ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

sogei

Information Risk Management in sistemi complessi

Sistema di Gestione della Sicurezza in SOGEI

Applicazione di analisi del rischio - IBEA

(a cura dell'Ing. **Fabio Lazzini – SOGEI SpA**)

INDICE DELLA PRESENTAZIONE :

1. Premessa
2. Principi generali
3. Organizzazione della sicurezza
4. Metodologia di assessment e trattamento del rischio
5. Analisi del rischio di perimetro
6. Gestione di un bene infrastrutturale: modalità operative
7. Applicazione IBEA
8. Conclusioni

Parte 1 – Premessa

- Sogei, nell'ambito dell'impegno a migliorare la qualità dei servizi offerti ai propri clienti, ha stabilito di definire e attuare un **Sistema di Gestione per la Sicurezza delle Informazioni** (SGSI), strutturato in linea con le migliori pratiche ed in particolare con lo standard ISO/IEC 27001:2005.

- Secondo tale standard è stato definito ed è in corso di attuazione un piano di certificazione per i servizi più critici erogati da Sogei.

- In Sogei sono stati definiti 67 servizi (perimetri) e 225 beni infrastrutturali a supporto dei diversi servizi erogati.

- Nell'ambito di tale piano:
  - sono stati certificati nel periodo 2006-2007 il servizio doganale "SAISA"(Servizio Autonomo Interventi Settore Agricolo) ed il servizio "Telematico Entrate" per la presentazione delle dichiarazioni dei redditi.
  - è stato certificato nel 2008 il sevizio dell'Agenzia dell'Entrate "Anagrafe dei rapporti"
  - è in corso di certificazione il servizio "Totalizzatore Concorsi pronostici sportivi"

- Le certificazioni sono state rilasciate dalla società DNV.

Parte 2 – Principi generali

Sistema di Gestione per la Sicurezza delle Informazioni …

Il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) basato sull'analisi e il trattamento dei rischi, stabilisce, realizza, attua, controlla, rivede, riadatta e migliora la sicurezza delle informazioni gestite da Sogei.

Per fare ciò, il SGSI prevede principalmente:

- una specifica organizzazione, con attribuzione chiara di ruoli, responsabilità e regole;
- metodologie, procedure, linee guida, processi e risorse in linea con quanto previsto dagli standard di riferimento;
- obiettivi di sicurezza da perseguire;
- un'attività di monitoraggio e pianificazione degli interventi per la riduzione dei rischi.

È necessario il coinvolgimento di tutti i dipendenti che rivestono il ruolo di attore protagonista in maniera tale che la sicurezza diventi parte **integrante dei processi aziendali**

Sicurezza percepita come centro di *Profitto* e non di *Costo*

Obiettivi perseguiti con il SGSI

Garantire la gestione della sicurezza, in linea con le aspettative delle parti interessate, con gli obiettivi aziendali e con gli standard internazionali.

Normalizzare per tutta l'azienda l'approccio alla gestione della sicurezza, ottimizzando e coordinando le risorse disponibili

Creare un'organizzazione della sicurezza condivisa, documentata, organica, efficiente e capillare

Consentire un miglioramento continuo del sistema della sicurezza

Creare una consapevolezza di tutto il personale sulle problematiche di sicurezza

Ambito del SGSI

Garantire la sicurezza di tutte le informazioni strutturate residenti in banche dati informatiche.

Normare il processo di distribuzione e classificazioni dei documenti contenenti informazioni riservate, confidenziali, uso interno e pubbliche.

Il SGSI è un processo di business aziendale che basandosi sull'approccio di gestione del rischio si propone di:

> Organizzare, governare, implementare, perseguire operativamente, controllare, rivedere, mantenere e migliorare la **sicurezza delle informazioni**, garantendo nel tempo il soddisfacimento della politica di sicurezza.

In questo contesto l'analisi del rischio rappresenta il **punto di partenza** per procedere all'implementazione del SGSI

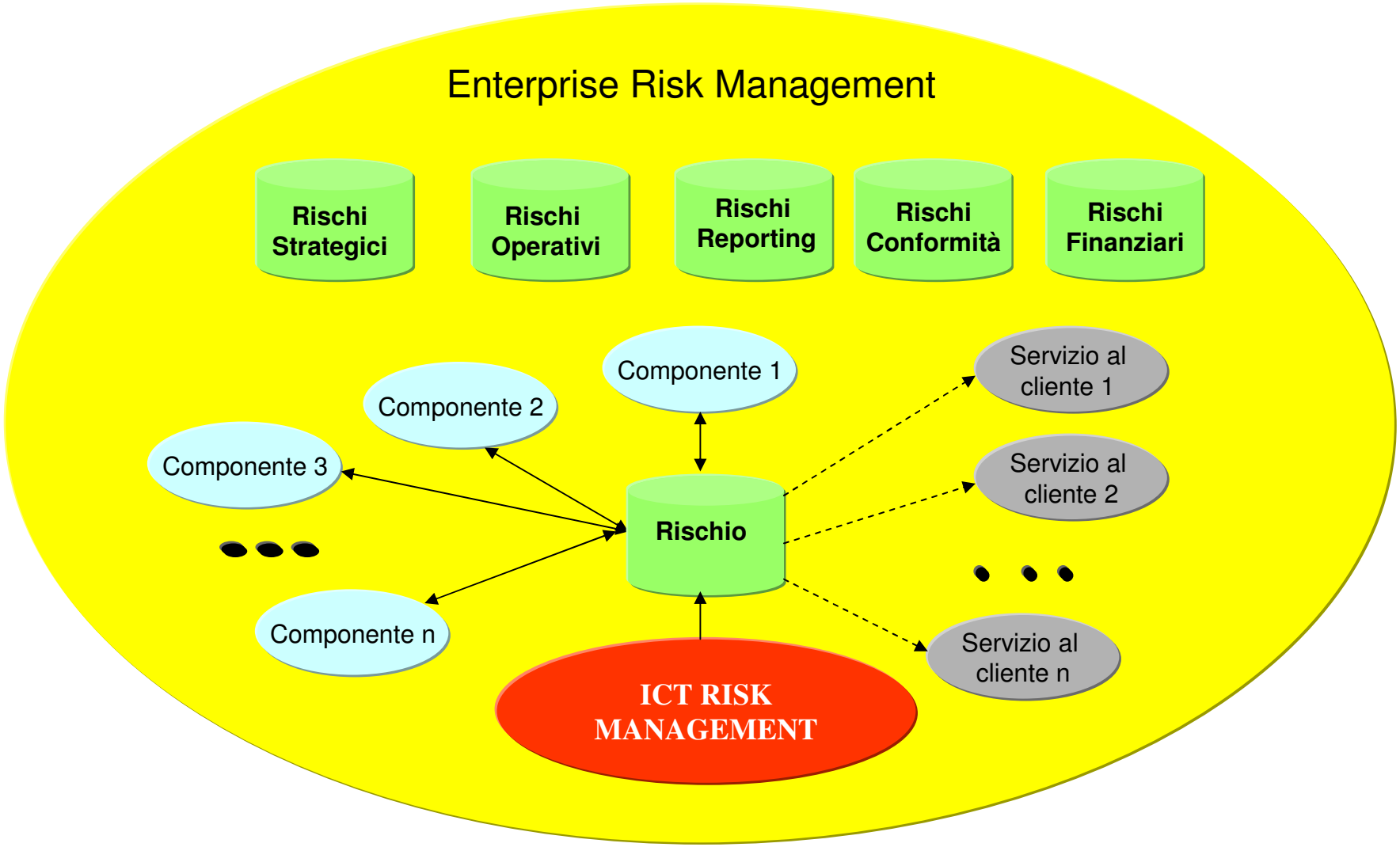
Sistema di Gestione per la Sicurezza delle Informazioni (SGSI)

- Il modello SGSI prevede più livelli di analisi (beni infrastrutturali, perimetri/servizi, minacce) e **produce diversi indicatori di rischio**: per istanza di controllo (base), per bene infrastrutturale (derivato), per controllo (derivato), per obiettivo di controllo (aggregato), per categorie, per componente, per perimetro, per minaccia, ecc.).

- Partendo da questi indicatori si può **evidenziare come si correlano i componenti ed i servizi oggetto della governance, in funzione dei profili di rischio che la governance stessa definirà.**

- Pertanto partendo dal Sistema di Gestione per la Sicurezza delle Informazioni(SGSI) è possibile determinare:
  - un **rischio che l'ICT trasmette alle singole componenti** in base ai sistemi informatici che supportano tali componenti (Rischio Residuo Percentuale (RRP) del perimetro Sistema Informativo Aziendale del SGSI),
  - un **rischio che l'ICT trasmette ai singoli servizi erogati al cliente** in base ai sistemi informatici che supportano tali servizi (Rischio Residuo Percentuale (RRP) del perimetro Presidio Mercati del SGSI),
  - il **contributo che le componenti offrono alla riduzione del rischio ICT** (Rischio Residuo Percentuale (RRP) dei beni infrastrutturali propri delle componenti).
- Il rischio per singola componente di governance è ottenuto attraverso la composizione secondo un criterio combinatorio dei rischi sopra definiti
- Una volta definite le strategie generali ed il livello di rischio ICT tollerabile per ciascuna componente, questa classificazione dei rischi in categorie distinte, ma connesse o sovrapponibili - relativamente ad esigenze diverse dell'azienda - consente di approfondire differenti aspetti della gestione del rischio.

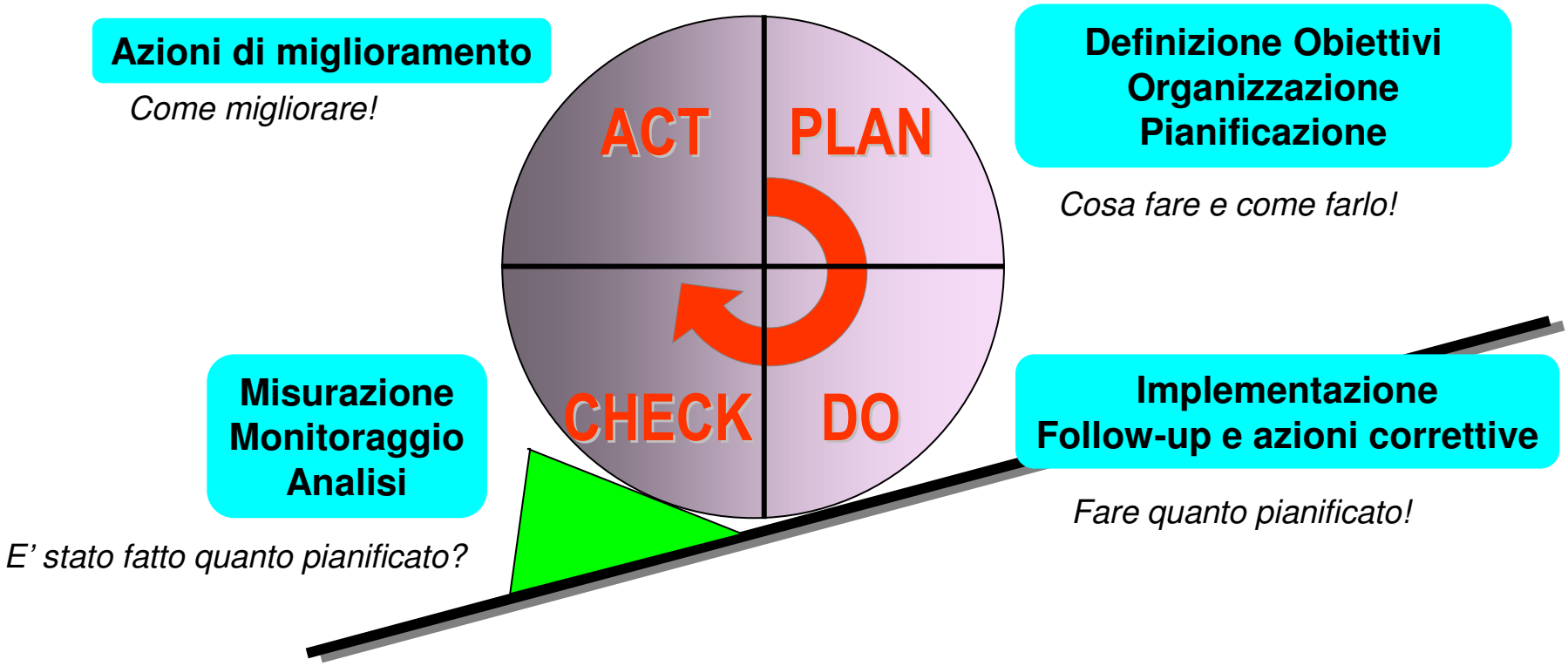
… Correlazione dei rischi ICT al business aziendale



Modello logico di riferimento: Ciclo di Deming (PDCA)

Il modello di riferimento è basato sul ciclo Pianificazione, Realizzazione, Verifica, Miglioramento.

Tale modello riprende concettualmente lo schema generale PDCA, proprio della norma ISO 27001, utilizzato nel SGSI.



Cos'è l'informazione per Sogei

- L'informazione è costituita dai dati e dal loro significato, cui Sogei attribuisce uno specifico valore ai fini del conseguimento della propria missione.

- L'informazione si presenta in diverse forme: può essere stampata o scritta su carta, memorizzata elettronicamente, trasmessa tramite posta o strumenti elettronici, mostrata in filmati, oppure espressa in conversazioni; qualunque sia la forma presa dall'informazione, o il mezzo utilizzato per condividerla o memorizzarla, essa deve essere sempre adeguatamente protetta.

- La politica per la sicurezza delle informazioni, perseguita dalla Sogei, è basata sui seguenti principi:

  - la sicurezza è una priorità aziendale sostenuta dalla Direzione aziendale;
  - la sicurezza impegna trasversalmente e complessivamente l'azienda. Tutto il personale Sogei è "attore protagonista" per gli aspetti specifici del proprio ruolo;
  - I principi generali di sicurezza devono essere messi in pratica, coerentemente con le proprie attività, da tutto il personale dipendente che opera presso le sedi aziendali.
  - ogni dipendente, gruppo o struttura aziendale deve ridurre i rischi e i possibili effetti negativi che possono derivare da eventi dannosi (incidenti, errori …);
  - il processo di sicurezza è in continua evoluzione perché sottoposto a un continuo miglioramento e adattamento alla luce di soluzioni tecnologiche innovative, di nuovi rischi ovvero in base ai risultati delle attività di verifica e di monitoraggio;
  - i sistemi informativi, i servizi e le applicazioni sviluppate e mantenute da Sogei devono tenere conto delle problematiche legate alla sicurezza sia nella fase di progettazione e realizzazione che in quella di esercizio.
  - I principi generali devono altresì essere recepiti nella stesura dei contratti di acquisizione di servizi quali esternalizzazioni, supporto e assistenza (manutenzione e installazione hardware e software, ecc.), servizi ausiliari (pulizie, ristorazione, vigilanza, trasporto di beni contenenti informazioni, ecc.), consulenza, prestazioni di lavoro interinale ovvero di servizi dati in outsourcing.

Framework documentale del SGSI

- La documentazione del SGSI è articolata nelle seguenti categorie:

1. **Politica per la sicurezza delle informazioni**
2. **Manuale della sicurezza**
3. **Procedure per la gestione della sicurezza**
   - Procedure per la gestione del rischio
   - Procedure per il controllo e miglioramento
   - Procedure per la gestione delle misure di sicurezza
   - Procedure per la gestione della documentazione
4. **Procedure operative di sicurezza**
5. **Fascicolo di perimetro**

L'intero sistema dei documenti del SGSI viene sottoposto a riesame periodico ed è prevista la revisione in caso di: rilevanti incidenti di Sicurezza, introduzione di nuove tecnologie e variazioni significative dell'organizzazione aziendale.

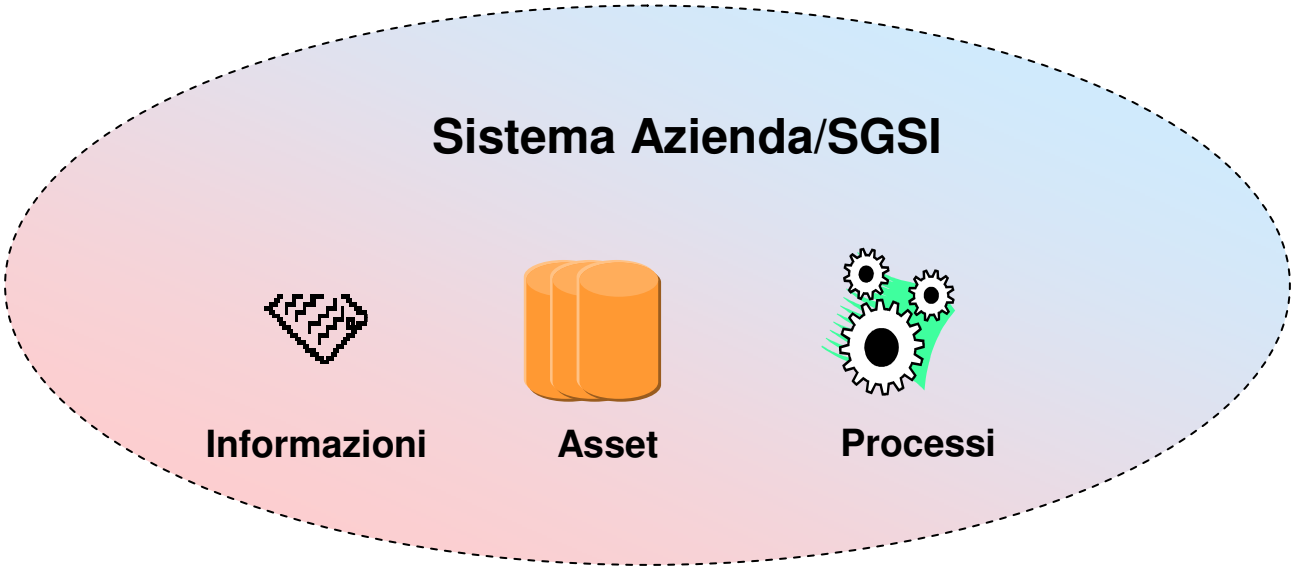
Parte 3 – Organizzazione della sicurezza

Rappresentazione dei beni …

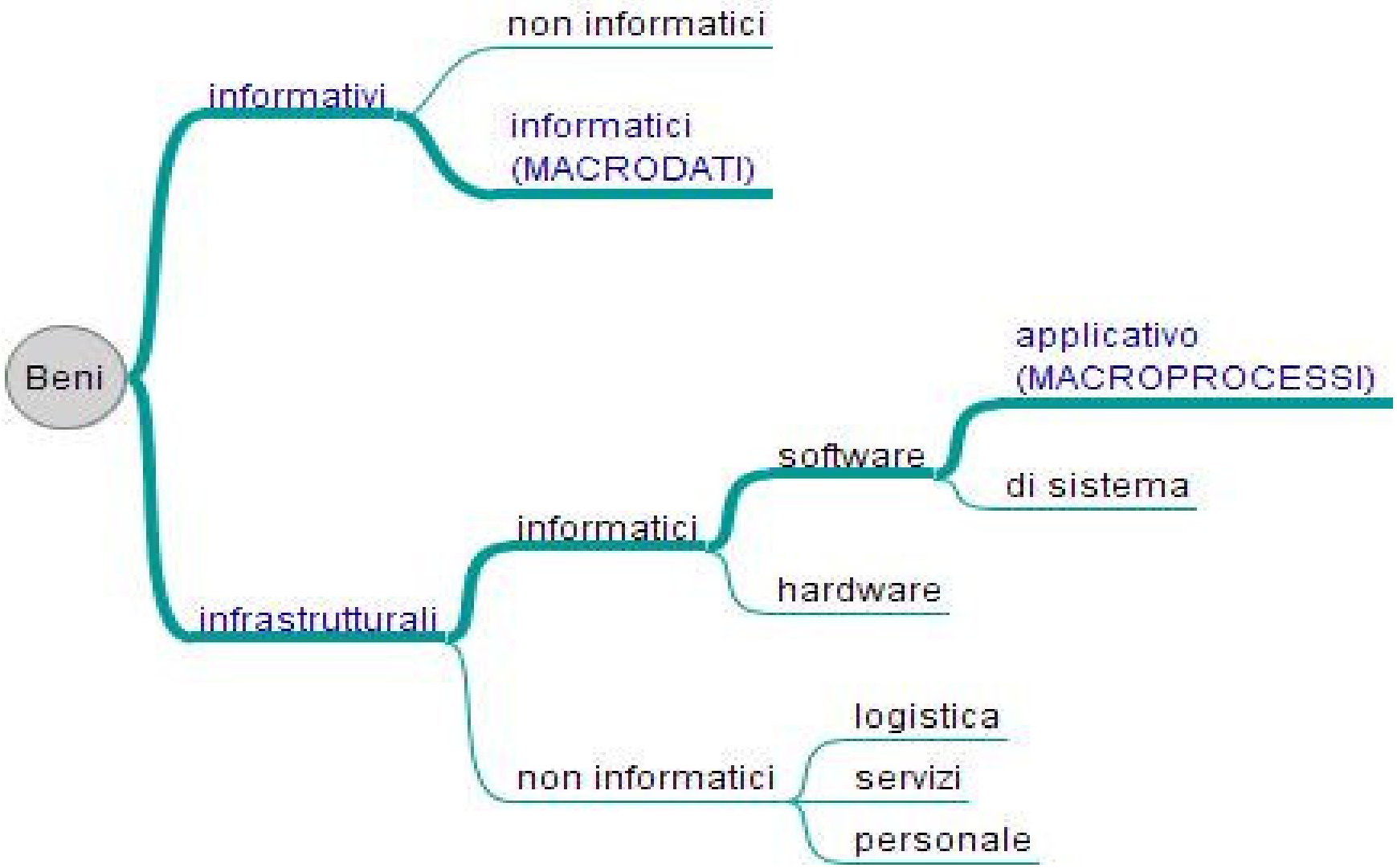
Un **bene informativo** è un insieme di informazioni alle quali viene associato un valore da parte di Sogei

Un **bene infrastrutturale** è una risorsa che concorre al trattamento delle informazioni e comunque ne influenza la sicurezza. In altre parole è la risorsa che protegge le informazioni contrastando le minacce cui è soggetta, attuando opportune contromisure.

Devono essere identificati tutti i beni che **hanno valore** nell'ambito del SGSI di perimetro



… Rappresentazione dei beni



- Per individuare i beni infrastrutturali si analizzano **i processi informatici** / **kit** di applicazione utilizzati nell'erogazione dei servizi del perimetro. Anche i processi informatici / Kit di applicazioni sono dei beni infrastrutturali (software); partendo da essi, si individuano gli altri componenti hardware, software, logistica, servizi e persone che li supportano e che quindi concorrono alla erogazione del servizio.
- Questa attività deve essere svolta dopo aver esaminato l'inventario dei beni definito a livello aziendale. In particolare:
  - se il bene infrastrutturale definito a livello aziendale attua per il perimetro le misure di sicurezza standard aziendali, non dovrà essere oggetto di ulteriore scomposizione (es. Sala CED, SGSI, Gestione Incidenti, Acquisti, Antivirus);
  - se il bene infrastrutturale definito a livello aziendale, attua delle specificità per il perimetro, dovrà essere oggetto di specifico approfondimento (es. Gestione elaborazioni, supporti sistemistici, gestione accessi, sicurezza perimetrale);
  - se il bene infrastrutturale è specifico del perimetro e non presente nell'inventario dei beni aziendale dovrà essere rilevato e censito (es. software applicativo, apparati, software di sistema).
  - ad ogni bene infrastrutturale individuato deve essere associato un unico Gestore.
  - una volta individuati, i beni infrastrutturali, devono essere inseriti nell'"applicazione di supporto al SGSI di perimetro" per procedere all'analisi del rischio.

Bene informativo

- Per individuare i beni informativi occorre:
  - partendo da ogni macroprocesso censito all'interno del perimetro, analizzare i kit di applicazione che lo compongono per individuare i data base utilizzati o, eventualmente, anche un loro sottoinsieme (vista, singola tabella, ecc..);
  - non considerare le banche dati temporanee o quelle di servizio;
  - aggregare più data base o sottoinsieme in base alla omogeneità del significato delle informazioni trattate ed alla relativa criticità;
  - utilizzare il bene informativo già definito a livello aziendale nel caso in cui l'aggregazione porti ad un risultato con esso coincidente;
  - assegnare, negli altri casi, un nome alle diverse aggregazioni ottenendo, di conseguenza, i beni informativi che dovrebbero, in linea generale, essere figli del bene informativo padre definito nell'inventario generale;
  - individuare il proprietario;
  - inserire i beni informativi nell'"applicazione di supporto al SGSI di perimetro IBEA";
  - correlare, nell'"applicazione di supporto al SGSI di perimetro IBEA", i beni informativi con il bene informativo padre presente nell'inventario dei beni a livello aziendale.

Bene informativo di Perimetro

- Per individuare i beni informativi del perimetro occorre:
  - partendo da ogni macroprocesso censito all'interno del perimetro, analizzare i kit di applicazione che lo compongono per individuare i data base utilizzati o, eventualmente, anche un loro sottoinsieme (vista, singola tabella, ecc..);
  - non considerare le banche dati temporanee o quelle di servizio;
  - aggregare più data base o sottoinsieme in base alla omogeneità del significato delle informazioni trattate ed alla relativa criticità;
  - utilizzare il bene informativo già definito a livello aziendale nel caso in cui l'aggregazione porti ad un risultato con esso coincidente;
  - assegnare, negli altri casi, un nome alle diverse aggregazioni ottenendo, di conseguenza, i beni informativi che dovrebbero, in linea generale, essere figli di un bene informativo padre definito nell'inventario generale;
  - individuare il proprietario;
  - inserire i beni informativi nell'"applicazione di supporto al SGSI di perimetro IBEA";
  - correlare, nell'"applicazione di supporto al SGSI di perimetro IBEA", i beni informativi con il bene informativo padre presente nell'inventario dei beni a livello aziendale.

Perimetro …

- Il concetto di **Perimetro** è stato introdotto, ai fini della gestione della sicurezza delle informazioni, per avere ambiti di gestione più circoscritti e mirati rispetto all'intera azienda. L'elemento preso come riferimento nella definizione dei perimetri, e che conferisce una valenza di business all'ambito considerato, è il servizio erogato, esternamente o internamente a Sogei.

  Nel dettaglio:

  – Il perimetro può essere anche l'intera azienda.

  – Il Perimetro raggruppa i Beni informativi trattati per erogare il servizio e i Beni infrastrutturali che partecipano all'erogazione del servizio.

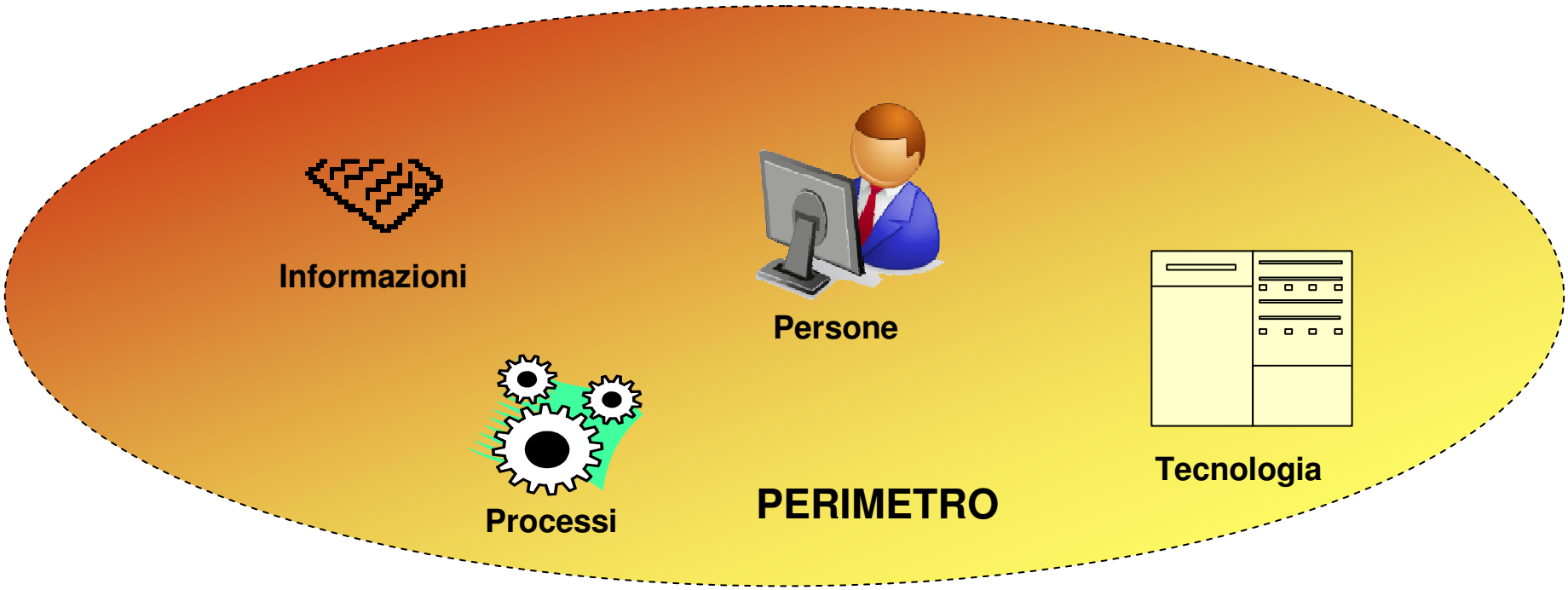
  – Nell'ambito di un Perimetro i Beni infrastrutturali ereditano la criticità RID dai Beni informativi che trattano.

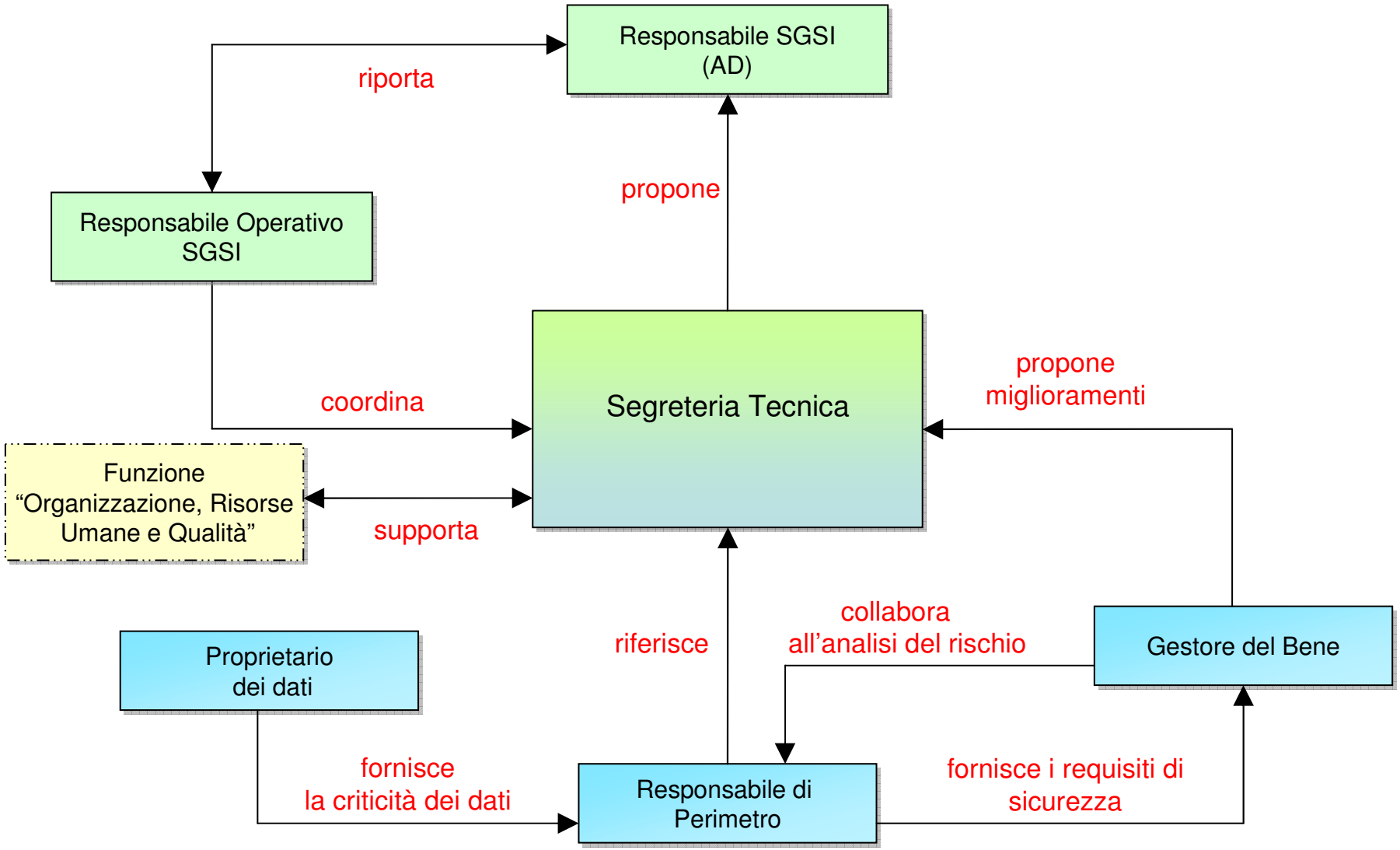
  – Nell'ambito del perimetro valgono tutte le regole di sicurezza definite a livello di SGSI, ma devono essere dettagliati i controlli specifici del servizio erogato.

  – Per ogni Perimetro viene definito il rispettivo Responsabile.

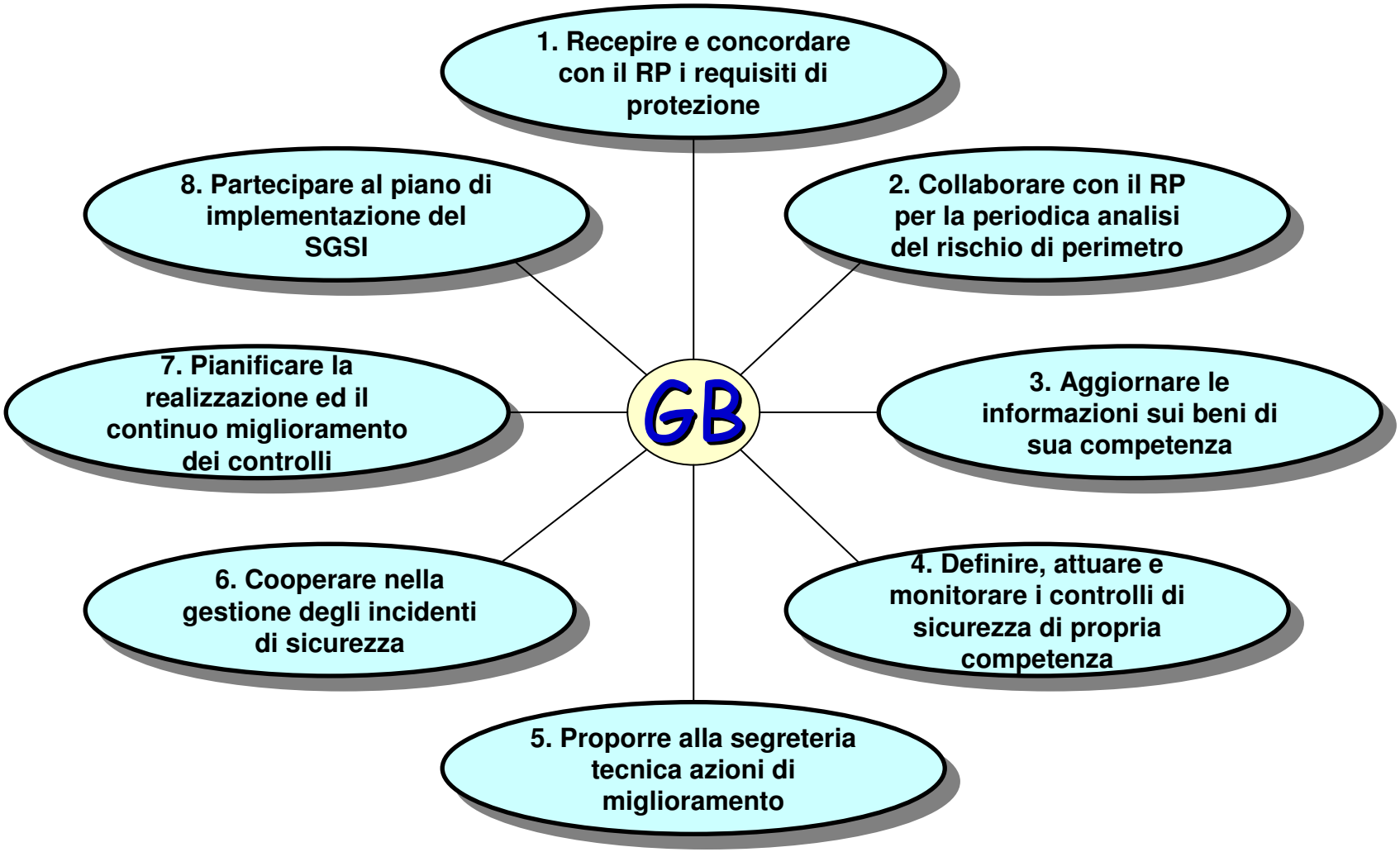
… Perimetro

- Il perimetro è l'insieme dei processi informativi e delle relative risorse finalizzate all'erogazione di uno specifico servizio:

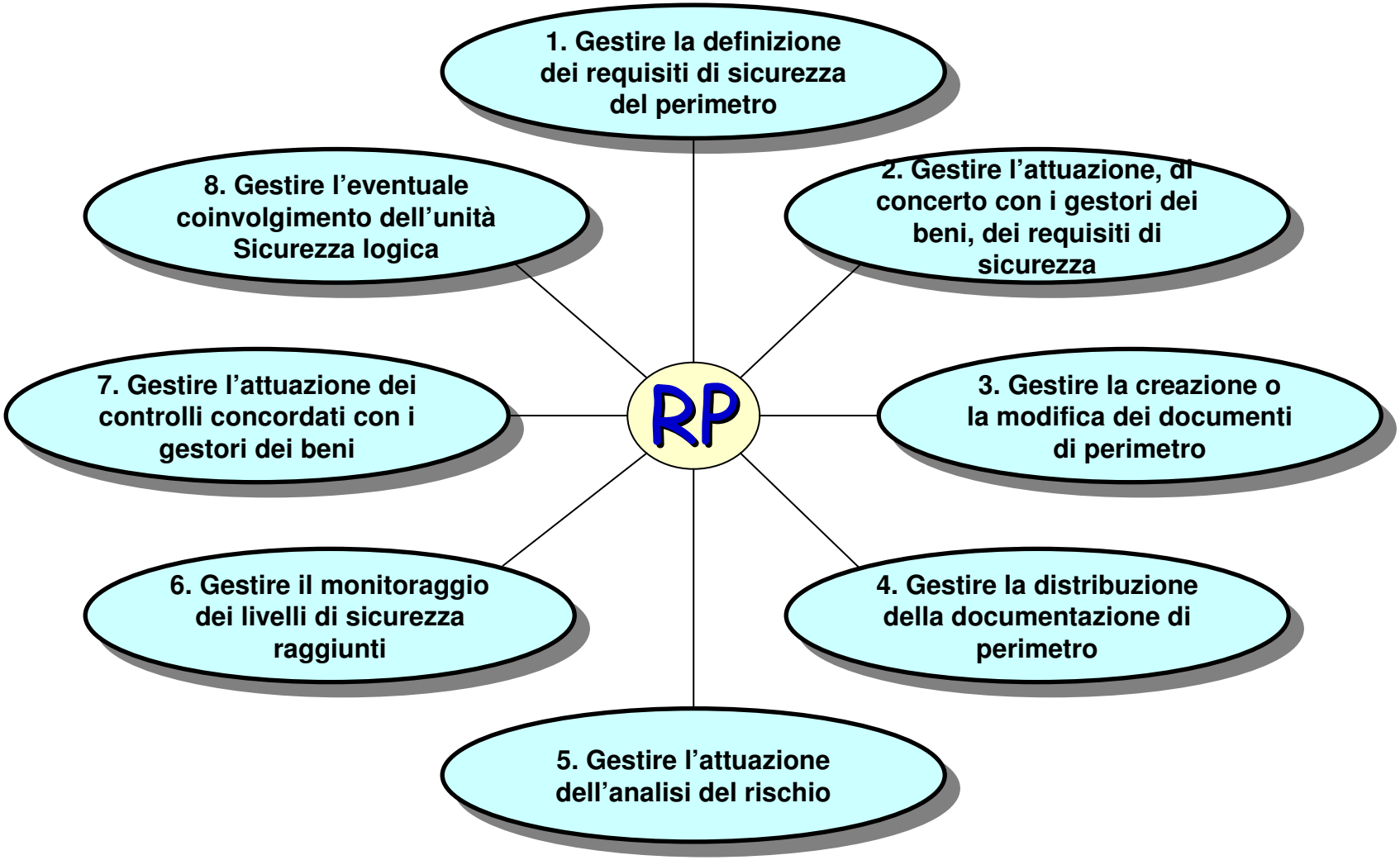



Responsabile SGSI (AD)
riporta
Responsabile Operativo SGSI
propone
coordina
Segreteria Tecnica
propone miglioramenti
Funzione "Organizzazione, Risorse Umane e Qualità"
supporta
Proprietario dei dati
riferisce
collabora all'analisi del rischio
Gestore del Bene
fornisce la criticità dei dati
Responsabile di Perimetro
fornisce i requisiti di sicurezza

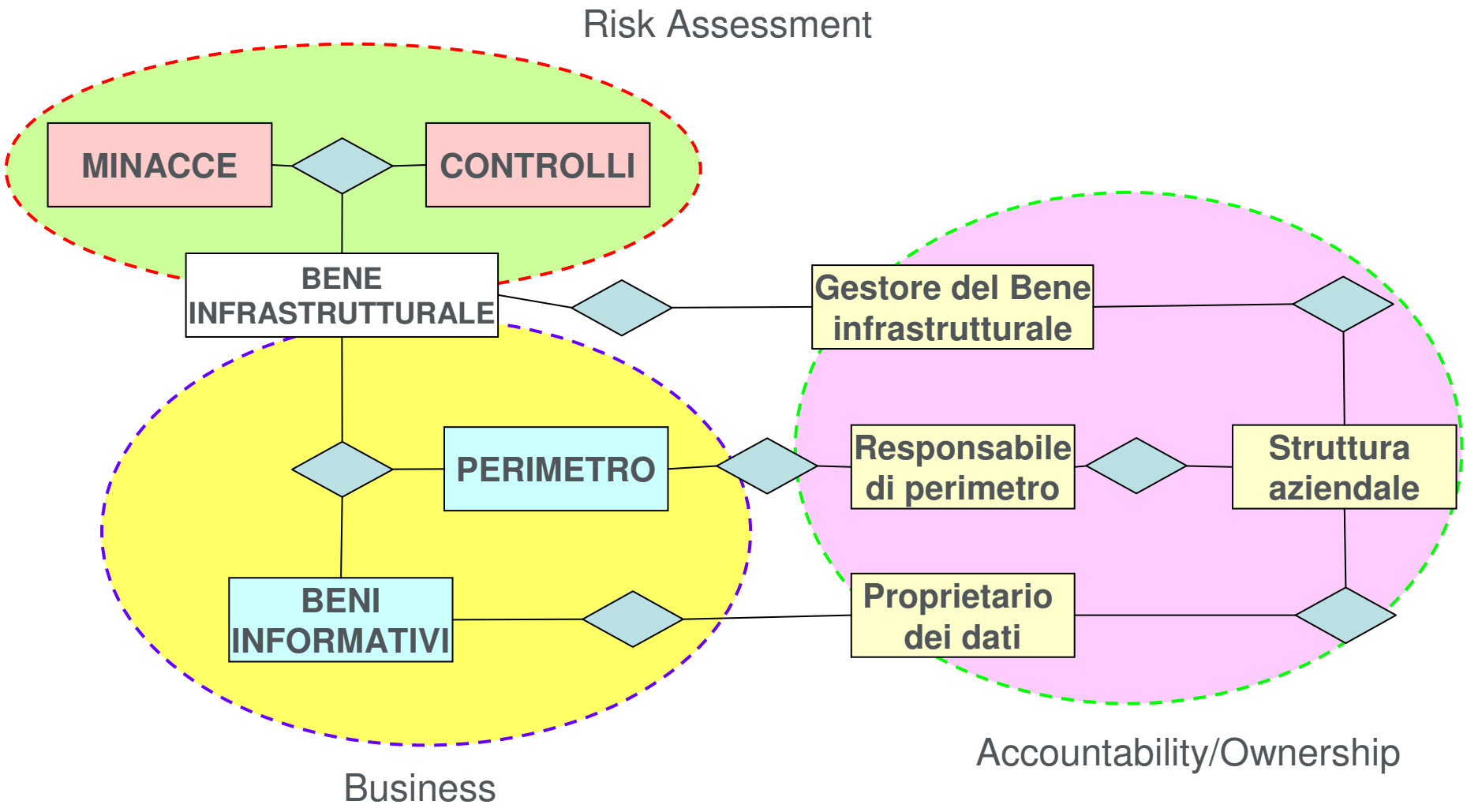
Responsabilità del Gestore del bene



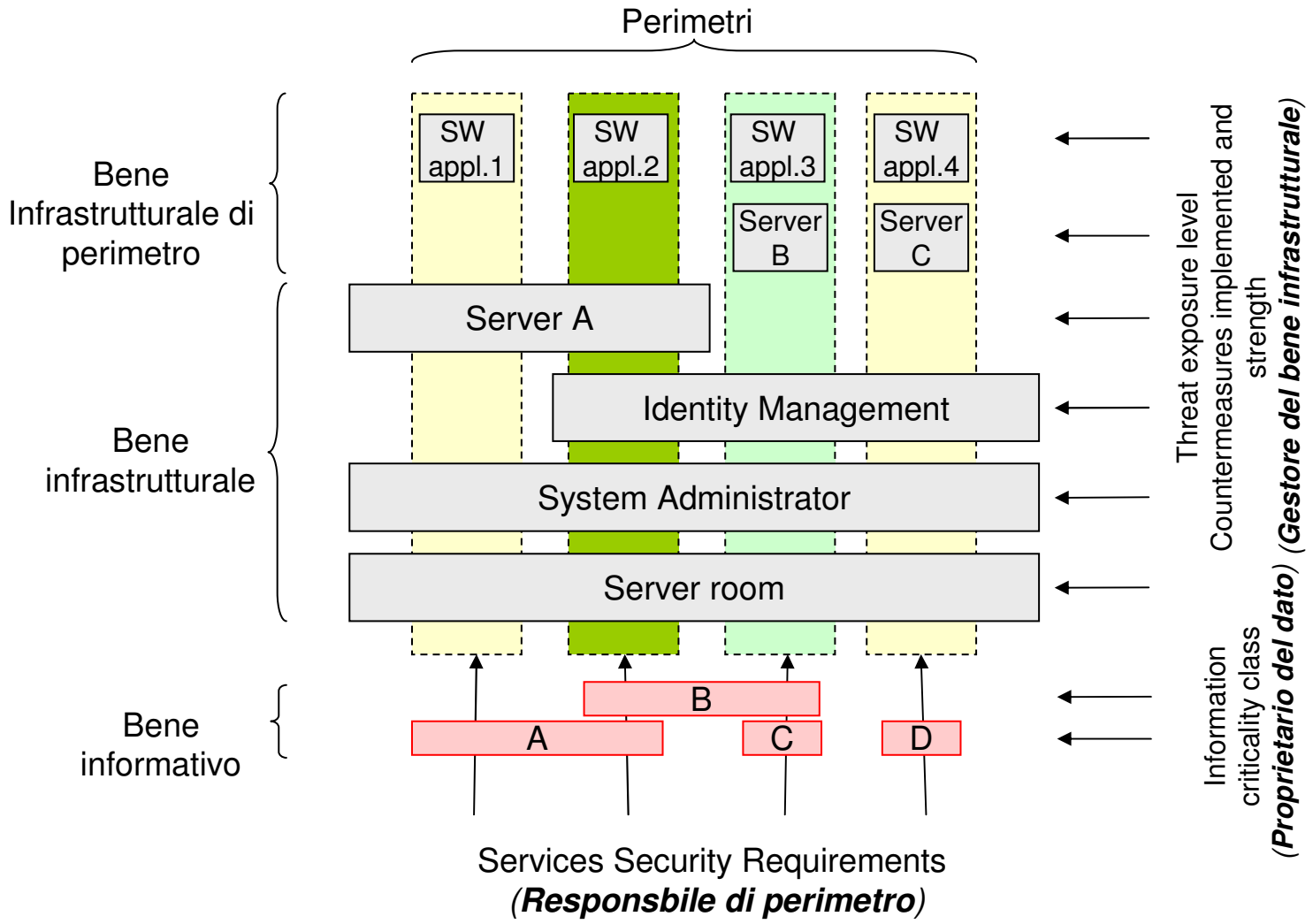
Responsabilità del Responsabile di Perimetro



Parte 4 – Metodologia di assessment e trattamento del rischio


Risk Assessment
MINACCE
CONTROLLI
BENE INFRASTRUTTURALE
Gestore del Bene infrastrutturale
PERIMETRO
Responsabile di perimetro
Struttura aziendale
BENI INFORMATIVI
Proprietario dei dati
Business
Accountability/Ownership

… Modello di Riferimento della Sicurezza

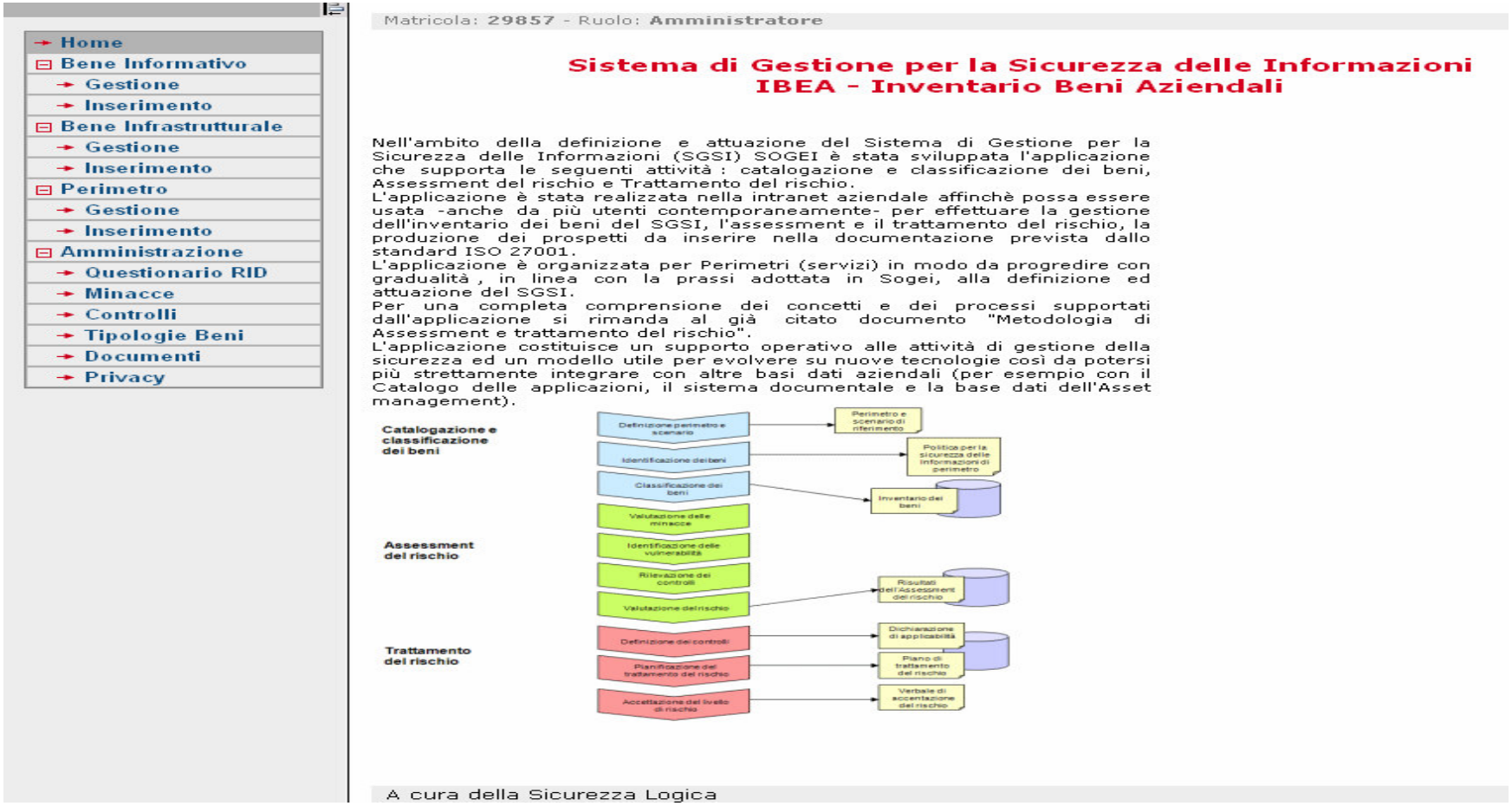


- Nell'ambito della definizione e attuazione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) SOGEI è stata sviluppata l'applicazione "**IBEA**" che supporta le attività di: *Catalogazione e Classificazione dei beni*, *Assessment del rischio* e *Trattamento del rischio*.

- L'applicazione **IBEA**:
  - è disponibile nella intranet aziendale per effettuare la gestione dell'inventario dei beni, l'assessment e il trattamento del rischio, la produzione dei report da inserire nella documentazione prevista dallo standard ISO 27001.
  - è organizzata per Perimetri (servizi) in modo da progredire con gradualità, in linea con la prassi adottata in Sogei.
  - costituisce un supporto operativo alle attività di gestione della sicurezza ed un modello utile per evolvere su nuove tecnologie così da potersi integrare con altre basi dati aziendali (per esempio con il Catalogo delle applicazioni, il sistema documentale e la base dati dell'Asset management).

… Strumento a supporto dell'analisi del rischio

- Obiettivo primario degli attori coinvolti nell'attuazione del SGSI è mantenere costantemente aggiornata la basi dati di IBEA ed allineata con il Catalogo delle applicazioni, secondo la propria profilatura di accesso.



Principi generali della metodologia di anali del rischio …

La letteratura più autorevole sulla analisi del rischio dell'informazioni quale:

- BS 7799 (DISC PD 3002 Guide to Risk Assessment and Risk Management)
- ISO (ISO/IEC TR 13335-3 "Information technology – Guidelines for the management of IT Security – Techniques for the management of IT Security")
- NIST(NIST Special 800-30 "Risk Management Guide for Information Technology Systems - Recommendations of the National Institute of Standards and Technology")

individua le seguenti tipologie di approccio all'assessment del rischio:

- **Qualitativo**
- Quantitativo

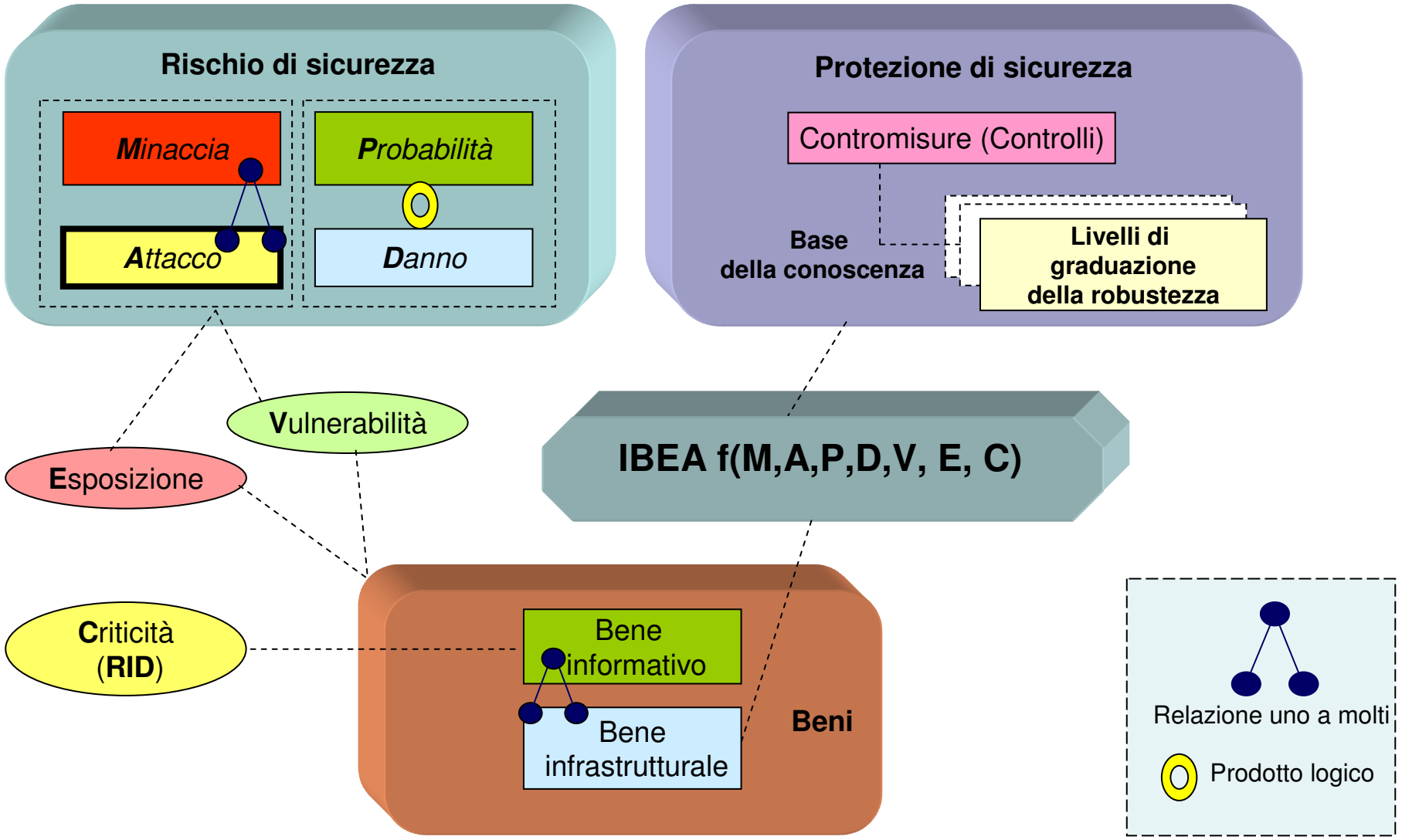
Nell'ambito dell'approccio qualitativo, in particolare, si individua:

- Basic Risk Assessment
- **Detailed Risk Assessment**
- Combined Approach

… Principi generali della metodologia di anali del rischio

- Valutando i vantaggi e gli svantaggi dell'approccio quantitativo rispetto al qualitativo si è deciso di utilizzare il qualitativo e, in tale ambito l'"*Assessment del rischio dettagliato*" (DISC PD 3002).
- Valutazione del rischio di tre fattori:
  - l'**entità del danno** che l'organizzazione riceve se una informazione perde la sua riservatezza, integrità e disponibilità
  - l'**esposizione alle minacce** dell'informazione nell'ambito di un bene infrastrutturale
  - le **misure di protezione** in essere nell'ambito di un bene infrastrutturale
- Le tassonomie utilizzate sono:
  - per le misure di protezione i controlli indicati nello standard ISO 27001
  - per le minacce si sono definite per semplicità 15 minacce che rappresentano tutti gli attacchi alle informazioni. Le minacce sono state definite partendo dalle seguenti riferimenti:
    - BS 7799 DISC PD 3200 Guide to BS 7799 - Risk Assessment and Risk Management (Annex A)
    - NIST SP 800-30
    - SANS The Twenty Most Critical Internet Security Vulnerabilities
    - ISO 13335-3 Annex C
    - ISO/IEC 18028 information Technology – Security Techniques –IT network security
    - IT-Grundschutz Threats Catalogue

Schema generale del modello di analisi e gestione del rischio …



… Schema generale del modello di analisi e gestione del rischio

- Sinteticamente:
  - Individuazione del perimetro in esame
  - Individuazione, nell'ambito dello specifico perimetro, dei diversi beni (informativi ed infrastrutturali) in gioco
  - Classificazione di ciascun bene, mediante i questionari presenti nell'applicazione IBEA
  - Valutazione del livello di esposizione di ciascun bene del perimetro in esame a tutte le possibili minacce pertinenti (la pertinenza è indicata nella base della conoscenza)
  - Selezione delle contromisure pertinenti (specifiche attuative) a ciascun bene/minaccia, al livello di robustezza individuato dal prodotto logico tra Criticità e Livello di Esposizione

Processo di valutazione del rischio

Il processo di valutazione del rischio ha l'obiettivo di permettere al Responsabile di perimetro, Proprietario del dato e Gestore del bene infrastrutturale la definizione di un insieme di misure di protezione, commisurate alle reali necessità di sicurezza, da adottare nell'ambito del perimetro in esame. Il processo si compone di due fasi:

- Calcolo del ***livello di rischio intrinseco*** di ogni bene infrastrutturale rispetto alle varie minacce a cui è esposto, si conclude con la definizione di un ***profilo di protezione ottimale*** per ciascuno dei beni infrastrutturali del perimetro in esame.

- Gestione del rischio durante la quale, attraverso il confronto tra il profilo di protezione ottimale suggerito da IBEA e le misure di protezione effettivamente realizzate o pianificate descritte dall'utente, viene calcolato ***il livello di rischio residuo*** al quale il perimetro in esame ed i relativi beni infrastrutturali sono esposti. Qualora si decida di realizzare puntualmente il profilo di protezione ottimale suggerito, il rischio residuo viene posto convenzionalmente a zero.

- Ciascun bene infrastrutturale di un perimetro è esposto ad una o più minacce. Il ***Livello di Esposizione (LE) del bene rispetto alla minaccia*** consente di valutare quanto il bene può essere danneggiato dalla minaccia e viene espresso qualitativamente tramite una scala di quattro valori (0, 1, 2, 3).

- L'utente di IBEA deve indicare, per ogni bene infrastrutturale nel perimetro in esame, una stima del livello di esposizione alle diverse minacce.

- Per stimare correttamente il livello di esposizione alle varie minacce è opportuno tenere presente che nel modello di analisi del rischio adottato in IBEA, si assume che la ***frequenza di potenziale accadimento della minaccia*** sia indipendente dai controlli e cioè dalle misure di protezione attuate.

- Si definisce *Livello di rischio intrinseco* di un bene infrastrutturale rispetto ad una minaccia, una terna di valori calcolati in funzione di:
  - livello di esposizione del bene infrastrutturale alla minaccia
  - classe di criticità del bene infrastrutturale
  - pertinenza RID della minaccia

- Gli elementi della terna vengono calcolati in modo che costituiscano un indice di quanto è opportuno proteggere, nei confronti della minaccia in esame, la riservatezza, l'integrità e la disponibilità dell'informazione associata al bene infrastrutturale.

GESTIONE DEL RISCHIO E LIVELLO DI RISCHIO RESIDUO

- Nella processo di gestione del rischio, il Gestore del bene infrastrutturale descrive le misure di protezione in atto (o pianificate) in modo che l'applicativo possa confrontarle con quelle suggerite nel profilo di protezione ottimale relativo ai diversi beni infrastrutturali.

- IBEA utilizza due parametri per indicare il risultato di questo confronto:
  - lo scostamento dalla graduazione ottimale associato alle varie istanze di controllo
  - il livello di rischio residuo (assoluto e percentuale) associato ad un bene infrastrutturale o ad un perimetro.

CALCOLO DELLO SCOSTAMENTO DALLA GRADUAZIONE OTTIMALE

- A livello delle singole istanze di controllo, IBEA utilizza il parametro SGR (Scostamento dalla Graduazione Richiesta) come misura di quanto le istanze di controllo utilizzate per contrastare un determinata minaccia si discostano da quelle ottimali.

Calcolo del livello di rischio residuo

- A livello di bene infrastrutturale o di intero perimetro, IBEA stima, invece un ***livello di rischio residuo*** ovvero un livello di rischio calcolato tenendo conto delle misure di protezione in atto. Sulla base del livello di rischio residuo, il Gestore del bene infrastrutturale o il Responsabile di perimetro decide se è necessario adottare ulteriori protezioni o se quelle già in atto sono sufficienti.

- Il procedimento di valutazione del livello di rischio residuo si basa sull'assunzione che un livello di rischio residuo non nullo sia dovuto alla non attuazione, o all'attuazione con graduazione inferiore a quella suggerita, delle misure di protezione incluse nel profilo di protezione ottimale (insieme delle misure di protezione ottimali suggerite dall'applicativo per il bene infrastrutturale o per il perimetro).
- In particolare, per ogni istanza di controllo, possono presentarsi i seguenti casi:
  - la misura di protezione è stata attuata con una graduazione pari o superiore a quella suggerita;
  - la misura di protezione è stata attuata con una graduazione inferiore a quella suggerita;
  - la misura di protezione non è stata attuata.

- Inoltre, la pertinenza RID dell'istanza di controllo partecipa all'analisi del rischio congiuntamente alla pertinenza RID della minaccia.

- La valutazione del rischio e della conformità privacy è suddivisa in quattro passi:
  - il primo per determinare i Livelli di Rischio Intrinseco (LRI),
  - il secondo per calcolare lo scostamento dei controlli realizzati rispetto al Livello di Rischio Intrinseco,
  - il terzo per valutare il Livello di Rischio Residuo (LRR), ed
  - il quarto per valutare il grado di Non Conformità Privacy (NCP).

	Criticità		
Bene Inform.	**R**	**I**	**D**
INF01	M	M	B
INF02	A	M	T

Campi da inserire

	Criticità		
Bene Infrast.	**R**	**I**	**D**
B01	A	M	B

Criticità	A	M	B	A	M	B	A	M	B	A	M	B
LE												
LRI												

Minacce														
Grado di robustezza effettivo del controllo														
Controllo di sicurezza	**R**	**I**	**D**	**R**	**I**	**D**	**R**	**I**	**D**	**R**	**I**	**D**		
LRR	Basso			Basso			Alto			Medio				
														RRP

Inserimento delle minacce e dei rispettivi LE …

Criticità	A	M	B	A	M	B	A	M	B	A	M	B
LE	Alto			Alto			Medio			Medio		
LRI												

		Minacce	M01			M06			M09			M15				
		Grado di robustezza effettivo del controllo	Abuso di privilegi			Errore umano			Guasti e malfunzionamenti			Carenze organizzative				
Controllo di sicurezza			R	I	D	R	I	D	R	I	D	R	I	D		
		LRR														
																RRP

- A seguito dell'attività di individuazione e valutazione sono state aggiunte nelle tabelle le seguenti informazioni:
  - il livello di esposizione "LE" per ogni minaccia, nella seconda riga della tabella in alto;
  - Codice e Nome delle Minacce cui è soggetto il bene, nelle 4 colonne della tabella in basso.

… Inserimento delle minacce e dei rispettivi LE

Criticità		A	M	B	A	M	B	A	M	B	A	M	B				
LE		Alto			Alto			Medio			Medio						
LRI																	
Minacce		M01			M06			M09			M15						
Grado di robustezza effettivo del controllo		Abuso di privilegi			Errore umano			Guasti e malfunzionamenti			Carenze organizzative						
Controllo di sicurezza		**R**	**I**	**D**	**R**	**I**	**D**	**R**	**I**	**D**	**R**	**I**	**D**				
10.01.01	Documentazione delle procedure operative	Basso															
10.01.02	Gestione del cambiamento	Alto															
10.10.04	Log delle attività dell'amminis./operatore	Medio															
10.10.05	Log dei malfunzionamenti	Tras.															
		LRR															RRP

- A seguito dell'attività di rilevazione e valutazione dei controlli sono state aggiunte nelle tabelle le seguenti informazioni:
  - codice e nome dei controlli in grado di contrastare le minacce precedentemente individuate;
  - il grado di robustezza con cui al momento sono realizzati i controlli.

Inserimento dei vari Livelli di Rischio Intrinseco

Criticità	A	M	B	A	M	B	A	M	B	A	M	B
LE	Alto			Alto			Medio			Medio		
LRI	A	A	M	A	A	M	A	M	B	A	M	B

Minacce		M01			M06			M09			M15				
Grado di robustezza effettivo del controllo		Abuso di privilegi			Errore umano			Guasti e malfunzionamenti			Carenze organizzative				
Controllo di sicurezza		R	I	D	R	I	D	R	I	D	R	I	D		
10.01.01	Documentazione delle procedure operative														
10.01.02	Gestione del cambiamento														
10.10.04	Log delle attività dell'amminis./operatore														
10.10.05	Log dei malfunzionamenti														
	LRR														RRP

- A seguito dell'attività di calcolo del rischio intrinseco sono state aggiunte, nella tabella in alto alla terza riga, il Livello di Rischio Intrinseco (LRI) di ogni minaccia per i tre requisiti RID.
- Il calcolo del LRI viene effettuato in base alla criticità RID del bene infrastrutturale e il livello di esposizione della minaccia.

Inserimento degli scostamenti delle graduazioni di robustezza

Criticità	A	M	B	A	M	B	A	M	B	A	M	B
LE	Alto			Alto			Medio			Medio		
LRI	A	A	M	A	A	M	A	M	B	A	M	B

		Minacce	M01			M06			M09			M15				
		Grado di robustezza effettivo del controllo	Abuso di privilegi			Errore umano			Guasti e malfunzionamenti			Carenze organizzative				
Controllo di sicurezza			R	I	D	R	I	D	R	I	D	R	I	D		
10.01.01	Documentazione delle procedure operative	Basso										2	1	0		
10.01.02	Gestione del cambiamento	Alto							0	0	0					
10.10.04	Log delle attività dell'amminis./operatore	Medio	1	1	0	1	1	0								
10.10.05	Log dei malfunzionamenti	Tras.							3	2	1					
		LRR														RRP

- A seguito dell'attività di determinazione dello scostamento sono state aggiunte nella tabella gli scostamenti delle graduazioni di robustezza dei controlli effettivi da quelli richiesti in base al LRI.
- Gli scostamenti sono indicati, in forma numerica, per ogni minaccia ed ogni requisito RID.
- Lo scostamento viene posto a zero (Nullo) nel caso in cui la graduazione effettiva sia uguale o superiore a quella richiesta.
- (Alto = 3, Medio = 2, Basso = 1, Nullo = 0)

Inserimento dei valori di LRR e RRP

Criticità	A	M	B	A	M	B	A	M	B	A	M	B
LE	Alto			Alto			Medio			Medio		
LRI	A	A	M	A	A	M	A	M	B	A	M	B

		Minacce	M01			M06			M09			M15				
		Grado di robustezza effettivo del controllo	Abuso di privilegi			Errore umano			Guasti e malfunzionamenti			Carenze organizzative				
Controllo di sicurezza			R	I	D	R	I	D	R	I	D	R	I	D		
10.01.01	Documentazione delle procedure operative	Basso										2	1	0	3	6
10.01.02	Gestione del cambiamento	Alto							0	0	0				0	6
10.10.04	Log delle attività dell'amminis./operatore	Medio	1	1	0	1	1	0							4	16
10.10.05	Log dei malfunzionamenti	Tras.							3	2	1				6	6
		LRR	Basso			Basso			Alto			Medio			13	34
															38 %	RRP

- A seguito dell'attività di calcolo del rischio residuo sono state aggiunte nell'ultima riga della tabella i Livelli di Rischio Residuo per ogni minaccia pari al massimo scostamento dei vari controlli che contrastano la minaccia.
- Sulla penultima colonna a destra sono stati sommati, per ogni controllo, gli scostamenti. Sull'ultima colonna a destra sono stati sommati i LRI in forma numerica. Ambedue le colonne riportano in basso il totale per tutti i controlli. Il rapporto fra questi due totali, moltiplicato per cento, fornisce il Rischio Residuo Percentuale (RRP)

- Il Responsabile del Perimetro, una volta individuati i beni infrastrutturali che partecipano alla erogazione dei servizi ed i relativi beni informativi trattati, attiva il processo, reso automatico dall'applicazione Intranet IBEA, di valutazione della conformità Privacy per il proprio Perimetro, producendo il report "Risultati dell'Assessment di Conformità Privacy" (RACP).

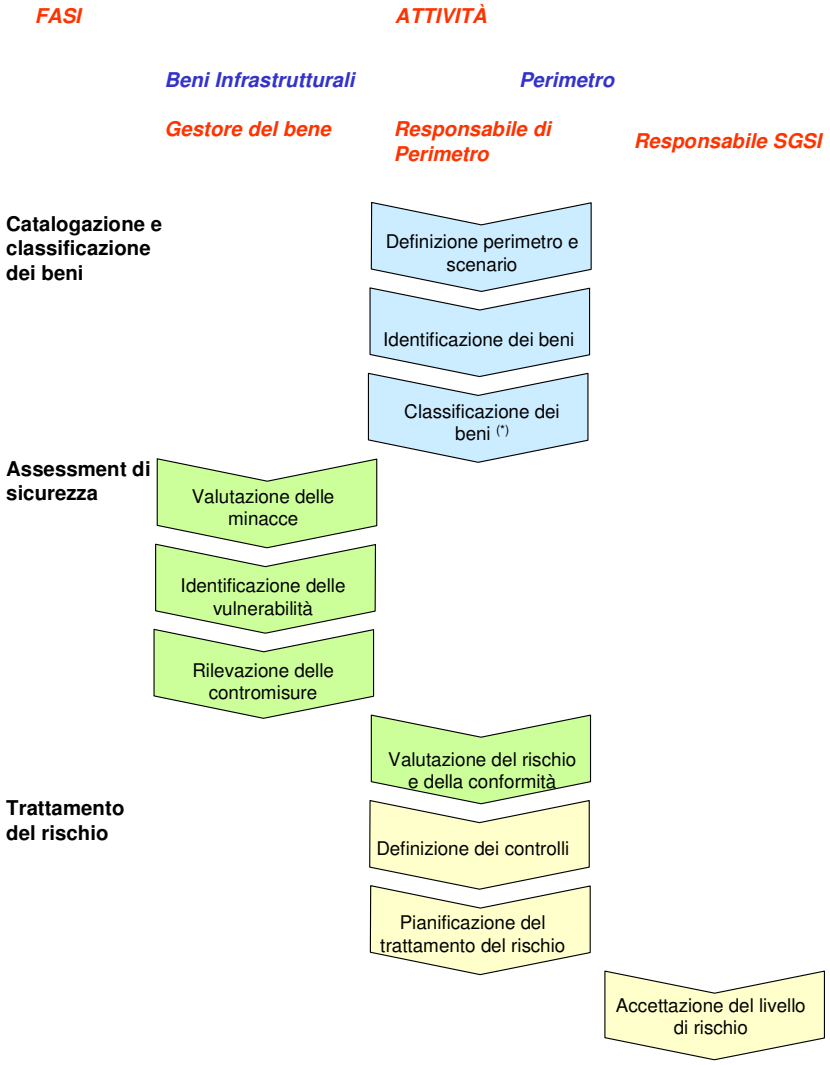
- Il risultato delle valutazione è la produzione di un indice di Non Conformità Privacy (NCP) a livello perimetro e di altrettanti indici NCP per ogni bene del perimetro a cui sono stati associati dei Requisiti Privacy da attuare.

- L'indicatore costituisce il risultato del processo di analisi di Conformità Privacy e rappresenta in percentuale il grado di non attuazione delle misure minime di sicurezza Privacy. Se l'indicatore ha il valore zero significa che il perimetro è perfettamente conforme alle suddette misure minime di sicurezza.

- Considerazioni:
  - Verificare se i Requisiti Privacy sono stati realizzati nei beni infrastrutturali del perimetro, tenendo conto della natura dei dati trattati.
  - Il Responsabile del Perimetro, qualora si evidenziassero delle non conformità (NCP di Perimetro non uguale allo 0%), deve porre in essere tutte le azioni necessarie per sanare la non conformità coordinandosi con i Gestori dei beni infrastrutturali interessati in quanto la conformità privacy, rispetto alle misure minime di sicurezza, è un obbligo di legge.
  - Una volta raggiunta la piena conformità Privacy, il Responsabile del Perimetro riproduce il report "Risultati dell'assessment di conformità Privacy" (RACP) in cui, per tutti i bene infrastrutturali risultano attuati i relativi Requisiti Privacy e redige il documento omonimo.
  - Il citato documento viene richiamato dal "Verbale di conformità Privacy del perimetro".

Parte 5 – Analisi del rischio di Perimetro

Attuazione del SGSI nei perimetri: ruoli



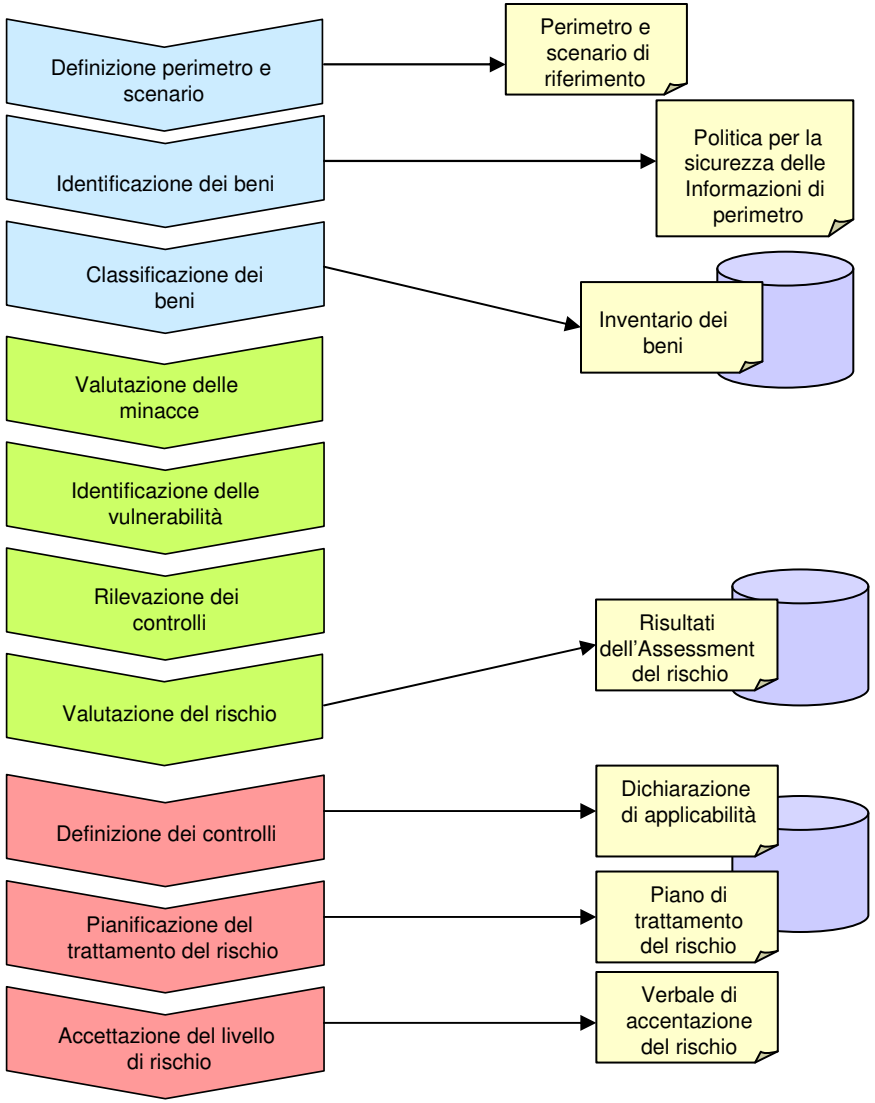
(*) Con il coinvolgimento dei Proprietari dei Dati

Attuazione del SGSI nei perimetri: output

Catalogazione e classificazione dei beni

Assessment del rischio

Trattamento del rischio



Definizione del perimetro e rilevazione dello scenario

Individuazione dei confini e delle interfacce del perimetro di riferimento, e descrizione dell'ambiente organizzativo e tecnologico

- Il documento "***Perimetro e Scenario di riferimento***" definisce l'ambito ed i confini del perimetro secondo le caratteristiche del business, aspetti organizzativi, logistici, di beni e tecnologie utilizzate, motivando eventuali esclusioni.

- Il documento "***Politica per la sicurezza delle informazioni***" definisce le regole di sicurezza del perimetro che soddisfano i requisiti di business e normativi, evidenziando le relazioni e le dipendenze con le Politiche di sicurezza generali definite da Sogei.

- L'**inventario dei beni** del perimetro è realizzato tramite una base dati contenente le informazioni sugli aspetti di sicurezza da utilizzare nell'assessment del rischio. Disponibile nell'applicativo IBEA.

- Il Responsabile di Perimetro conduce tutte le attività, consultando i Proprietari dei dati per la classificazione delle informazioni. I documenti prodotti devono essere approvati dal responsabile della struttura aziendale

Identificazione dei beni

Vengono identificati sia i beni informativi che quelli infrastrutturali del perimetro di riferimento e
viene creato l'inventario dei beni

Inventario dei beni

- Il documento “Inventario dei Beni” viene estratto dall’applicazione di supporto al SGSI di perimetro (IBEA) secondo quanto indicato nella metodologia. Tale documento è strutturato in forma tabellare e riporta i seguenti elementi:
  - tipologia del bene;
  - nome del bene;
  - struttura organizzativa del proprietario/gestore;
  - nome del proprietario/gestore;
  - processo/macro attività.

Classificazione dei beni

La classificazione dei beni informativi viene fatta in base all'impatto aziendale causato dalla compromissione della ***Riservatezza***, ***Integrità***, ***Disponibilità***

… Catalogazione e classificazione dei beni …

- La classificazione dei beni, prevista da uno specifico controllo dello standard ISO/IEC 17799:2005 ha l'obiettivo di assicurare che ogni bene riceva un appropriato livello di protezione.

- Generalmente la classificazione/valorizzazione dei beni informativi viene effettuata mediante interviste a tutti coloro che sono proprietari del bene.

- Per la classificazione si utilizza un questionario con una serie di domande che mirano a valutare i danni derivanti dalla perdita dei requisiti RID.

- La classificazione dei beni provvede a determinare, per ciascun bene informativo ed in termini qualitativi, la classe di criticità associata a ciascuno dei requisiti RID (Alto, Medio, Basso, Trascurabile).

- Le classi di criticità concorrono alla definizione del livello di protezione e quindi ai controlli da attuare.

- Le classi di criticità RID concorrono alla definizione del livello di protezione adeguato: le informazioni con le stesse classi di criticità, a parità d'esposizione alle minacce, richiedono protezioni analoghe.
- Viene inoltre indicata la natura dal punto di vista Privacy delle informazioni (personale[1] o sensibile[2]/giudiziario[3]).
- Se il bene informativo ha dati di natura sia personale che sensibile/giudiziaria, la valutazione dell'entità del danno derivante dalla compromissione della Riservatezza deve essere assolutamente alta.
- Le classi di criticità concorrono alla definizione del livello di protezione e quindi ai controlli da attuare. I beni infrastrutturali nell'analisi del rischio condotta nel perimetro, ereditano la classe di criticità delle informazioni che trattano all'interno del perimetro.

[1] Per *dato personale* si intende, ai sensi dell'articolo 4 comma 1 lettera b) del D.Lgs 196/2003, qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

- [2] Per *dati sensibili* si intendono, ai sensi dell'articolo 4 comma I lettera d) del D.Lgs 196/2003, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
- [3] Per *dati giudiziari* si intendono, ai sensi dell'articolo 4 comma I lettera e) del D.Lgs 196/2003, i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del DPR 14 novembre 2002, n.313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

- Il calcolo della classe di criticità di un bene informativo viene fatto applicando un algoritmo alle risposte del questionario che:
  - serve a calcolare le classi di criticità dell'informazione
  - dà un peso a ciascuna risposta alle domande del questionario
    - N/A=…; Bassa=…; Media=…; Alta=…
  - somma i pesi assegnati alle varie risposte per il singolo attributo RID
  - determina le tre classi di criticità secondo la tabella seguente:

Classe di criticità	Ampiezza della classe
Nulla	xx<=p<=zz
Bassa	kk<=p<=tt
Media	yy<=p<=ww
Alta	rr<=p

Assessment del rischio: attività previste

- L'Assessment del rischio comprende:
  - *Individuazione e valutazione delle minacce*
  - *Identificazione delle vulnerabilità*
  - *Rilevazione e valutazione dei controlli*
  - *Valutazione del rischio residuo*
- Nel corso dell'attività viene prodotto il documento "Risultati dell'Assessment del Rischio" (RAR).
- Le prime tre attività sono di competenza dei gestori dei beni e vengono svolte predisponendo le schede dei beni.
- Il Responsabile di perimetro potrà anche acquisire i risultati di analoghe attività già svolte su beni comuni a più perimetri. In tale caso il Responsabile di Perimetro deve solo acquisirne i risultati per valutare il rischio residuo in relazione alle criticità dei dati trattati nel Perimetro.
- Il processo, condotto secondo i criteri indicati nella "Metodologia di assessment e trattamento del rischio", termina con la produzione del documento "*Risultati dell'Assessment del Rischio*".

Attività	Dati in ingresso	Documenti in uscita	Responsabilità			
			Resp. perimetro	Gest. Sw applicativo (2)	Gest. Comp. infrastrutturali	Sicurezza logica
Individuazione e valutazione delle minacce	Inventario dei beni Perimetro e scenario di riferimento Politica per la sicurezza delle informazioni del perimetro	Risultati dell'assessment del rischio	P	R	R	P (1)
Identificazione delle vulnerabilità	Inventario dei beni del perimetro Perimetro e scenario di riferimento	Risultati dell'assessment del rischio	P	R	R	P(1)
Rilevazione e valutazione dei controlli	Inventario dei beni	Risultati dell'assessment del rischio	P	R	R	P(1)
Valutazione del rischio residuo	Inventario dei beni	Risultati dell'assessment del rischio	R	P		P

Legenda

R = Responsabile

P = Partecipa

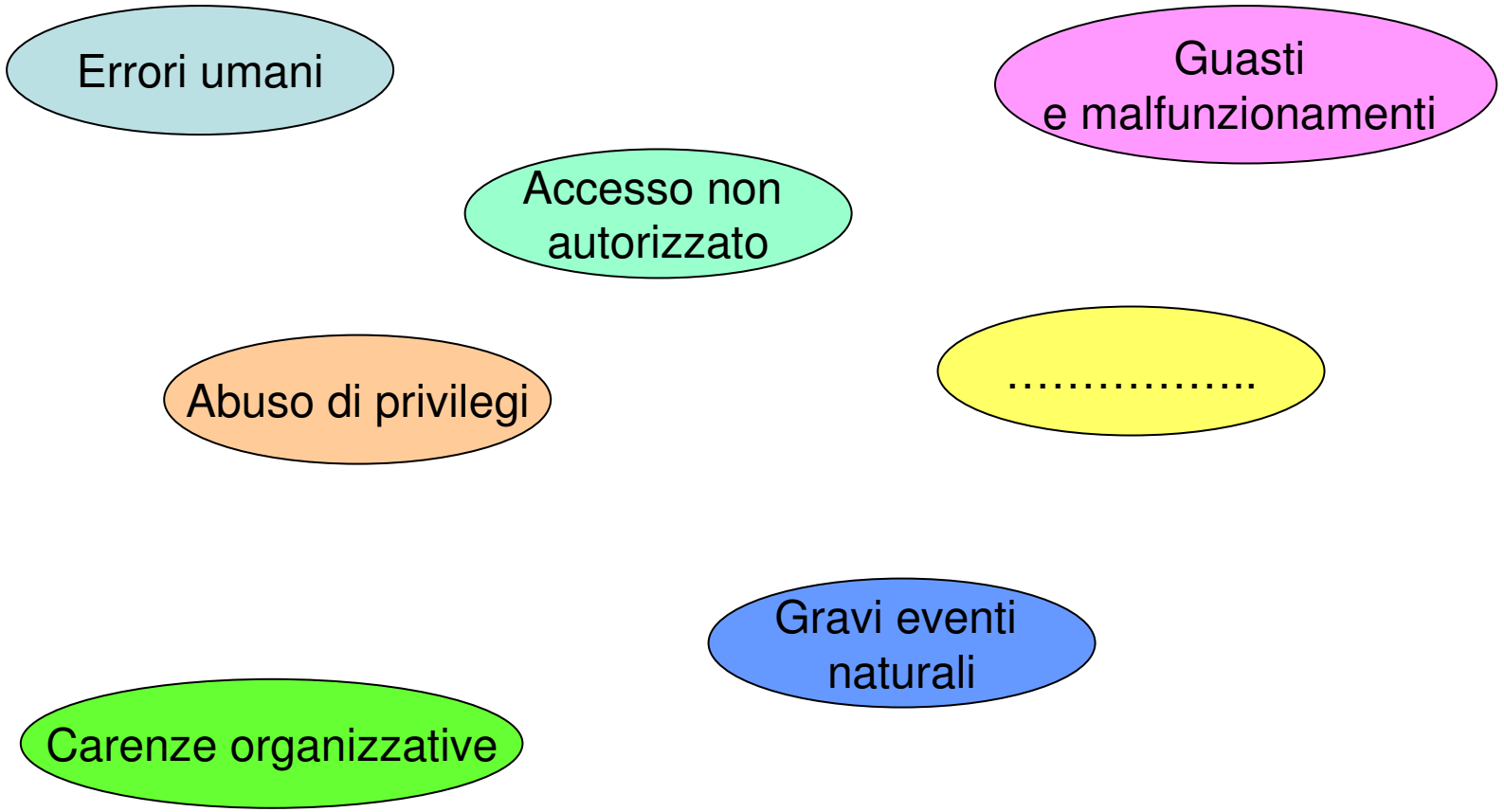
(1) La partecipazione della struttura che si occupa di sicurezza logica non è vincolante per tale attività.

(2) Il Gestore del software applicativo coincide in genere con il Responsabile dell'applicazione

Valutazione delle minacce

Individuazione di tutte le minacce che insistono sui beni infrastrutturali inventariati. Ad ogni minaccia viene assegnato un livello di esposizione, funzione della frequenza di accadimento e dell'entità dell'impatto

Esempi di minacce



Partendo dalle minacce identificate si procede all'identificazione delle vulnerabilità

Identificazione delle vulnerabilità

Identificazione delle carenze di sicurezza intrinseche del bene infrastrutturale e del conseguente impatto

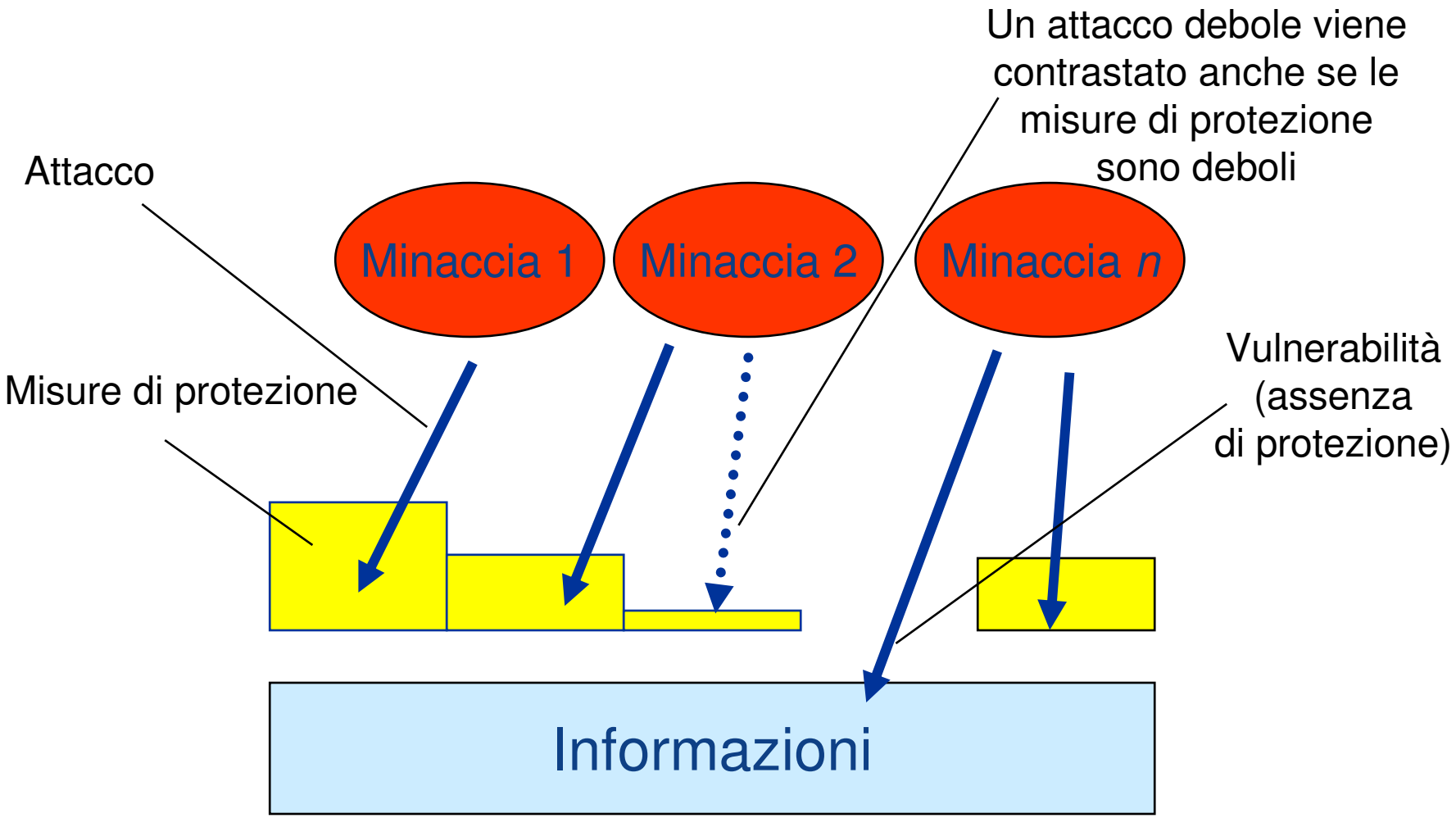
L'individuazione delle vulnerabilità viene effettuata sulla base delle conoscenze specifiche dei Gestori e consente di:

- valutare il Livello di Esposizione (LE)
- individuare i controlli che riducono la vulnerabilità

La Vulnerabilità è:

- l'essere in condizione di essere attaccato, leso, danneggiato,
- un punto debole nella protezione del bene,
- una condizione che facilita anche una potenziale azione negativa delle minacce.

L'abbattimento del rischio si ottiene riducendo il livello di vulnerabilità delle minacce.


Un attacco debole viene contrastato anche se le misure di protezione sono deboli
Attacco
Minaccia 1
Minaccia 2
Minaccia *n*
Misure di protezione
Vulnerabilità (assenza di protezione)
Informazioni

Esempi di Vulnerabilità

- Carenza organizzativa
- Personale non addestrato sulle problematiche della sicurezza
- Errori nella gestione dei diritti di accesso alle informazioni
- Assenza di controlli sulle procedure di sicurezza
- Carenza controlli nella circolazione delle persone
- Mancanza di protezioni perimetrali
- Carenza negli aggiornamenti delle protezioni perimetrali
- ……

Rilevazione dei controlli

Consiste nella rilevazione delle protezioni presenti e della loro adeguatezza rispetto al Livello di Esposizione alle minacce, per valutare se le protezioni attuali sono commisurate ai rischi, sia per quantità, sia per robustezza

Per robustezza si intende la capacità di:

- resistere ad attacchi più o meno sofisticati
- resistere ad azioni di aggiramento e di riduzione della efficacia delle protezioni
- assicurare e monitorare l'efficacia delle protezioni nel tempo

Definizione dei controlli da implementare

Valutazione dei controlli da implementare per ridurre il valore dei rischi ad un livello accettabile

- L'attività è mirata alla definizione dei controlli di sicurezza, non ancora realizzati o inadeguati in termini di robustezza, che consentono di raggiungere, per ogni bene, un livello di rischio residuo accettabile, in linea con le politiche aziendali.
- L'attività prevede due passi:
  - definizione dei controlli applicabili;
  - definizione del profilo di protezione ottimale.
- Una volta definiti i controlli applicabili deve essere prodotto il documento "Dichiarazione di Applicabilità" (DA).
- La definizione del profilo di protezione ottimale porta alla creazione di una tabella, da inserire nel documento "Piano di trattamento del rischio".

Trattamento del rischio: Dichiarazione di applicabilità (controlli applicabili)

- L'attività consiste nell'analisi dei controlli previsti dallo standard ISO/IEC 27001:2005, con l'obiettivo di identificare quelli applicabili, in tutto o in parte, e quelli non applicabili, rispetto al contesto analizzato.
- Nel documento "Dichiarazione di Applicabilità" (DA) vanno motivate le scelte effettuate rispetto ad ogni controllo.
- La informazioni sull'applicabilità dei controlli vengono dedotte dall'assessment e dalla "Dichiarazione di applicabilità generale".
- In linea generale sono dichiarati non applicabili i controlli:
  - definiti non applicabili nella "Dichiarazione di applicabilità generale";
  - per i quali non sono risultate presenti nell'ambito le minacce che questi contrastano;
  - che, pur riferiti a minacce presenti nell'ambito, sia stato scelto di contrastare tali minacce e di conseguenza i rischi che ne derivano con altri controlli ritenuti più efficienti, in linea con i requisiti di operatività e di prestazioni. (Es: il controllo 11.04.3 (Identificazione dell'apparato sulla rete) nel caso in cui si è preferito ricorrere all'autenticazione degli utenti).

Pianificazione del trattamento del rischio

Definizione del piano di attività relativo ai controlli da implementare

In base ai risultati ottenuti nelle fasi di “Catalogazione e Classificazione dei beni”, “Assessment del Rischio”, viene prodotto il “Piano di Trattamento del Rischio” (PTR), che contiene gli interventi necessari per abbattere il rischio residuo al livello ritenuto accettabile, con l’indicazione delle priorità, delle responsabilità e della tempistica.

- Obiettivo dell'attività è quello di pianificare gli interventi necessari per portare il rischio residuo ad un valore accettabile.
- Al termine dell'attività, deve essere prodotto il "Piano di Trattamento del Rischio" (PTR).
- L'attività si basa sui risultati ottenuti nelle fasi di "*Catalogazione e Classificazione dei beni*", "*Assessment di sicurezza*" e sulla definizione del Profilo di Protezione ottimale.
- Per ogni istanza di controllo che non sia ritenuto adeguata, ovvero abbia scostamento diverso da Nullo, viene assegnata una priorità, che coincide con lo scostamento fra la graduazione richiesta e quella effettiva.
- In conformità a tali considerazioni, vengono elencati e documentati, con la collaborazione dei Gestori dei beni in esame, gli interventi necessari per abbattere il rischio residuo ad un livello accettabile.
- La definizione dei livelli accettabili è riportata nel documento SOGEI "*Criteri e livelli di accettabilità del rischio residuo*".

- L'insieme degli interventi previsti confluiscono nel "Piano di trattamento del rischio" (PTR) dove sono riportate, per ogni bene infrastrutturale e per ogni controllo pertinente, le seguenti informazioni:
  - l'istanza di controllo (bene a cui l'istanza di controllo è associata e codice del controllo);
  - le specifiche attuative che l'intervento realizza;
  - la responsabilità dell'azione (Gestore del bene);
  - il grado di robustezza richiesto;
  - il grado di robustezza effettivo;
  - l'indice di priorità dell'azione.

- Il Piano di Trattamento del Rischio, una volta definito, deve essere analizzato per definire le risorse necessarie agli interventi ritenuti prioritari e verificarne la disponibilità

Accettazione del livello di rischio

L'applicazione dei controlli consente di ridurre il livello di rischio entro limiti ritenuti accettabili dalla Direzione

- L'attività, ha i seguenti obiettivi:
  - verificare e condividere con la direzione l'accettabilità dei rischi residui dopo l'applicazione degli interventi previsti nel Piano di Trattamento del Rischio,
  - documentare la conformità alle misure minime Privacy,
  - riesaminare gli interventi in un'ottica aziendale per analizzare eventuali ricadute o sinergie con altri perimetri.

- Al termine dell'attività deve essere stilato:
  - il "**Verbale di accettazione del rischio**", che riporta le soluzioni adottate in merito al rischio residuo.
  - Il "**Verbale di conformità Privacy del perimetro**" che attesta la conformità.

… Accettazione del livello di rischio

- L'accettazione del rischio rappresenta l'attività di approvazione della Direzione aziendale delle modalità di trattamento del rischio pianificate.

- Il Responsabile del Perimetro predispone il "*Verbale d'accettazione del rischio*" che, dopo la verifica da parte della Segreteria Tecnica, deve essere approvato dal responsabile della Funzione a cui appartiene il Perimetro, dal Responsabile Operativo del SGSI e successivamente approvato dal Responsabile SGSI (AD/).

- L'attività consiste nella realizzazione e messa in produzione, da parte dei Gestori dei beni, degli interventi previsti nel Piano di Trattamento del Rischio.

- Gli interventi possono essere: formazione del personale, realizzazione o modifiche di procedure, impostazione delle matrici di accesso, introduzione di contromisure fisiche o logiche, ecc.

- Eventuale documentazione operativa prodotta deve essere gestita secondo quanto indicato nel documento "*Documentazione delle procedure inerenti aspetti di sicurezza*".

- Il Responsabile di Perimetro viene informato dello stato di avanzamento degli interventi e ne verifica gli esiti.

Parte 6 - Gestione di un Bene Infrastrutturale: modalità operative

- La scheda informativa di un bene infrastrutturale è composta da cinque sezioni:
  - *Dati identificativi del bene,*
  - *Minacce che incombono sul bene e calcolo del Livello di Esposizione,*
  - *Contromisure da applicare,*
  - *Correlazione tra minacce e controlli,*
  - *Requisiti relativi alla tutela della privacy.*

- La scheda del bene contiene tutte le informazioni necessarie per poter effettuare l'analisi del rischio e di conformità privacy nell'ambito di un uno specifico perimetro.

- Il Gestore del bene è chiamato a partecipare alle attività di Analisi del Rischio e delle conformità alle norme, di competenza primaria del Responsabile di Perimetro. In particolare:
  - Fornisce tramite la scheda del bene le informazioni necessarie per eseguire l'analisi del rischio
  - Chiarisce ed approfondisce aspetti relativi al modo con cui il bene partecipa al SGSI del perimetro. Durante tale approfondimento può evidenziarsi l'esigenza di creare, a partire da un bene a livello aziendale, un bene figlio a livello di perimetro che ne rappresenti meglio le specificità (per esempio livelli di esposizione a minacce, controlli o graduazioni diverse).
- Il Gestore partecipa alla preparazione dei "Risultati dell'Assessment del Rischio" (RAR).
- Il Gestore del bene concerta con i Responsabili dei perimetri e/o la Segreteria Tecnica eventuali interventi di miglioramento delle contromisure del bene da inserire nel Piano di Trattamento del Rischio (PTR) del perimetro.

- Il Gestore apporta il proprio contributo di conoscenza del bene per la gestione delle contromisure e per la realizzazione degli interventi di miglioramento stabiliti con i Responsabile di Perimetro.

- Gli interventi possono essere di tipo tecnologico (acquisto di nuovi prodotti, riconfigurazioni di sistemi, ecc), organizzativo (nuovi ruoli o compiti per gli addetti alla gestione del bene) o documentale (redazione o modifica alla documentazione operativa, ecc).

- Ai fini del miglioramento del SGSI aziendale, il Gestore del bene ha l'obbligo di segnalare qualsiasi evento di sicurezza correlato al proprio bene, secondo quanto previsto dalla procedura *"Modalità operative per la segnalazione degli incidenti di sicurezza".*

Modalità operative per la compilazione della scheda del bene

- La scheda di un bene infrastrutturale permette di disporre delle informazioni sugli aspetti rilevanti del bene ai fini della sicurezza delle informazioni; tali notizie vengono utilizzate nell'assessment del rischio e nell'analisi di conformità privacy per i perimetri che utilizzano il bene infrastrutturale.

- La scheda di un bene infrastrutturale, effettuata dal Gestore del bene, nasce dalla:
  - identificazione e descrizione del bene stesso
  - assessment delle minacce e delle contromisure
  - analisi delle misure minime di sicurezza previste dalla normativa privacy

Parte 7 – Applicativo IBEA

- IBEA:
  - è una metodologia ed un'applicazione software di supporto SGSI realizzata per governare la sicurezza con un processo maturo,
  - costituisce il sistema informativo per la gestione della sicurezza "integrata" e non solo un'applicazione di analisi del rischio,
  - è un'applicazione web che utilizza la metodologia di analisi del rischio proprietaria,
  - gestisce le misure di sicurezza evidenziando la loro eventuale adeguatezza ai requisiti definiti,
  - esegue automaticamente l'analisi del rischio e l'analisi di conformità a norme di legge (privacy),
  - fornisce indicatori, a più livelli, di rischio e di conformità
  - produce report e documentazione per la Direzione aziendale e per i Gestori dei beni infrastrutturali e Responsabili di perimetro.

Parte 6 - Conclusioni

Considerazioni finali!