematiche relative alla sicurezza ICT nell'ambito del Sistema Informativo Integrato Regionale (SIIR) della Regione Autonoma Friuli-Venezia Giulia, partendo dal quadro normativo di riferimento (4. **Breve storia dell'evoluzione dei servizi IT in Regione**) e da una breve descrizione del contesto attuale e degli sviluppi a breve e medio termine. Il documento prosegue poi descrivendo gli elementi caratteristici del modello di IT Security del SIIR e la suddivisione delle competenze nella gestione della sicurezza ICT tra Ente Regione e società in-house (Insiel S.p.a.) (5. **La gestione della sicurezza IT in Regione FVG**).

Ampio spazio viene dedicato alla gestione della Continuità Operativa (5.c. Continuità Operativa) con particolare riguardo alle problematiche del Disaster Recovery (5.c.iv. Gestione degli eventi straordinari) per poi affrontare gli aspetti relativi alla Cultura organizzativa della Sicurezza (6. La cultura organizzativa della sicurezza ICT in Regione: policy di sicurezza, formazione, sensibilizzazione) nel cui ambito si introducono le attività del CERT – raFVG (6.a. CERT – raFVG), che svolge importanti funzioni di consulenza e disseminazione di conoscenza in campo IT Security.

Da ultimo, nell'appendice (7. Appendice: IT security presso la Regione Friuli Venezia Giulia e successivi), vengono riassunti gli aspetti più tecnici dell'IT Security regionale, partendo dai Presidi di sicurezza (7.a. Presidi di sicurezza) nel cui contesto sono descritte più estesamente le tipologie di attività del CERT – raFVG e passando per le strategie utilizzate nella definizione delle politiche di sicurezza (7.b. Strategie per la definizione di policy di sicurezza), la valutazione della sicurezza delle applicazioni (7.c. Application security).

2. Introduzione

Il sistema ICT della Regione Friuli-Venezia Giulia e del suo territorio ha subito una lunga e complessa evoluzione che, partendo da una realtà scarsamente informatizzata e dominata dai sistemi centralizzati quale quella dei primi anni '70, ha portato alla situazione attuale in cui possiamo dire di disporre di un Sistema Informativo Integrato Regionale (SIIR) che comprende, oltre all'Ente Regione stesso, la maggior parte delle PA del territorio (enti locali, enti del sistema socio sanitario, enti pubblici economici) e mette a fattor comune infrastrutture di comunicazione di rete, infrastrutture applicative nonché un'ampia gamma di servizi, a vantaggio non solo delle PA in senso stretto ma di tutta la popolazione e delle imprese che agiscono sul territorio.

Parlando di un sistema integrato uno degli aspetti chiave dell'integrazione è la gestione dell'IT Security, che ha subito anch'essa un'analoga e fondamentale evoluzione, partendo dal mondo monolitico dei mainframe anni '70 sino a giungere alla realtà complessa e multiforme del Cloud in tutte le sue declinazioni odierne. Scopo di questo documento è dunque illustrare, per quanto sinteticamente, l'approccio all'IT Security da parte della Regione Friuli-Venezia Giulia, dando conto sia degli aspetti organizzativi e culturali che di quelli più eminentemente tecnici andando a toccare alcuni degli aspetti più rilevanti quale ad esempio la realizzazione del CERT - raFVG.

3. Contesto: presentazione della Regione Friuli Venezia Giulia

La Regione Autonoma Friuli Venezia Giulia è stata istituita con la legge costituzionale n.1 del 31 gennaio 1963. E' una Regione a statuto speciale e come tale dispone di forme e condizioni particolari di autonomia sotto il profilo politico, legislativo, amministrativo e finanziario all'interno di uno Stato che per la sua Costituzione "riconosce e promuove le autonomie locali".

In virtù della "specialità", lo Stato ha affidato alla Regione una gamma di compiti o, come si dice, di funzioni pubbliche più ampia rispetto a quella attribuita alle Regioni a statuto ordinario. La Regione Friuli Venezia Giulia è così responsabile del sistema sanitario regionale (degli ospedali e delle aziende sanitarie, della spesa farmaceutica, dell'assistenza domiciliare, ecc.), delle politiche di sostegno del diritto allo studio, dell'industria, del commercio, dell'artigianato, dell'agricoltura e del turismo, della caccia e della pesca, delle funzioni di assistenza sociale, del finanziamento dei comuni, delle province e delle comunità montane, delle strade regionali, delle politiche di sostegno delle zone svantaggiate di confine, delle misure di tutela delle minoranze linguistiche, di alcune politiche dell'ambiente, del demanio marittimo, degli interventi di protezione civile.

L'impegno primario dell'Ente Regione nel settore ICT nasce proprio da quanto sopra enunciato ed è funzionale all'attuazione del dettato legislativo di autonomia: la realizzazione di un Sistema Informativo Integrato Regionale, previsto dalla L.R. n. 9 del 14/7/2011 (di cui si dirà in seguito) è la chiave di volta per poter garantire una gestione integrata e trasversale delle realtà e dei fenomeni che insistono sul proprio territorio, senza la quale sarebbe impossibile ottenere gli obiettivi di efficacia, efficienza, coordinamento, consolidamento, razionalizzazione della spesa e sviluppo omogeneo che la Regione si è prefissa.

4. Breve storia dell'evoluzione dei servizi IT in Regione

L'attenzione verso il mondo dell'ICT in Friuli-Venezia Giulia nasce da lontano: già nel 1972 venne promulgata la prima legge organica sull'informatica (Legge regionale 27 aprile 1972, n. 22 "Istituzione di un sistema informativo elettronico di interesse regionale ed intervento a favore del Centro di calcolo dell'Università di Trieste") e, in maniera sorprendente per i tempi, il focus era rivolto non solo all'Ente Regione e alle sue "dipendenze" strette ma veniva esteso a tutte le PPAA del territorio regionale anticipando i concetti di trasversalità ed integrazione. A seguito della promulgazione della Legge n. 22 nasce Insiel S.p.a. (all'epoca Informatica Friuli-Venezia Giulia), inizialmente partecipata tra Italsiel e l'Azienda Ospedaliera Udinese: la società evolve nel tempo, venendo acquisita al 100% da RAFVG nel 2005 per assumere l'assetto definitivo nel 2009 con lo scorporo delle attività non in-house e il reintegro del ramo d'azienda finalizzato alla realizzazione della rete regionale in banda larga.

Si arriva così all'impianto legislativo attuale, definito dalla Legge regionale 14 luglio 2011, n. 9 "Disciplina del sistema informativo integrato regionale del Friuli Venezia Giulia" in cui non a caso si parla di sistema informativo integrato, inteso come l'insieme degli asset ICT (basi dati, software, servizi, infrastrutture) delle PPAA che operano sul territorio regionale. La Regione assume in questo contesto un ruolo di indirizzo, coordinamento e controllo del Sistema Informativo Integrato Regionale (con apposito rilievo per ciò che riguarda gli aspetti della sicurezza) ponendosi gli obiettivi di aumento dell'efficacia e dell'efficienza complessiva del sistema, razionalizzazione complessiva degli oneri nel settore ICT, sviluppo dell'interoperabilità ICT tra i vari soggetti facenti parte del SIIR, sviluppo uniforme e omogeneo delle funzionalità attinenti al SIIR ed infine di promozione della trasparenza (open data). La gestione operativa del sistema viene poi affidata, mediante apposito disciplinare, ad Insiel che assume a sua volta il ruolo di attuatore e gestore del SIIR.

4.a. Ruolo e funzioni attuali dell'IT in Regione

4.a.i. Il contesto attuale

Riprendendo quanto detto nei paragrafi precedenti, il risultato complessivo dello sforzo normativo ed organizzativo messo in atto sinora è una infrastruttura che è nata, sin dal 1972, come un sistema integrato all'interno del quale le PPAA del territorio regionale beneficiano di una serie di servizi e infrastrutture messe a fattor comune dall'Ente Regione, ed in particolare:

- Portfolio di soluzioni applicative comuni messo a disposizione di Enti Locali e Aziende Socio Sanitarie ed Ospedaliere;
- 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;
- Rete unitaria della PA regionale, che potrà avvalersi entro la fine 2015 del completamento del progetto "Ermes" (realizzazione Rete Pubblica Regionale in fibra ottica) collegando tutte le PA del territorio;
- 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.

Il processo di consolidamento ed evoluzione prosegue con molteplici ed importanti attività: per la Sanità sono stati avviati progetti quali il Fascicolo Sanitario Elettronico, la Prescrizione e la Dematerializzazione delle ricette, il collegamento in rete dei Medici di Medicina Generale e i Pediatri di Libera Scelta, il Progetto PACS. Nell'ambito degli

Enti Locali invece è ormai disponibile un repertorio applicativo che copre la quasi totalità delle esigenze di informatizzazione degli enti. A questo si è aggiunto nel corso del 2014 un servizio Cloud in modalità IaaS rivolto specificamente agli EELL e sarà attivato tra breve un servizio VoIP a favore delle amministrazioni territoriali.

4.a.ii. **Azioni previste nel quadriennio 2014-2018**

Nel Piano Strategico Regionale 2014-2018, approvato con deliberazione della Giunta regionale n. 1332 dell'11 luglio 2014, sono anche indicate le linee di azione secondo cui si muoverà lo sviluppo della ICT regionale nel prossimo quadriennio. Come detto più volte, assumono particolare importanza le azioni che hanno una valenza trasversale e sono rivolte all'integrazione, tra queste ricordiamo in breve le più significative, alcune delle quali già menzionate in precedenza:

- Sviluppo di un Data Center a beneficio del territorio;
- Completamento del programma Ermes per la costruzione della Rete Pubblica Regionale tramite il collegamento con infrastrutture a banda larga di tutti i comuni della regione e le strutture sanitarie;
- Coordinamento dello sviluppo da parte di Insiel di un sistema di gestione informatizzata delle procedure di acquisizione di beni e servizi finalizzato alla realizzazione di una Centrale di Acquisto al servizio delle PPAA regionali;
- Coordinamento lo sviluppo dei sistemi informativi a livello locale e, in questo ambito, introduzione del nuovo sistema finanziario-contabile derivante dall'armonizzazione dei bilanci pubblici (a regime dal 2015), accompagnando gli enti locali al fine di costruire un sistema consolidato;
- Garanzia di accesso in banda larga a tutte le scuole per lo sviluppo della cultura digitale.

5. La gestione della sicurezza IT in Regione FVG

5.a. **Breve cronistoria**

Il sistema informatico regionale, nato e sviluppatosi a partire dagli anni '70, è stato da sempre utilizzato per il trattamento di informazioni legate alle attività della pubblica amministrazione, sia interne sia ovviamente inerenti ai cittadini. E in tale contesto la sicurezza informatica è sempre stato argomento rilevante.

Nei primi anni dello sviluppo del sistema, sostanzialmente basato su un modello centrale con architettura mainframe con una rete ad estensione limitata e perimetro ben definito e controllato, il concetto di sicurezza era per lo più legato alla protezione del dato in termini di disponibilità e integrità. Trovavano quindi spazio contromisure legate a controlli sull'elaborazione, salvataggio dei dati oltre a controlli stringenti sull'accesso alle risorse di elaborazione centrali. Il tutto completato da procedure di controllo degli accessi fisici e gestione dell'emergenza e dell'operatività specifiche in caso di indisponibilità del sistema informatico.

Con la progressiva transizione tecnologica verso sistemi dipartimentali e la contestuale migliore connettività disponibile agli Enti sono emerse ulteriori esigenze: l'introduzione della 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.

Sono quindi progressivamente 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 e sensibilizzazione, accompagnate da atti di responsabilizzazione degli operatori, il tutto nell'ottica di indirizzare in maniera coerente i rischi connessi con il trattamento delle informazioni stesse.

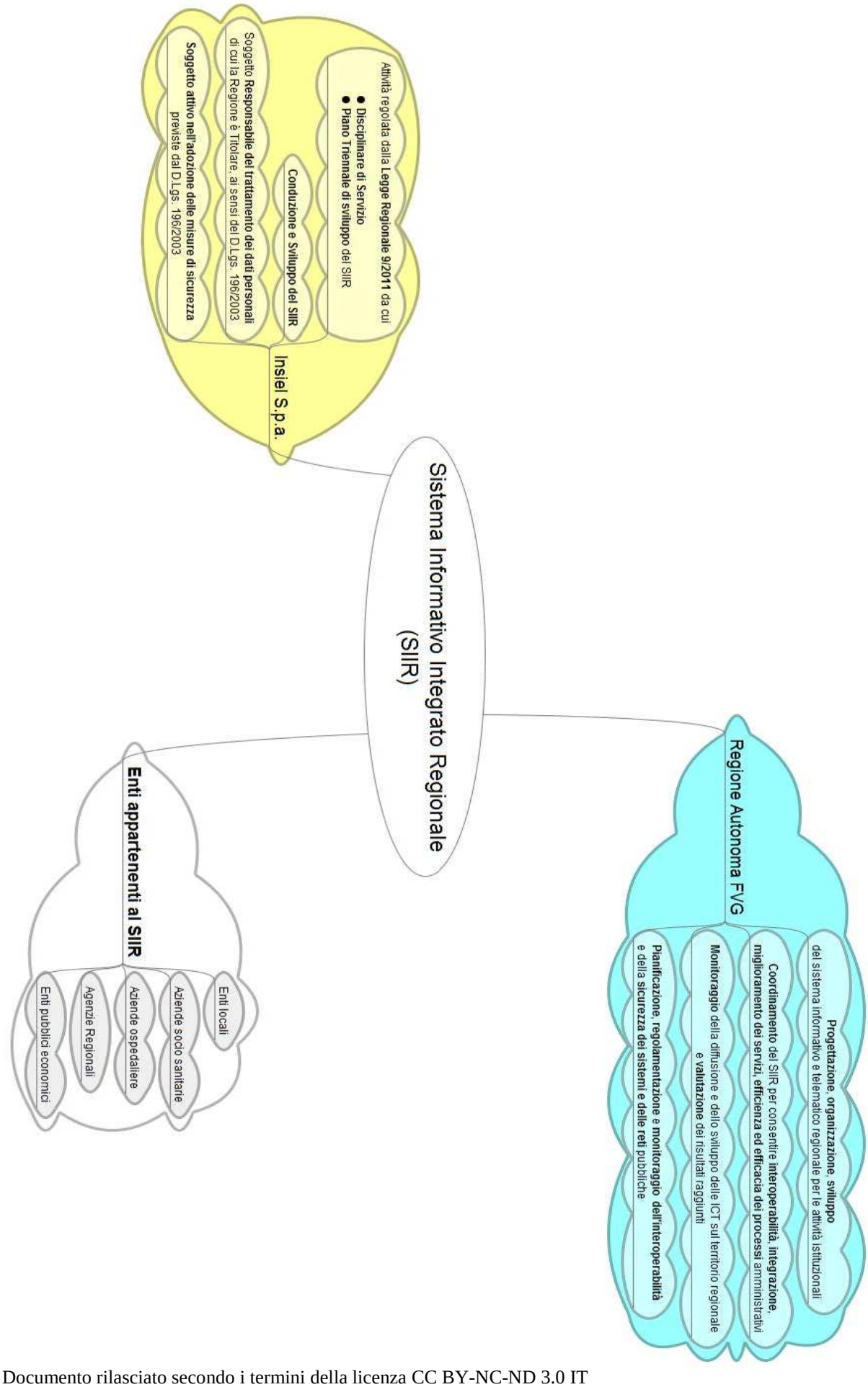
5.b. Organizzazione attuale

Attualmente il sistema informativo integrato regionale (SIIR) del Friuli-Venezia Giulia è disciplinato secondo quanto disposto dalla Legge Regionale 14 luglio 2011, n.9.

Il dettato legislativo prevede che l'Ente Regione promuova lo sviluppo, la diffusione e l'utilizzo integrato delle tecnologie dell'informazione e della comunicazione (ICT) nelle pubbliche amministrazioni del proprio territorio e nella società regionale al fine di favorire:

- lo sviluppo organico e integrato sul territorio regionale della società dell'informazione in coerenza con il contesto normativo comunitario e nazionale;
- il miglioramento della qualità della vita dei cittadini nel rapporto con le pubbliche amministrazioni del territorio regionale e la promozione dello sviluppo economico del territorio favorendone la competitività;
- lo sviluppo di infrastrutture e servizi innovativi idonei a potenziare la cooperazione, l'efficienza e la capacità di servizio delle amministrazioni pubbliche del territorio regionale

In tale contesto i soggetti che contribuiscono alla erogazione del SIIR, anche in termini di sicurezza informatica, sono la Regione e la società informatica in-house Insiel. Il dettaglio dei ruoli assunti dai due attori principali (RAFVG e Insiel) è definito di seguito.



5.b.i. **Identificazione elementi caratteristici del modello IT Security della Regione**

Gli elementi caratteristici del modello del sistema informativo integrato regionale (SIIR) sono quelli evidenziati nei punti precedenti, e mirano a premiare il concetto di integrazione tra i soggetti presenti sul territorio.

Quindi pur operando in presenza di realtà (enti e aziende) che possiedono e fanno valere la propria autonomia, il sistema informativo integrato regionale è la chiave di volta per garantire un'unitarietà di paradigmi nei servizi ICT in genere ed in quelli relativi alla sicurezza nello specifico.

Pertanto, anche l'IT Security deve tener conto di tale linea di indirizzo in tutte le sue manifestazioni; grazie al sistema integrato tutti gli enti che rientrano nel suo ambito godono di un meccanismo complessivo di sicurezza e in forza di tale meccanismo devono sottostare ad un insieme di regole , quali la previsione di misure di separazione tra la rete dell'ente e la rete RUPAR-FVG, l'individuazione di un soggetto di riferimento, e l'impegno a implementare nel contesto di riferimento tutte le misure di sicurezza previste dalla normativa, in modo da non costituire una minaccia per la rete regionale e gli altri Enti connessi

L'adesione di un Ente al sistema regionale non comporta tuttavia solamente un impegno da parte di quest'ultimo a rispettare tali misure di sicurezza, ma offre anche la possibilità di fruire di alcuni servizi specifici per la sicurezza IT. In sintesi le misure di sicurezza di cui un Ente connesso può beneficiare sono:

- Protezione antimalware, anche "cloud"
- Canale di navigazione Internet protetto
- Posta elettronica protetta

Tali servizi di sicurezza completano un contesto di "repertorio applicativo" per gli Enti composto da decine di applicazioni il cui dettaglio è reperibile a questo **link: goo.gl/zj4cnR**

5.c. Continuità Operativa

5.c.i. **Premessa**

Insiel eroga oltre 2000 servizi alle aziende socio-sanitarie e ospedaliere, alle direzioni e agli enti locali della regione Friuli Venezia-Giulia.

Un simile contesto ben rappresenta un portfolio completo delle soluzioni che le pubbliche amministrazioni offrono quotidianamente agli operatori, ai cittadini e ai pazienti. Appare perciò evidente come la necessità di assicurare la continuità del servizio, oltre ad un obbligo normato dalle vigenti leggi, diventi una priorità inderogabile. Allo stato attuale è attivo un progetto regionale inerente la revisione di tutte le infrastrutture tecnologiche che, aderendo alle indicazioni di AgID e alle più comuni Best Practices in materia di ICT, si prefigge l'obiettivo di assicurare la continuità operativa di tutti i servizi erogati. Alcuni dettagli del progetto sono disponibili sul sito dell'Amministrazione Regionale seguendo questo **link: http://goo.gl/vnFTTW.**

Tale progetto prevede delle tempistiche sfidanti che includono una fase di testing da concludersi entro dicembre 2014, l'applicazione della protezione di DR ad un primo nucleo di applicazioni entro dicembre 2015, per concludersi nel corso del 2016. Il progetto rientra nell'ambito del Piano Triennale Regionale per il consolidamento e la

razionalizzazione dei CED di tutte le pubbliche amministrazioni che contribuiscono a formare il Sistema Informativo Integrato Regionale (SIIR). I punti cardine del progetto sono sintetizzabili negli obiettivi seguenti :

- adeguare il Data Center primario alle Linee Guida AgID;
- utilizzare infrastrutture già esistenti di altre PA regionali per garantire il Disaster Recovery e la continuità operativa.

Nel prosieguo, non ci si soffermerà sul dettaglio delle fasi di analisi, di disegno e di realizzazione del progetto, che descrivo no un percorso molto specifico ed ampiamente conosciuto e consolidato per gli specialisti di settore. Ci si soffermerà invece sulle esperienze fino ad ora maturate, utilizzate nella definizione dei requisiti di progetto, e sul significato che viene attribuito al concetto di continuità operativa, applicato ad ogni "categoria" di servizi erogati.

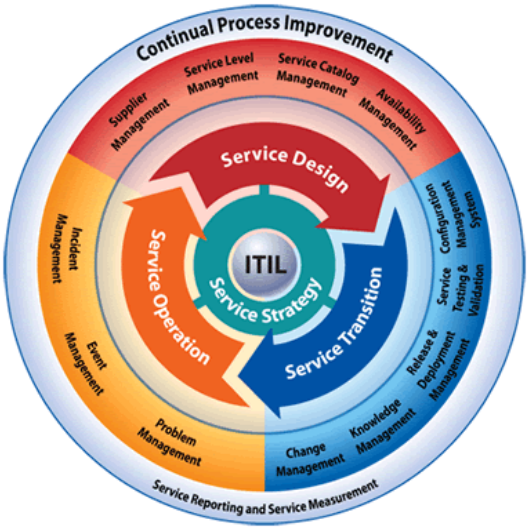
5.c.ii. **Affidabilità dei sistemi e gestione ordinaria**

Affinché i servizi informatici possano essere erogati con continuità e piena rispondenza alle esigenze degli utilizzatori finali, è essenziale ben operare sin dalla fase relativa alla loro **gestione ordinaria**: ci si deve quindi dotare di dispositivi informatici affidabili e gestiti da personale competente, che operi sulla base di processi conosciuti e ben documentati.

In rispondenza a questa affermazione di base, Insiel applica gli accorgimenti di seguito descritti.

1. Robustezza, resilienza ed affidabilità dei dispositivi utilizzati;
2. Eliminazione di ogni "single point of failure" per tutti i servizi erogati. Requisito di base di ogni architettura ospite del Data Center regionale è la duplicazione delle componenti, l'utilizzo di sistemi di alta affidabilità, l'adozione di sistemi di bilanciamento automatico del carico di lavoro. Il più delle volte queste soluzioni sono sviluppate per assicurare la continuità del servizio anche senza l'ausilio di un presidio operativo o sistemistico. Una tipica architettura di riferimento si compone di :
    1. un'infrastruttura di sicurezza finalizzata al controllo del "traffico", dei "contenuti" e degli "accessi" (IDS, IPS, Firewall, Reverse Proxy, …);
    2. un sistema di bilanciamento del carico elaborativo, configurato in modalità ridondata, che distribuisce le transazioni sui server di riferimento;
    3. un livello "application server" configurato in modo che ogni "aggregato", cioè ogni gruppo omogeneo identificato dal servizio ospitato, possa crescere in modo "orizzontale" all'aumentare del carico di lavoro;
    4. un livello " Data Base", in configurazione High Availability, che utilizza la tecnologia che meglio si adatta alla criticità del servizio reso (active-active; active-standby, real cluster, …);
    5. un sistema di monitoraggio del "servizio" ;
3. Utilizzo della metodologiaITIL quale modello riferimento nel disegno dei processi ICT . Alcuni processi sono già stati attivati mentre è in corso la progressiva adozione di quelli restanti. Per meglio specificare, in una prima fase ci si è concentrati sui processi che ITIL identifica all'interno del Service Operation :Incident Management, Problem Management, Monitoring and Control. L'adozione di questi processi, che ha consentito di intervenire in modo efficace principalmente durante la fase di erogazione del servizio, si è concretizzato con

la definizione di un iter che regola il monitoraggio costante finalizzato alla prevenzione degli incidenti e con la definizione di un iter che regola, con interventi rapidi e strutturati, le operazioni di correzione dei guasti conclamati. Sono in fase di sviluppo i processi che ITIL identifica all'interno del Service Transition quali Planning, Change Management, Deployment Management". Successivamente verranno presi in considerazione i processi inerenti il "Service Design" e il "Service Strategy".



5.c.iii. **Gestione delle attività di manutenzione programmata**

Le attività di manutenzione programmata, soprattutto se in riferimento a sistemi informatici critici (es. sistemi ospedalieri) che operano con continuità (in modalità 24x7), devono essere adeguatamente progettate e supportate da idonei dispositivi, al fine di evitare lunghe interruzioni del servizio.

Insiel ha adottato diverse tecnologie che, ognuna applicata alle soluzioni di riferimento, consentono di intervenire senza interruzioni del servizio. In tutto ciò l'utilizzo pervasivo delle tecnologie di virtualizzazione offre un grande aiuto, in quanto rende più flessibili e modulari gli interventi sulle risorse del sistema informatico.

5.c.iv. **Gestione degli eventi straordinari**

In questo ambito ricadono quegli eventi che escono da un contesto ordinario e quindi non gestibili sulla base delle normali procedure operative.

Gli eventi "straordinari" rappresentano le situazioni che obbligano all'innesco del "piano di continuità operativa". Il progetto sviluppato da Insiel, che è in fase di realizzazione, prevede diversi livelli di intervento, volti ad assicurare la continuità del servizio a fronte di tali eventi.

Livello-1 "continuità operativa con replica sincrona dei dati"

In questo contesto vanno considerate le situazioni di "guasto grave", che però non rientrano nelle casistiche assoggettabili ad un piano di disaster recovery

Lo scopo primario di queste procedure è di assicurare la continuità del servizio, garantendo un RPO = 0 (zero data loss). Per raggiungere tale obiettivo verranno utilizzate delle strutture secondarie preesistenti, poste a distanza tale da garantire la replica "sincrona" dei dati gestiti. Tali strutture andranno a formare una "rete di data center" secondari sui quali distribuire i servizi critici, nella logica di protezione degli investimenti già operati dalla PA regionale.

I servizi maggiormente interessati a questa tipologia di protezione sono quelli afferenti all'ambito sanitario-ospedaliero: a fronte di un possibile guasto gli utenti percepiranno solo una breve interruzione del servizio e continueranno a disporre di una base dati congruente e aggiornata.

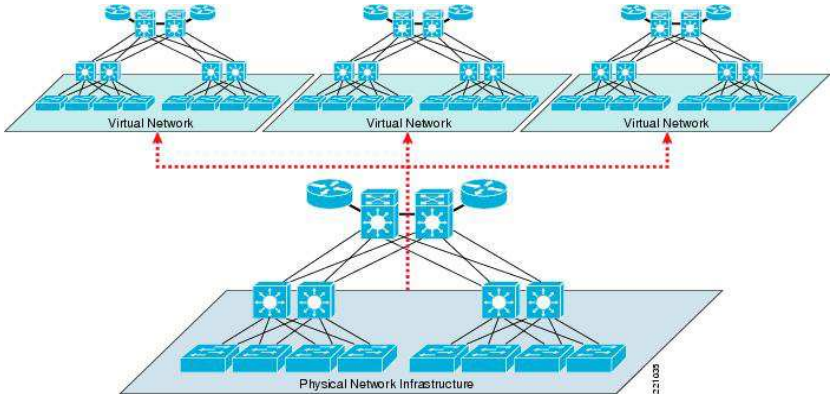
Livello-2 "disaster recovery"

In questo contesto vanno considerate le situazioni di "disastro", che rientrano nelle casistiche assoggettabili ad un piano di disaster recovery.

Le tecnologie e le procedure da utilizzarsi sono quelle necessarie ad assicurare una continuità operativa sulla base di accordi relativamente al massimo tempo di indisponibilità del servizio (RTO) ed al massimo tempo di perdita di aggiornamento dei dati (RPO), per ogni singolo servizio normalmente erogato.

Il ripristino del sito primario alla sua piena funzionalità implica un'importante attività di riallineamento dati e di approvvigionamento/ripristino delle tecnologie. Attualmente è attivo un piano di DR a protezione di un numero limitato di servizi erogati.

Il progetto di DR in fase di attuazione verrà esteso a tutti i servizi ospitati presso il Data Center regionale ed è correlato con l'attività di razionalizzazione delle infrastrutture tecnologiche presenti nel territorio regionale che, coerentemente con le indicazioni di AgID, vede impegnata l'amministrazione regionale nella proposizione di progetti che ne facilitino l'attuazione. In tale contesto è attivo dal mese di Luglio 2014 un servizio denominato "Cloud degli Enti Locali" attraverso il quale viene offerto agli Enti che ne fanno richiesta un "cloud di infrastruttura" (IaaS).



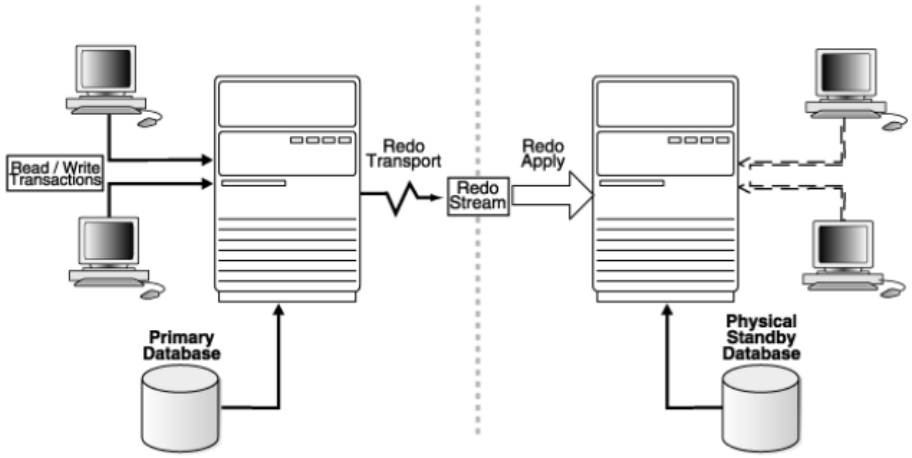
Modello Virtuale a supporto del progetto Cloud

5.c.v. **Tecnologie di riferimento**

Qualsiasi progetto di DR deve essere accompagnato da un'attività propedeutica di razionalizzazione e consolidamento delle infrastrutture ICT che porti all'adozione di specifiche architetture e tecnologie, tali da semplificare la successiva replica di dati e programmi.

Ad oggi oltre il 90% dei servizi attivi presso il Data Center regionale usufruiscono di sistemi virtualizzati. Queste tecnologie hanno facilitato lo svecchiamento del parco hardware installato ed il consolidamento dei sistemi su di un numero limitato di server fisici. Il software di gestione delle infrastrutture virtuali consente inoltre di avere un controllo semplificato dei sistemi installati, del loro effettivo utilizzo e delle risorse necessarie.

Inoltre, per ogni tecnologia utilizzata, sono state acquisite le specifiche “feature” che abilitano al trattamento dei dati e dei sistemi all’interno di architetture volte ad assicurare la continuità del servizio. Tra queste vanno citate le feature che consentono la replica dei dati a livello di “storage subsystem” (mirror, copy, snapshot); gli strumenti che facilitano la replica dei dati dei DB a livello logico (es. standby DB); il software di allineamento e gestione della consistenza delle infrastrutture virtuali.



Esempio di tecnologia di allineamento DB

6. La cultura organizzativa della sicurezza ICT in Regione: policy di sicurezza, formazione, sensibilizzazione

Per quanto riguarda gli aspetti inerenti la cultura della sicurezza IT, che vadano anche oltre alla dimensione puramente tecnologica, la Regione Friuli- Venezia Giulia si è attivata sia verso l’ambito interno alla macchina amministrativa regionale, ma anche rivolti in maniera più estesa ad altre realtà presenti sul territorio.

Per dar conto di ciò vengono citate ed espanse due iniziative: la prima, il CERT – raFVG, rappresenta un esempio di valorizzazione del concetto di sicurezza nei confronti dell’amministrazione interna; la seconda , il Security Summit FVG, rappresenta un esempio di valorizzazione specifica dei temi della sicurezza all’esterno della sola amministrazione regionale, interessando gli altri Enti del territorio del Friuli-Venezia Giulia.

Inoltre, per dare conto ai cittadini delle iniziative inerenti al rispetto e all’armonizzazione con l’agenda digitale italiana, la Regione ha pubblicato nella sezione del proprio portale dedicata all'Agenda Digitale FVG l’elenco delle iniziative intraprese sul fronte della digitalizzazione e della sicurezza.

Infine, il concetto di sicurezza trova spazio nel “Programma triennale per lo sviluppo delle ICT dell'e-government e delle infrastrutture telematiche della Regione Friuli Venezia Giulia per gli anni 2014-2016” con un’apposita sezione dove possono trovare spazio le specifiche iniziative che dovessero essere necessarie o richieste.

6.a. 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 particolare i servizi erogati nel tempo sono i seguenti:

- **Reactive Services**
  - Alerts and Warnings: fornitura di informazioni che descrivano vulnerabilità di sicurezza, intrusioni informatiche, virus o altre minacce e fornitura di indicazioni sulle modalità di comportamento per la gestione del potenziale problema segnalato.
  - Incident Handling: gestione di situazioni di potenziale violazione alla sicurezza informatica
- **Proactive Services**
  - TechnologyWatch: monitoraggio e aggiornamento sul trend delle evoluzioni delle minacce alla sicurezza e della tecnologia di protezione
  - Security Audits or Assessments: verifica periodica dello stato di sicurezza delle infrastrutture gestire per azioni correttive e o migliorative
  - Intrusion Detection Services: protezione e monitoraggio da eventuali attacchi o intrusioni informatiche
- **Security Quality Management Services**
  - Security Consulting: fornitura di linee guida per la realizzazione e l'erogazione dei servizi con adeguati livelli di sicurezza
  - Awareness Building e Education/Training: attività formative e di sensibilizzazione sui temi della sicurezza informatica

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.

6.b. **Organizzazione del Security Summit FVG**

Il "Security Summit FVG" è una iniziativa organizzata 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, mutuando la formula del "Security Summit", principale convegno sulla sicurezza informatica in Italia. Il convegno è stato indirizzato 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.

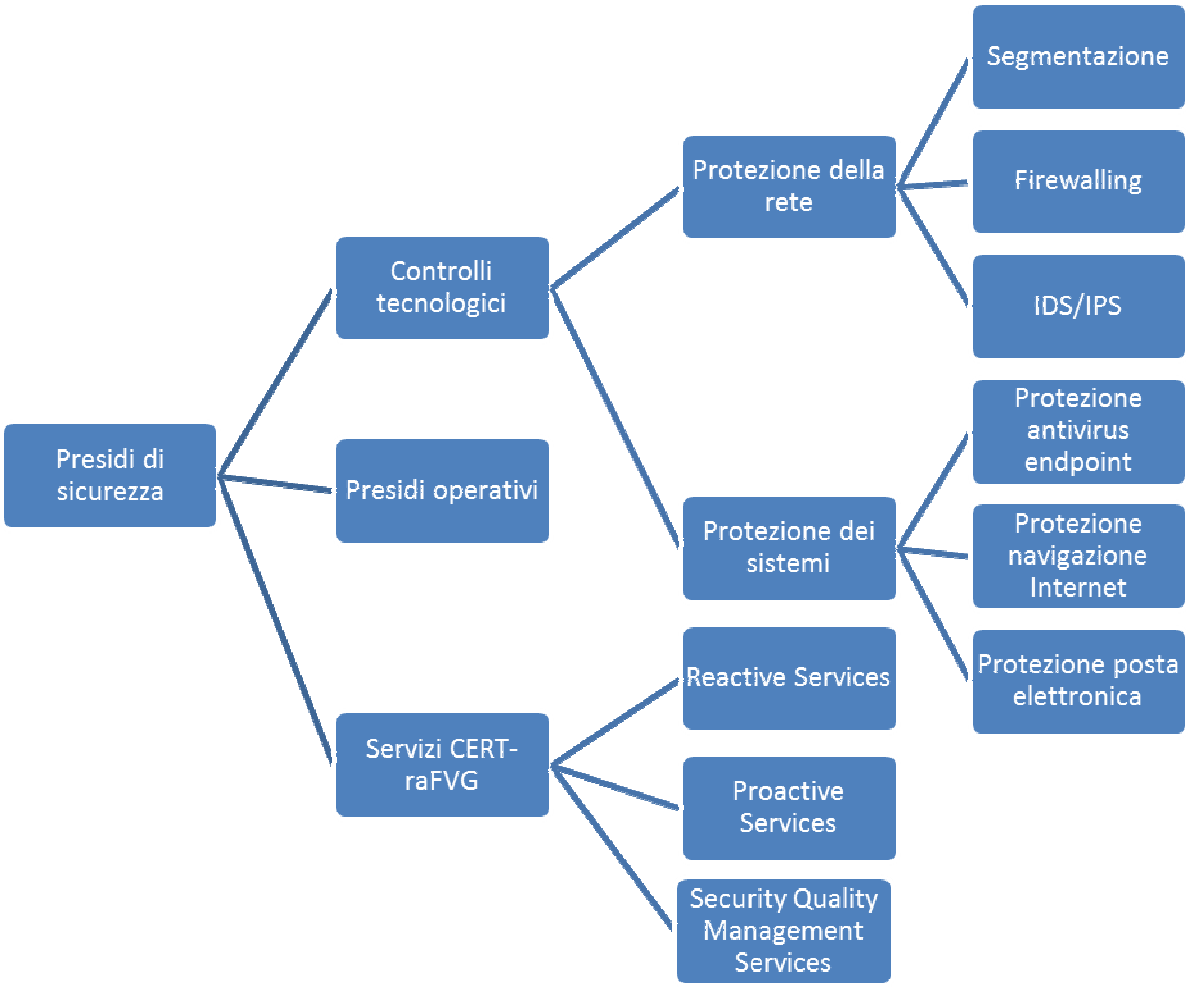
Inoltre per dare conto ai cittadini delle iniziative inerenti al rispetto e all'armonizzazione con l'agenda digitale italiana, la Regione ha pubblicato nella sezione del proprio portale dedicata all'Agenda Digitale FVG l'elenco delle iniziative intraprese sul fronte della digitalizzazione e della sicurezza.

7. Appendice: IT security presso la Regione Friuli Venezia Giulia

7.a. Presidi di sicurezza

I presidi di sicurezza a disposizione del Sistema Informativo Integrato Regionale (SIIR) sono composti sia da controlli tecnologici implementati per ridurre i rischi insistenti sul patrimonio informativo sia da presidi operativi necessari alla loro corretta gestione.

Di seguito un quadro di sintesi che sono stati di seguito descritti a titolo esemplificativo ma non esaustivo:



7.a.i. Controlli tecnologici

Per quanto riguarda i controlli tecnologici , essi comprendono vari elementi come di seguito indicato.

Protezione della rete

L'architettura delle reti gestite prevede l'isolamento dei singoli segmenti in sintonia con i servizi offerti ed i contratti esistenti. Tale segmentazione corrisponde dal punto di vista tecnico alla suddivisione della rete tra i vari Enti connessi alla rete regionale.

La protezione delle reti interne si basa sulla presenza di una struttura di accesso ad Internet a più livelli, separati dai dispositivi firewall. Inoltre, sono implementate politiche di segmentazione delle reti in contesti logici diversi a seconda delle caratteristiche dei servizi erogati.

Da tale punto di partenza, relativamente all'incremento delle capacità di prevenzione e reazione ai tentativi di violazioni esterne, sono in uso sistemi IDS (Intrusion Detection System) e IPS (Intrusion Prevention System).

Protezione antivirus, della navigazione Internet e dalla posta elettronica

Il sistema di protezione antivirus attualmente in uso ha la prerogativa di avere una gestione centralizzata, di provvedere alla distribuzione automatica di tutti gli aggiornamenti . La soluzione adottata è di tipo multi-piattaforma e provvede alla protezione dai malware a più livelli. Una console dedicata provvede al completo monitoraggio delle apparecchiature aventi installato il prodotto antivirus. La stessa rileva la presenza di virus, evidenzia gli elaboratori contagiati, permette la creazione di report sui virus più intercettati, le postazioni interessate e statistiche da cui può essere rilevato il servizio erogato.

Per il controllo antivirus della navigazione via Web viene utilizzato un prodotto specifico, che opera associato logicamente ai server proxy mentre il controllo antivirus della posta elettronica viene effettuato sia a livello di gateway Internet, per la verifica della posta proveniente da Internet, sia a livello dei server di posta Intranet, controllando i messaggi inviati da e verso tali server.

7.a.ii. **Presidi operativi Data Center Regionale**

Il Data Center Regionale viene presidiato 24 ore al giorno da personale Insiel che provvede alle attività necessarie a garantire la regolare operatività dei servizi. Tra le varie attività possiamo individuare:

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.

7.a.iii. **Cert raFVG**

Come già anticipato, il contesto CERT–raFVG raccoglie specifiche attività sulla sicurezza che sono state erogate nel tempo nel contesto dell'amministrazione regionale; esse si possono dividere in tre macrocategorie (*reactive services*, *proactive services*, *security quality management services*). Per ognuna di esse, di seguito dettagliate, nel contesto della regione sono stati erogati un sottoinsieme di servizi, che sono evidenziati in tabella e di seguito descritti

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

Reactive Services - Alerts and Warnings

Questo servizio consiste nel fornire informazioni che descrivano vulnerabilità di sicurezza, intrusioni informatiche, virus o altre minacce e fornire delle indicazioni sulle modalità di comportamento per la gestione del potenziale problema segnalato.

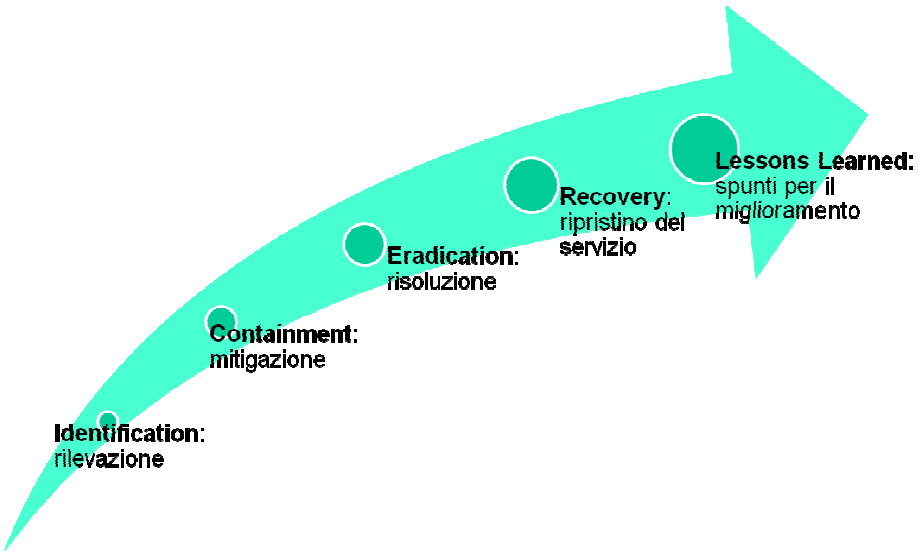
Nel contesto del CERT-raFVG questo servizio viene erogato inviando periodicamente alert relativi a vulnerabilità che superino una soglia di criticità concordata a priori con l'utenza.

Reactive Services – Incident Handling

Questo servizio consiste nel:

1. Identificare le situazioni di potenziale violazione alla sicurezza informatica;
2. Raccogliere le informazioni relative ed analizzarle;
3. Intraprendere azioni di risposta per mitigarne l'impatto, eliminarne le cause e ripristinare le condizioni di regolare servizio.

Le fasi che si possono identificare nell'attività di gestione di un incidente sono le seguenti:



Le fonti di informazione tramite le quali il CERT-raFVG viene a conoscenza di un avvenuto o presunto incidente informatico sono per lo più le seguenti:

1. Segnalazioni dai gruppi tecnici deputati all'erogazione del servizio (gestione dei sistemi regionali)
2. Infrastrutture di protezione implementate nel contesto regionale (a livello host, web, mail)
3. Sistemi di monitoraggio delle infrastrutture regionali
4. Sistemi IDS o IPS

Per avere un dato numerico indicativo sugli attacchi rilevati, intesi come eventi significativi per la sicurezza, si hanno i seguenti parametri:

- ~600.000 eventi gestiti ogni mese dal sistema IPS;
- ~3 milioni di blocchi effettuati ogni mese dal sistema di navigazione web su circa 25.000 utenti;
- ~30.000 malware bloccati ogni mese su circa 20.000 postazioni di lavoro;
- ~30.000 malware bloccati ogni mese su oltre 26.000 caselle di posta;
- ~ 800.000 mail di spam bloccate ogni mese su oltre 26.000 caselle di posta;
- 15 milioni di connessioni rifiutate ogni mese dal sistema antispam in quanto provenienti da spammers.

Proactive Services - Technology Watch

Questo servizio consiste nel monitorare costantemente sia il trend di evoluzione delle minacce alla sicurezza sia l'evoluzione delle tecnologie di protezione. Il personale che opera nel contesto del CERT-raFVG si mantiene aggiornato su queste tematiche attraverso:

- Aggiornamento on-line;
- Confronto con i vendor di tecnologie e servizi di sicurezza;
- Partecipazione a seminari e convegni specifici.

Proactive Services - Security Audits or Assessments

Questo servizio ha l'obiettivo di aumentare la consapevolezza dello stato di sicurezza delle infrastrutture gestite come punto di partenza per azioni correttive/migliorative e per una corretta gestione. Questo servizio è stato erogato

sostanzialmente attraverso attività di Vulnerability Assessment volte ad identificare vulnerabilità esportate sulla rete dalle infrastrutture gestite:

- Scansione;
- Analisi risultati;
- Identificazione interventi correttivi.

Proactive Services - Intrusion Detection Services

Questo servizio ha l'obiettivo di raccogliere informazioni circa la possibile presenza di attacchi o intrusioni informatiche sui sistemi in esercizio per indirizzare più efficacemente la risposta. Questo servizio è stato erogato tramite:

- L'introduzione di sonde con funzione di Network Intrusion Detection System (NIDS) in particolari punti della rete regionale;
- L'introduzione di Host Intrusion Detection System (HIDS) sui sistemi della server farm regionale.

Security Quality Management Services – Security Consulting

Questo servizio ha l'obiettivo di fornire linee guida per la realizzazione e l'erogazione dei servizi con adeguati livelli di sicurezza, nell'ambito di riferimento. Questo servizio è stato erogato tramite il supporto a :

- stesura di linee guida per l'implementazione delle soluzioni;
- stesura di linee guida per lo sviluppo sicuro del software;
- problematiche relative al contesto di sicurezza e protezione.

Security Quality Management Services – Awareness Building e Education/Training

L'obiettivo dell'Awareness Building è la sensibilizzazione dell'utenza sulle criticità in essere, mentre l'obiettivo dell'Education/Training è quello di fornire gli elementi per indirizzare le problematiche di sicurezza, coerentemente con il target di riferimento.

Per erogare questo servizio, nel contesto del CERT-raFVG fino ad ora sono state svolte le seguenti attività:

- Partecipazione alla realizzazione di Corsi e-learning su tematiche di sicurezza/privacy;
- Istituzione sessioni di sensibilizzazione su tematiche e trend di sicurezza;
- Erogazione di sessioni di formazione specifiche su tematiche di sicurezza/privacy.

Le attività nel contesto dei Security Quality Management Services sono attivate a richiesta da parte dell'Amministrazione.

Specializzazione delle risorse umane

I servizi che si possono annoverare nel contesto delle attività del CERT-raFVG sono erogati da personale esperto e certificato sulle tematiche di security e privacy. In particolare le competenze specifiche sono:

- Certificazioni CISSP, Lead Auditor ISO 27001, CISM e altre (Security in SDLC, …);
- Certificazioni di prodotto sulle tecnologie di protezione gestite;
- Conoscenze di tecniche e tool di sicurezza.

7.b. Strategie per la definizione di policy di sicurezza

7.b.i. **Accesso utente ai sistemi**

L'accesso ai sistemi è previsto, per gli utenti dell'amministrazione regionale, solo attraverso il superamento di una procedura di autenticazione/autorizzazione, attuata attraverso un sistema centrale. La gestione delle credenziali è svolta con dei criteri volti a ridurre al minimo la possibilità di violazioni o sottrazioni di identità quali, ad esempio, la lunghezza e la "complessità" della password ed un tempo massimo di validità della stessa.

7.b.ii. **Accesso ad Internet**

Oggi è indispensabile non solo predisporre opportune barriere che filtrino il traffico proveniente dall'esterno, bloccando sul nascere l'ingresso nella rete di contenuti potenzialmente dannosi, ma è necessario anche proteggere le risorse regionali e alle postazioni di lavoro dei dipendenti durante l'accesso a contenuti Internet. In tal senso è stata predisposta una **politica di protezione della navigazione Internet** che prevede:

Autenticazione	l'accesso a Internet avviene solo dopo che è stata eseguita una autenticazione dell'utente/risorsa interna verso un dominio di autenticazione;
Autorizzazione	solo l'utente autenticato ed abilitato alla navigazione Internet potrà effettivamente accedere al servizio di navigazione;
Controllo sui contenuti in base a categorizzazione	la pagina web richiesta verrà effettivamente acceduta solo se tale pagina non appartiene ad una categoria ritenuta non correlata alla attività lavorativa e quindi messa in modalità di blocco
Controllo su contenuti malevoli in base a categorizzazione	l'accesso alla pagina web richiesta verrà bloccata se appartiene ad una categoria ritenuta pericolosa dal punto di vista della sicurezza informatica (Es: siti riconosciuti come potenzialmente pericolosi ossia "Malicious Websites ", siti di phishing, di Spam, etc);
Controllo antivirus sulle pagine e sugli allegati scaricati	ogni pagina web e ogni allegato viene controllato per evidenziare e bloccare eventuali script malevoli e file infetti.

La peculiarità del sistema di accesso, nel contesto regionale, sta nella possibilità di essere configurato secondo le esigenze e le policy del singolo Ente, pur essendo erogato in maniera centralizzata e con tecnologia uniforme.

7.b.iii. **Accesso ospiti**

Per consentire la disponibilità di accesso alla rete anche a persone che occasionalmente hanno necessità di operare nel contesto dell'Amministrazione regionale (ospiti) viene garantito un servizio di connettività Internet attraverso una rete wireless.

Essa è di tipo aperto (senza protocollo di sicurezza e cifratura). Chiunque può collegarsi alla rete e ricevere un indirizzo ip. Gli ip appartengono ad una rete chiusa (segregata) che ha come *default gateway* un *firewall* che accede direttamente ad Internet. Un ospite, prima di poter navigare su Internet deve "superare" un portale di autenticazione. Non ci sono filtri né sui contenuti della navigazione né sui protocolli IP di comunicazione. Le credenziali di accesso vengono fornite da personale regione, abilitato alla creazione di utenti sul server di autenticazione, tramite una pagina web. Le informazioni inserite sono nome, cognome, numero di telefono della sim card italiana (per certi aspetti equivalente alla carta di identità in quanto il provider che ha rilasciato la SIM ha copia della carta di identità dell'utilizzatore della SIM). Le credenziali vengono inviate via sms e restano invisibili al personale che ha creato l'account. L'utente creato può avere validità 1 giorno, 1 settimana, 1 mese e 3 mesi.

7.c. Application security

Nell'ottica di perseguire un livello di protezione adeguato nel contesto delle applicazioni che sono alla base del sistema informativo integrato regionale, sono state intraprese diverse iniziative specifiche, ulteriori rispetto alle iniziative per la sicurezza generali descritte nelle sezioni precedenti, secondo le seguenti direttrici:

- Redazione di specifiche linee guida rivolte al personal e addetto allo sviluppo di applicazioni, con focalizzazione sulle applicazioni web, inerenti lo sviluppo sicuro: in particolare, in maniera coerente con la metodologia OWASP, sono presenti specifiche indicazioni circa le modalità di individuazione e gestione delle principali vulnerabilità riscontrabili in quel contesto
- Previsione di specifici interventi formativi indirizzati allo sviluppo sicuro delle applicazioni web
- Previsione di verifiche di sicurezza, con tool automatici ma anche con l'ausilio di soggetti terzi qualificati, relativamente alle applicazioni componenti il sistema regionale, compatibilmente con le disponibilità.

7.d. Information security (confidenzialità, integrità, autenticazione e non ripudio)

Di seguito vengono elencati alcuni processi relativi ai temi di cui sopra

7.d.i. **Gestione dei cambiamenti HW e SW**

Ogni infrastruttura tecnologica presente presso la server farm della amministrazione regionale ha un suo ciclo di vita che passa attraverso le seguenti fasi:

Progettazione	fase che prende in considerazione tutti i requisiti e formalizza in un documento tutte le componenti hw, sw e i relativi flussi rete/dati necessari all'infrastruttura
Attivazione	fase che consiste nella predisposizione dei sistemi come da progetto
Passaggio in esercizio	fase che consiste nell'avvio delle attività propedeutiche al

	corretto funzionamento del servizio e a garantirne i livelli di servizio previsti quali, ad esempio, le attività di monitoraggio e di backup. Viene innescata a seguito della configurazione della infrastruttura tecnologica e dei test di funzionamento e collaudo.
Richiesta di revisione	fase in cui viene riesaminato il progetto, vengono formalizzate le modifiche generando una nuova versione del documento di progetto e viene richiesta la effettiva modifica dell'infrastruttura; viene innescata nel caso in cui una infrastruttura tecnologica già in esercizio abbia bisogno di essere modificata o aggiornata
Dismissione	Fase che consiste nel liberare tutte le risorse allocate ad un infrastruttura e cessare le attività introdotte nella fase di passaggio in esercizio a garanzia del corretto funzionamento e dell'integrità dei dati; tale fase viene attivata formalmente quando un'infrastruttura deve cessare la sua funzione.

7.d.ii. **Politica di backup**

Come detto precedentemente, all'interno del ciclo di vita delle infrastrutture tecnologiche è presente la fase di passaggio in esercizio che, di fatto, rappresenta il momento in cui l'infrastruttura tecnologica diventa operativa. In questa fase vengono innescate anche alcune attività tra cui quella di backup. Ogni infrastruttura tecnologica prevede una procedura di backup standard con verifica giornaliera degli esiti. In caso una procedura di backup non abbia dato esito positivo, gli operatori della server farm effettuano una verifica sulle relative cause ed innescano, se necessario, l'intervento dei sistemisti di riferimento.

7.d.iii. **Regole per l'installazione del software sulle postazioni di lavoro.**

Nel contesto dell'amministrazione regionale, i PC dei dipendenti prevedono una installazione standard che comprende, oltre al sistema operativo, varie applicazioni di produttività personale secondo quanto concordato con il servizio preposto. L'accesso al PC del dipendente avviene con un utente senza abilitazioni di tipo privilegiato e che non permette l'installazione di nuovo software o la disinstallazione di quello presente. Tale disposizione ha vantaggi sia gestionali sia di sicurezza in quanto da una parte permette di mantenere un parco di installato standard e dall'altra impedisce l'installazione o l'esecuzione di software malevolo (*malware*) con diritti amministrativi.

In caso l'utente abbia bisogno di utilizzare un particolare software per il proprio lavoro che non è presente tra quelli preinstallati sul PC, dovrà seguire una procedura amministrativa che prevede una richiesta che dovrà essere approvata. In seguito il personale tecnico provvederà all'installazione richiesta.