Il rischio informatico, una nuova frontiera per il Risk Management

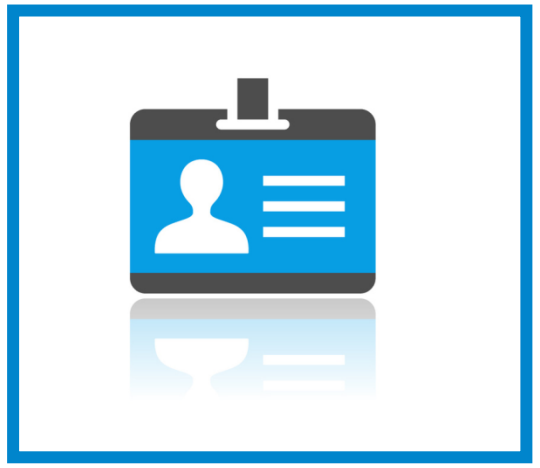
Roberto Pozzuolo
Responsabile Sicurezza, Controlli e Gestione del Rischio Operativo
Banca Sella Holding

Roma, 17 Giugno 2014

AGENDA

- Definizioni e compiti
- La sicurezza informatica nel Gruppo Banca Sella
- Processo di analisi
- Valutazioni ex-ante
- Presidi di controllo in corso di progetto
- Monitoraggio nel continuo
- Gestione degli incidenti informatici
- Gestione degli incidenti informatici nel Gruppo Banca Sella
- Coordinamento funzioni aziendali di controllo e flussi informativi

DEFINIZIONI E COMPITI (1/3)



- ***RISCHIO INFORMATICO (o ICT)***

Rischio di incorrere in perdite economiche, di reputazione e di quote di mercato in relazione all'utilizzo di tecnologia dell'informazione e della comunicazione (ICT – Information and Communication Technology).

Nella rappresentazione integrata dei rischi aziendali a fini prudenziali (ICAAP), il rischio informatico è considerato - secondo gli specifici aspetti - tra i **rischi operativi, reputazionali** e **strategici.**

DEFINIZIONI E COMPITI (2/3)

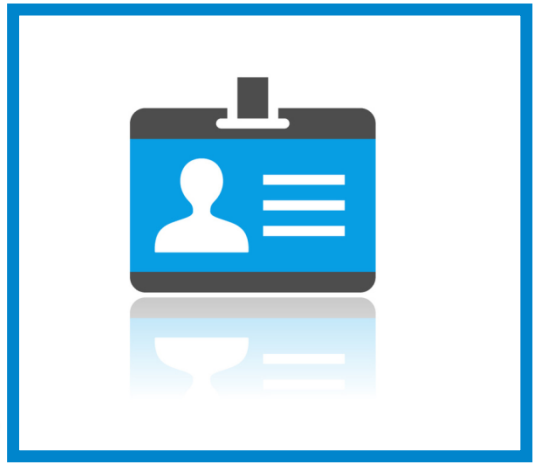
- ***CONTROLLO DEI RISCHI***

La funzione preposta a **garantire il presidio dei rischi**, attraverso flussi informativi periodici relativi all'evoluzione del rischio informatico ed il monitoraggio dell'efficacia delle misure di protezione delle risorse ICT.

- ***SICUREZZA INFORMATICA***

La funzione preposta a svolgere compiti specialistici in materia di sicurezza ICT, tra cui: predisposizione e aggiornamento delle **politiche di sicurezza**, assicurare la coerenza dei **presidi di sicurezza** con le politiche approvate, partecipa alla **progettazione e realizzazione dei presidi di sicurezza** dei data center, concorre alla valutazione del rischio e delle **mitigazioni nell'ambito dell'analisi del rischio informatico, monitoraggio nel continuo delle minacce**, svolgimento **dei test di sicurezza.**

DEFINIZIONI E COMPITI (3/3)



- ***CONTROLLO DEL RISCHIO INFORMATICO E LA COMPLIANCE ICT***

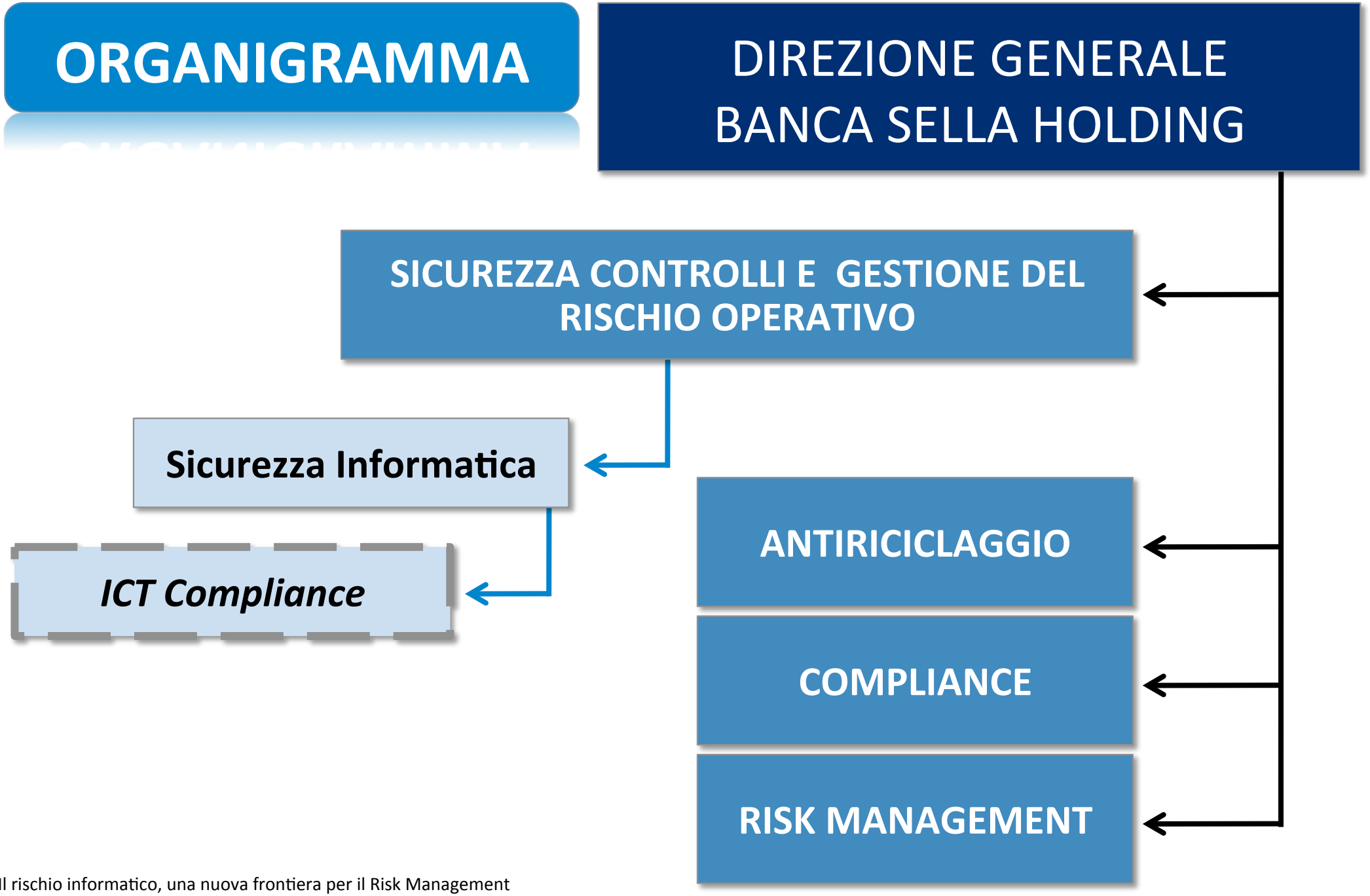
Nell'ambito del sistema dei controlli interni sono chiaramente assegnate responsabilità in merito allo svolgimento dei seguenti compiti di **controllo di secondo livello**:

- ***controllo dei rischi***, basato su flussi informativi continui relativi all'evoluzione del rischio informatico e sul monitoraggio dell'efficacia delle misure di protezione delle risorse ICT;
- ***rispetto*** *dei* ***regolamenti interni*** e delle ***normative esterne*** in tema di ICT (ICT Compliance).

La sicurezza informatica nel Gruppo Banca Sella

- definisce le **politiche di sicurezza logica**, emanando le regole e le linee guida per il Gruppo;
- effettua un **presidio proattivo e costante** volto a **prevenire azioni informatiche nocive**, con particolare attenzione alle infrastrutture tecnologiche;
- propone e promuove **soluzioni tecnologiche di sicurezza logica**;
- effettua, nell'ottica di prevenzione, **test di vulnerabilità sui sistemi** posti su reti esterne o su reti interne;
- **controlla il codice sorgente** delle applicazioni informatiche;
- valuta le **richieste di abilitazione di carattere informatico**;
- gestisce le tematiche relative alla materia di **protezione dei dati personali**.

ORGANIGRAMMA



PROCESSO DI ANALISI (1/2)

Il processo di analisi è svolto coinvolgendo l'utente responsabile, il personale della funzione ICT, le funzioni di controllo dei rischi, di sicurezza informatica e, ove opportuno, l'*audit*, secondo metodologie e responsabilità formalmente definite dall'organo con funzione di gestione.

Esso si compone delle seguenti fasi:

- **valutazione del rischio potenziale** cui sono esposte le risorse informatiche esaminate

➔ **tale attività interessa tutte le iniziative di sviluppo di nuovi progetti e di modifica rilevante del sistema informativo** e prende avvio con la classificazione delle risorse ICT in termini di rischio informatico;

- **trattamento del rischio** volto a individuare, se necessario, misure di mitigazione – di tipo tecnico o organizzativo – idonee a contenere il rischio potenziale.

PROCESSO DI ANALISI (2/2)

L'analisi individua il rischio residuo, da sottoporre ad accettazione formale dell'utente responsabile.

Qualora il rischio residuo **ecceda** la propensione al rischio informatico approvato dall'organo con funzione di supervisione strategica, l'analisi **propone** l'adozione di **misure alternative** o **ulteriori misure di trattamento del rischio**, definite con il coinvolgimento della funzione di controllo dei rischi e sottoposte all'approvazione dell'organo con funzione di gestione.

VALUTAZIONE EX ANTE (1/2)

Livelli di Rischio	
R1	Minimo
R2	Significativo
R3	Rilevante
R4	Critico
R5	Molto Critico
N.R.	Non Rilevato

nca Sella Holding
nagement e Controlli
azione dei Profili di Rischio

Scheda di valutazione dei Profili di Rischio relativo all'implementazione del servizio di Home Banking Dispositivo

Biella, XX/XX/XXXX

Redatto da	
Visto da	

Materiale Esaminato:
-
-

Tipologia di Rischio		Origine del rischio	Gestione del rischio	Controllo del rischio	Criticità Rilevate	Mitigazione delle Criticità	Livelli di Rischio	
							(*)	(**)
Rischio operativo	*Frode Esterna* *Sicurezza dei Sistemi* *Rischio reputazionale*	Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Nam liber tempor cum soluta nobis eleifend option congue nihil imperdiet doming id quod mazim placerat facer possim assum.	Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.			Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.	R2	R1

VALUTAZIONE EX ANTE (2/2)

Livelli di Rischio	
R1	Minimo
R2	Significativo
R3	Rilevante
R4	Critico
R5	Molto Critico
N.R.	Non Rilevato

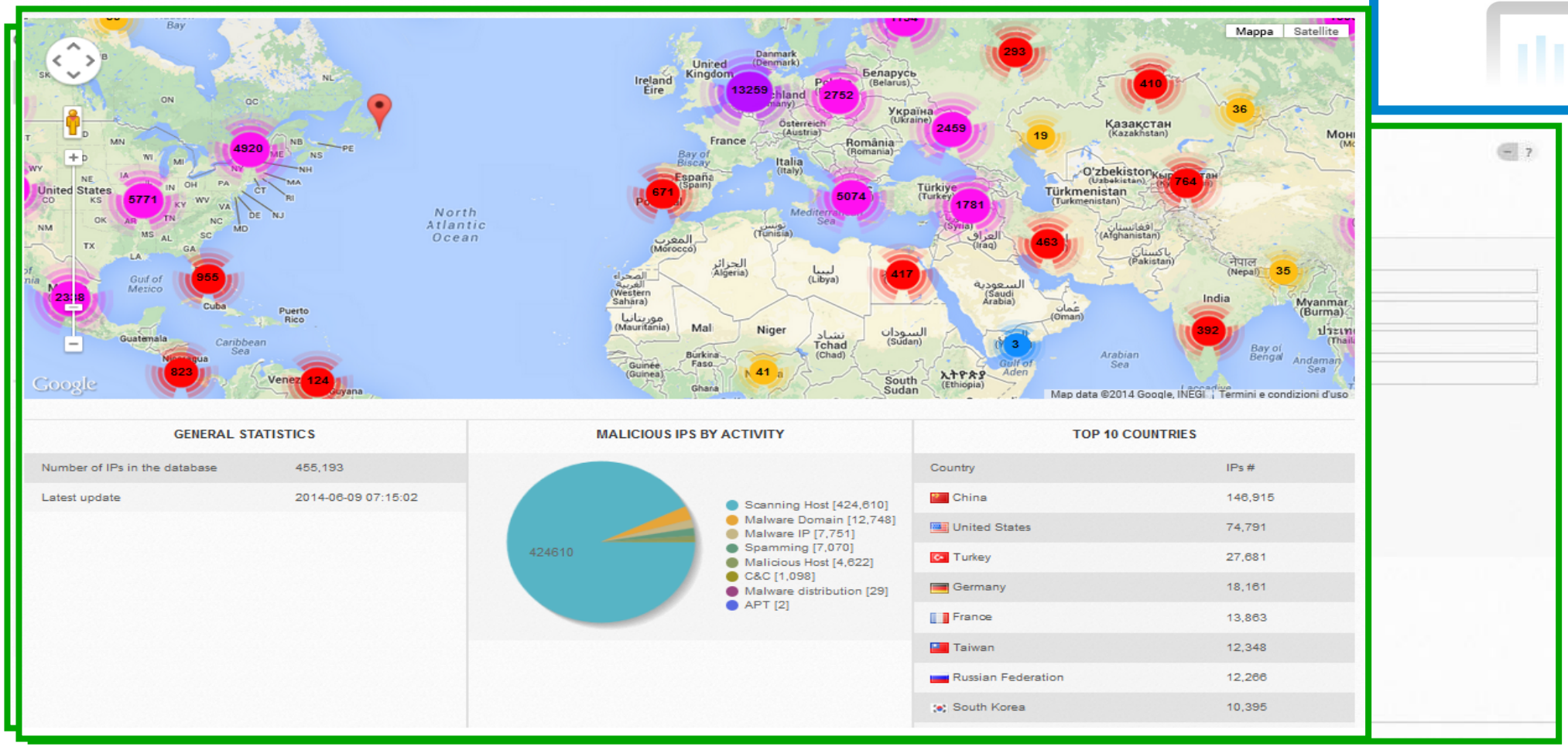
COMITATO RISCHI OPERATIVI

Il **Comitato Rischi Operativi** ha la funzione di esaminare, valutare e autorizzare operazioni, modelli organizzativi, lancio di nuovi prodotti, avvio di nuove attività ed in genere **ogni possibile iniziativa generatrice di rischi operativi, reputazionali, strategici, legali e di compliance**.

PRESIDI DI CONTROLLO IN CORSO DI PROGETTO

RAP	RIUNIONE ANALISI PROGETTI Le strutture preposte valutano ed analizzano nel dettaglio le soluzioni organizzative individuate, rilevando gli eventuali rischi operativi legati al progetto
CAR	CONTROLLO ARCHITETTURA - PARTECIPANO COMPONENTI DELLE FUNZIONI ICT, SICUREZZA INFORMATICA E OWNER DEL PROGETTO Valuta l'architettura del progetto in relazione agli standard interni ed esterni
CMIP	CONTROLLO MESSE IN PRODUZIONE Verifica l'effettiva adozione degli standard e che gli impegni assunti nelle valutazioni precedenti siano stati recepiti; verifica che siano state eseguite prima del rilascio in produzione ulteriori attività di controllo

MONITORAGGIO NEL CONTINUO



GENERAL STATISTICS

Number of IPs in the database	455,193
Latest update	2014-06-09 07:15:02

MALICIOUS IPS BY ACTIVITY

TOP 10 COUNTRIES

Country	IPs #
China	146,915
United States	74,791
Turkey	27,681
Germany	18,161
France	13,863
Taiwan	12,348
Russian Federation	12,266
South Korea	10,395

GESTIONE DEGLI INCIDENTI INFORMATICI (1/2)

La gestione degli incidenti di sicurezza informatica segue **procedure formalmente definite**, con l'obiettivo di **minimizzare l'impatto** di eventi avversi e garantire il **tempestivo ripristino** del regolare funzionamento dei servizi e delle risorse ICT coinvolte.

Le funzioni a cui comunicare l'incidente sono individuate secondo un'opportuna **procedura di escalation**; i casi più gravi che comportino rischi di **interruzione della continuità operativa** sono segnalati alla **struttura preposta a dichiarare lo stato di crisi**.

GESTIONE DEGLI INCIDENTI INFORMATICI (1/2)

ESTRATTO POLICY DI SICUREZZA INFORMATICA

CAPITOLO 12 - Incident Response.

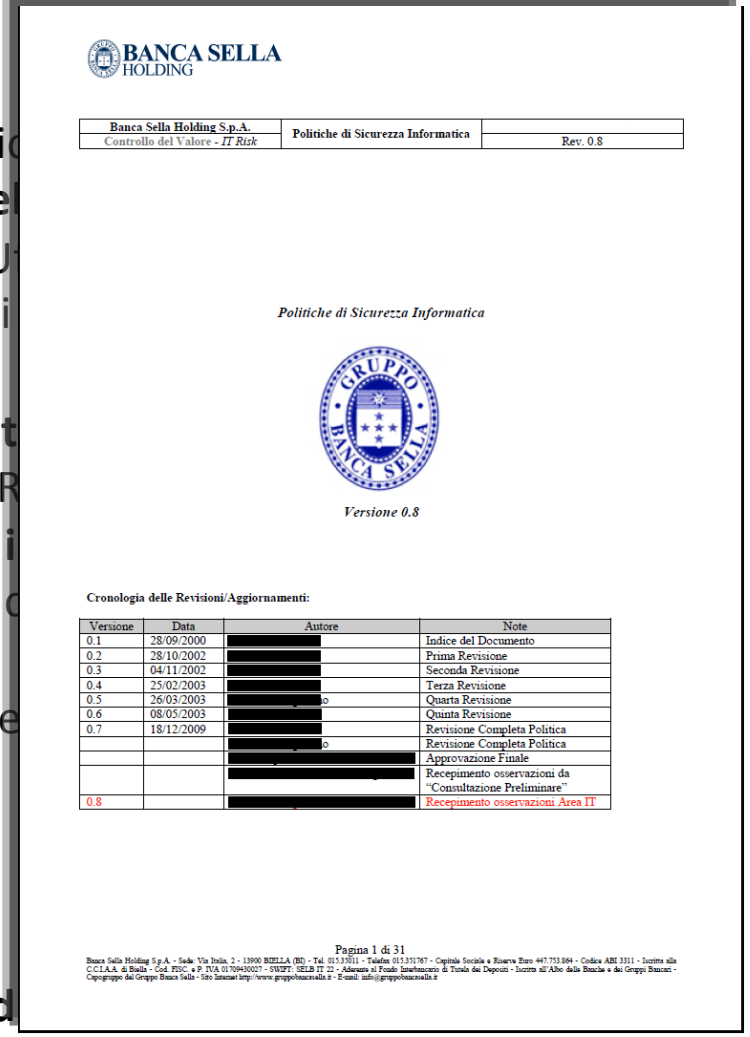
Ogni utente che abbia il sospetto di un incidente informatico (ad esempi
informare immediatamente il proprio responsabile e il responsabile de
(referente per la Sicurezza Informatica), che avranno cura di fornire all'U
dettagliata descrizione del rilevamento seguendo la classificazione qui di

omissis

In base al livello di gravità dell'accadimento anomalo, può essere costit
Management della Capogruppo, eventualmente informato dall'Uffici IT R
Response Team per fornire una rapida, efficace e ordinata **risposta all' i**
essere avviate le procedure per le segnalazioni degli eventi alle autorità
Le finalità del Team sono:

- Determinare le cause di incidente e le modalità con cui questo si è ve
  necessarie ed evitare che si ripeta.
- Definire eventuali contromisure necessarie nell'immediato.
- Raccogliere, se necessario, le eventuali evidenze.
- Favorire il contatto con altre aree/siti che possono essere coinvolti.

Favorire il contatto tra la Direzione e le **Autorità competenti in ambito d**



BANCA SELLA HOLDING

Banca Sella Holding S.p.A. Controllo del Valore - *IT Risk*	Politiche di Sicurezza Informatica	Rev. 0.8

Politiche di Sicurezza Informatica

Versione 0.8

Cronologia delle Revisioni/Aggiornamenti:

Versione	Data	Autore	Note
0.1	28/09/2000	[redacted]	Indice del Documento
0.2	28/10/2002	[redacted]	Prima Revisione
0.3	04/11/2002	[redacted]	Seconda Revisione
0.4	25/02/2003	[redacted]	Terza Revisione
0.5	26/03/2003	[redacted]	Quarta Revisione
0.6	08/05/2003	[redacted]	Quinta Revisione
0.7	18/12/2009	[redacted]	Revisione Completa Politica
		[redacted]	Revisione Completa Politica
		[redacted]	Approvazione Finale
		[redacted]	Recepimento osservazioni da "Consultazione Preliminare"
0.8		[redacted]	Recepimento osservazioni Area IT

Pagina 1 di 31

Banca Sella Holding S.p.A. - Sede: Via Italia, 2 - 13900 BIELLA (BI) - Tel. 015.35011 - Telefax 015.351767 - Capitale Sociale e Riserve Euro 447.753.864 - Codice ABI 3311 - Iscritta alla C.C.I.A.A. di Biella - Cod. FISC. e P. IVA 01709430027 - SWIFT: SELB IT 22 - Aderente al Fondo Interbancario di Tutela dei Depositi - Iscritta all'Albo delle Banche e dei Gruppi Bancari - Capogruppo del Gruppo Banca Sella - Sito Internet http://www.gruppobancasella.it - E-mail: info@gruppobancasella.it

COORDINAMENTO FUNZIONI AZIENDALI DI CONTROLLO E FLUSSI INFORMATIVI

CONSIGLIO DI AMMINISTRAZIONE

MECCANISMI E FUNZIONI AZIENDALI DI CONTROLLO

Presidio continuo delle attività fino alla rimozione definitiva delle cause

Rimozione immediata

Rimozione definitiva

Evento rischioso

Livelli di Rischio	
	Minimo
	Significativo
	nte
R4	
R5	Mo
N.R.	Non Rileva o

Flussi informativi

Il rischio informatico, una nuova frontiera per il Risk Management

Roberto Pozzuolo
Responsabile Sicurezza, Controlli e Gestione del Rischio Operativo
Banca Sella Holding

Roma, 17 Giugno 2014