Implementazione delle Politiche di Sicurezza

MODELLO PER L'IMPLEMENTAZIONE DELLE POLITICHE SICUREZZA INFORMATICA

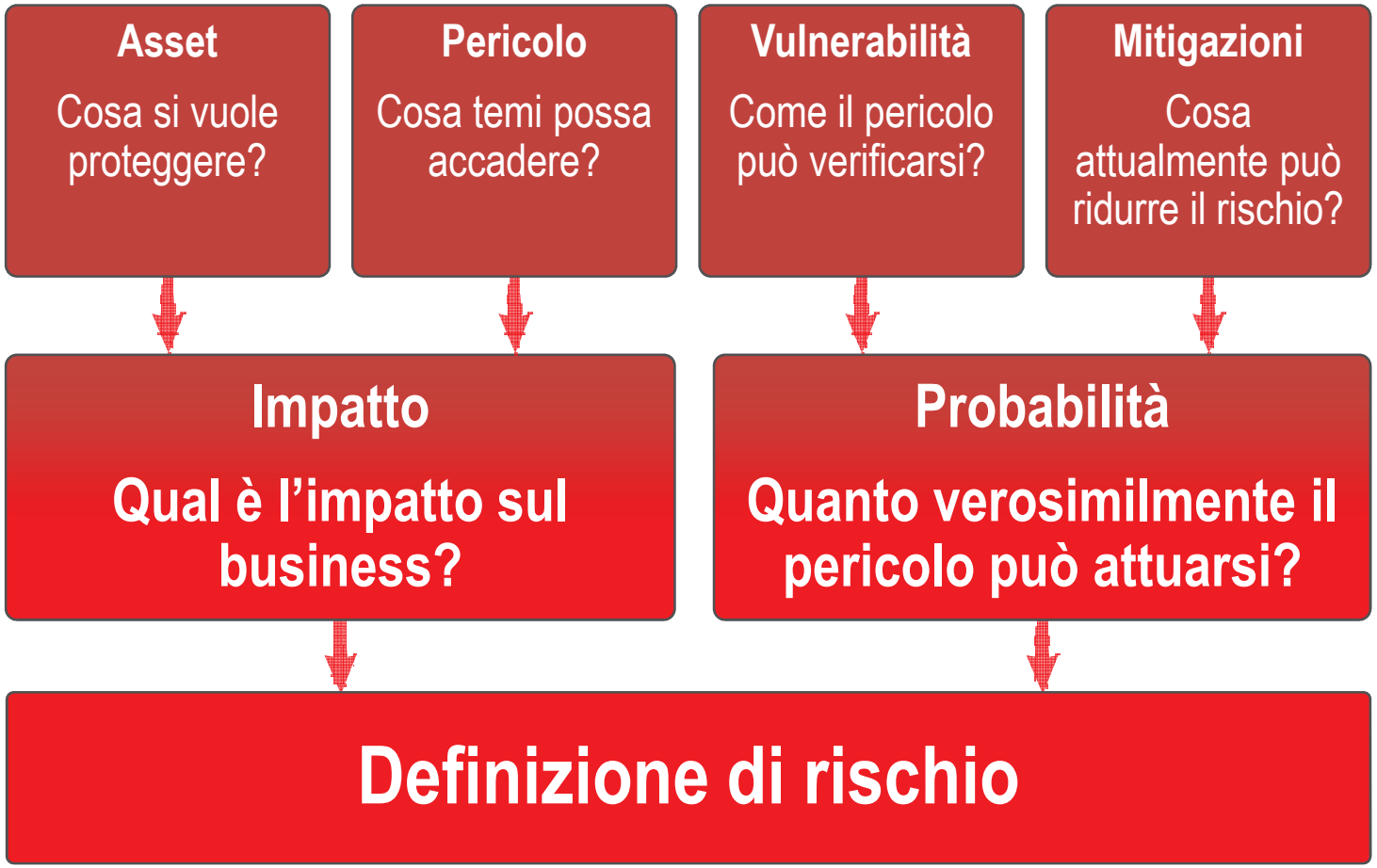
Il modello teorico dell'ingegneria della sicurezza prevede **tre passi distinti**:

Analisi delle minacce (Threat Model) - questa è la fase in cui si cerca di capire le reali minacce e se ne valutano i rischi.

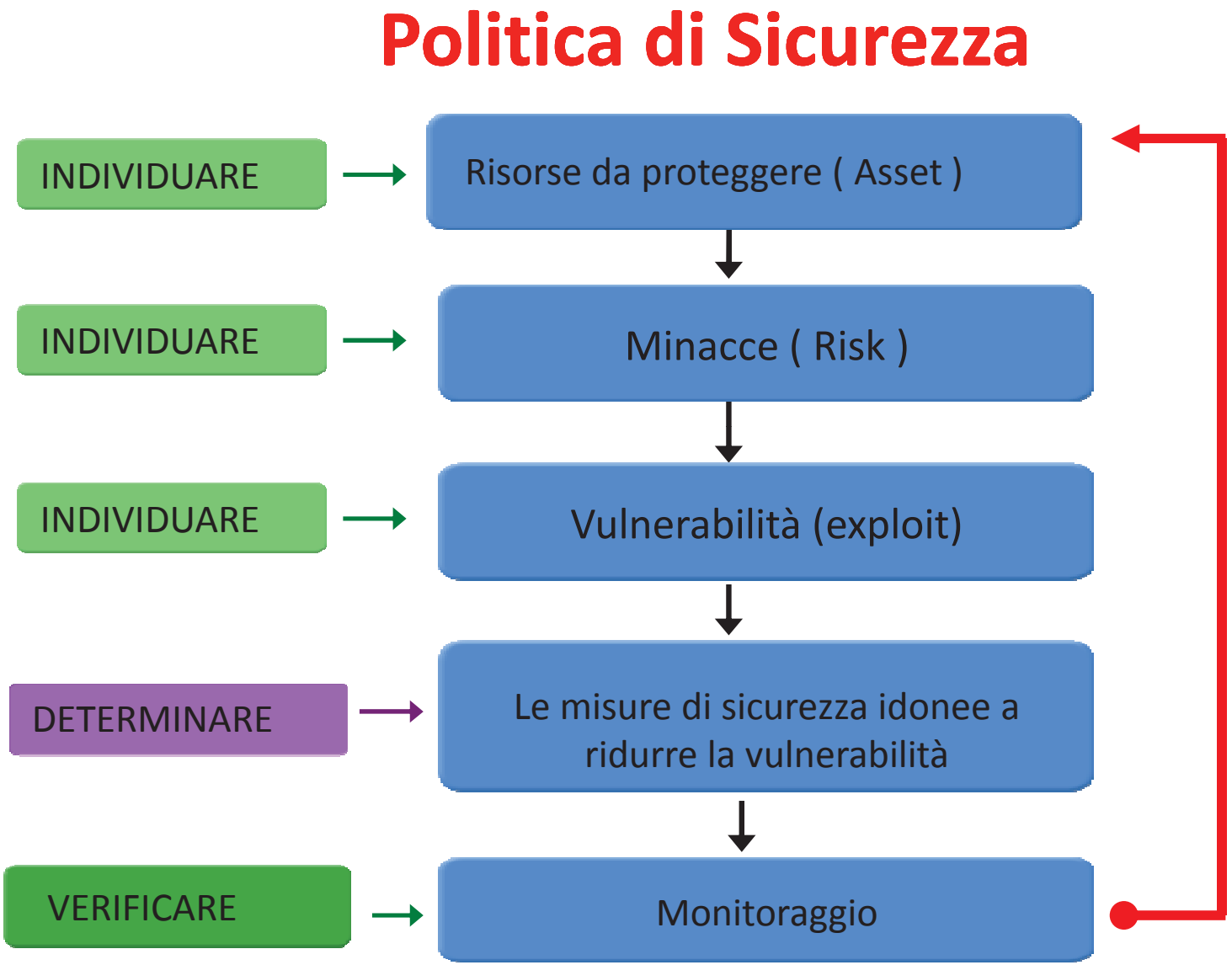
Politiche di sicurezza (Security Policy) - è una fase strategica, pertanto approvata dalla direzione, nella quale sono enunciati i principi generali.

Tecnologie di Sicurezza (Security Technologies) - è la fase nella quale si progettano (e realizzano) le adeguate contromisure.

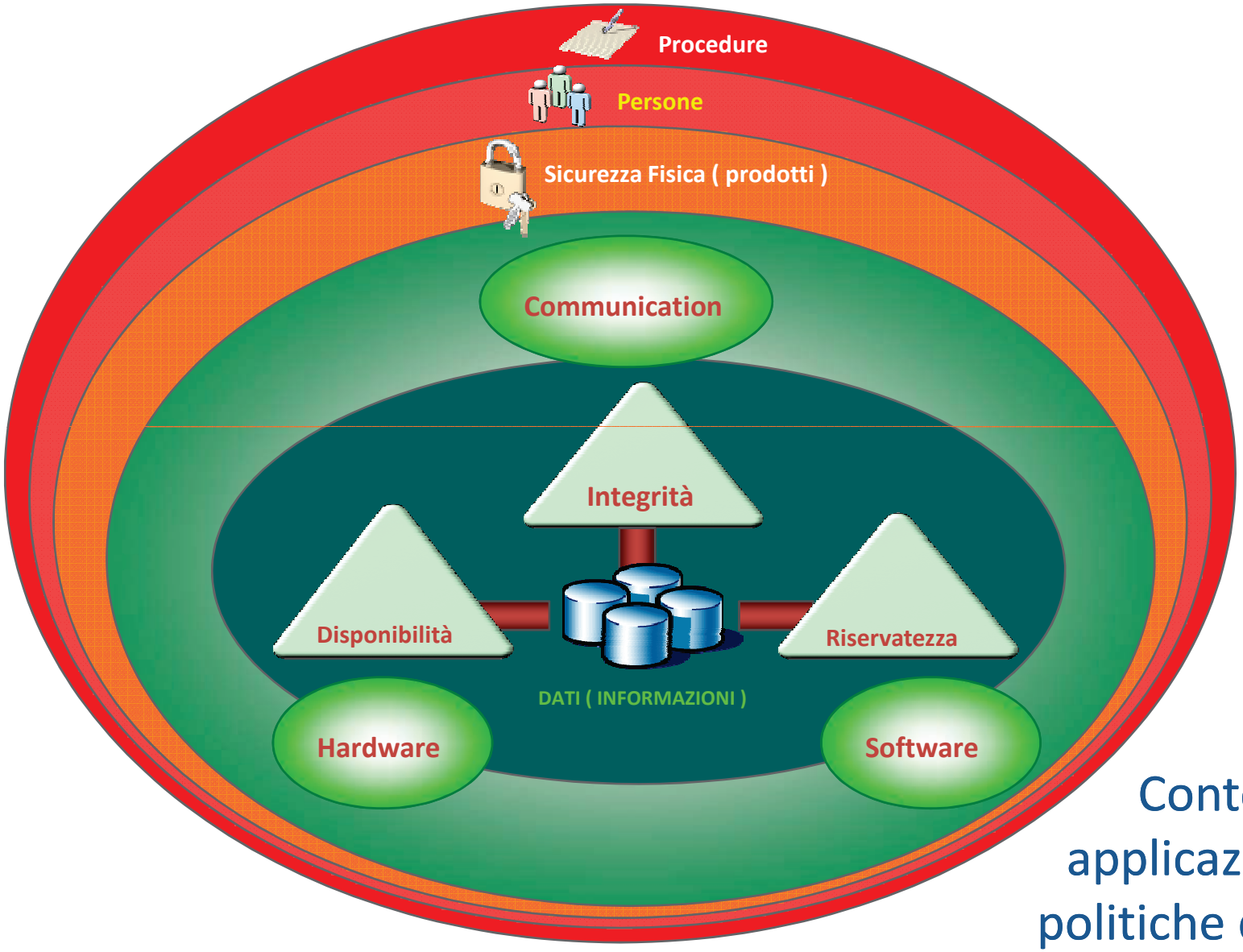
Processo di definizione dei rischi



Modello di Sicurezza Informatica


Politica di Sicurezza
INDIVIDUARE
Risorse da proteggere (Asset)
INDIVIDUARE
Minacce (Risk)
INDIVIDUARE
Vulnerabilità (exploit)
DETERMINARE
Le misure di sicurezza idonee a ridurre la vulnerabilità
VERIFICARE
Monitoraggio

Implementazione delle Politiche di Sicurezza



Contesto di applicazione delle politiche di sicurezza

3 Leggi fondamentali della Sicurezza Informatica

INDIPENDENTEMENTE DALLE POLITICHE DI SICUREZZA CHE POSSONO ESSERE IMPLEMENTATE è necessario ricordare tre delle leggi fondamentali della sicurezza informatica:

***Mai dire mai**: il dichiarare un sistema, un approccio, una soluzione, una metodica definitivamente sicuri e inattaccabili significa, a prescindere dalla scaramanzia, peccare di superficialità*

***La sicurezza totale non esiste**: è evidentemente un postulato, ma è indispensabile ribadirlo, specie se si guarda al problema da una prospettiva d'alto livello.*

***Non si possono risolvere i problemi di sicurezza con il solo software**. Conosciuta anche come la **legge di Ranum**, quest'affermazione è un chiaro messaggio: il malicious hacking si affronta su più livelli. I concetti sono esattamente gli stessi da un punto di vista legale, sia dal lato attivo (ovvero di chi debba prendere delle misure atte a scongiurare eventuali conseguenze nefaste) sia dal lato passivo (ovvero di chi debba semplicemente applicare alcune norme tecniche che spesso sono divenute espressamente norme giuridiche)*

Principio 1

NON ESISTONO SISTEMI SICURI

- Il software non può essere perfetto (privo di errori);
- Il mito del sistema inviolabile è affine al mito del caveau non svaligiabile o della nave inaffondabile (e.g. Titanic).
- Il grado di sicurezza è dato dal tempo necessario per violare il sistema, dall'investimento necessario e dalla probabilità di successo.

ne consegue che…

UN SISTEMA PIU' E' COMPLESSO E
PIU' E' INSICURO

... e la funzione è più che proporzionale.

- Per fare sistemi sicuri occorre applicare la **KISS rule**, cioè *Keep It Simple and Stupid*.
- Attenzione: i sistemi da proteggere possono essere molto complessi ma il sistema di protezione deve essere estremamente semplice. Ogni complessità non necessaria è solamente fonte di possibili errori e falle.

Principio 2

LE ENTITÀ COMPONENTI DI UN SISTEMA SICURO SONO TRE:

- hardware
- software
- Wetware (il fattore umano)
- Senza continuo apporto di lavoro nessun sistema può essere sicuro. Ciò che è sicuro oggi potrebbe non esserlo più domani, perché per esempio è stato scoperto un difetto del sistema. I sistemi che non vengono aggiornati diventano quindi fragili.

Principio 3

SICUREZZA = CONOSCENZA

- Nessun sistema del quale non si può comprendere a fondo il funzionamento può essere considerato sicuro.

L’importanza della conoscenza

- La conoscenza degli strumenti di sicurezza e la consapevolezza dei problemi collegati devono essere patrimonio di tutti gli utenti;
- L'illusione di sicurezza è più dannosa della assoluta mancanza di sicurezza;
- A un sistema riconosciuto insicuro non si possono affidare informazioni sensibili.

Stato dell'arte in Sicurezza

- La sicurezza

1. Richiederebbe spesso il ridisegno, il che non è sempre possibile!
2. E' una proprietà di vari livelli architetturali
   [OS, rete, ...]
3. Non è un semplice predicato booleano

4. E' costosa nel senso di risorse computazionali, gestione, mentalità, utilizzo
5. Rimane un campo aperto anche per i colossi dell'Informatica

Implementazione delle Politiche di Sicurezza

Per quanto riguarda, più in generale, le politiche da sviluppare per contrastare una minaccia, si può tenere in mente che le vulnerabilità possono essere:

eliminate - oppure rimosse o neutralizzate

minimizzate - ridotte cioè ad un livello residuale accettabile

monitorate – in questo caso ci si riferisce alle sole vulnerabilità già minimizzate cioè messe in uno stato di controllo continuo

Alfine di poter ottimizzare i processi delle politiche di sicurezza, rendendo più rapida ed efficace la loro applicazione, i **metodi di accertamento e valutazione** delle minacce rappresentano degli strumenti indispensabili.

Valutazione

La valutazione effettua una comparazione delle politiche di sicurezza adottate e standard internazionali , “de facto” e best practise al fine di classificare il sistema informatico oggetto di studio .

Alcuni tra i più importanti documenti per i criteri di valutazione e classificazione della sicurezza di sistemi e componenti ICT :

- Orange Book USA
- ITSEC Europa
- Combined Federal Criteria USA

Esempio di classificazione della sicurezza dei sistemi di calcolo : **Orange Book**

Il primo standard sulla sicurezza sviluppato dal Dipartimento di Difesa degli USA

Diversi livelli:

- D1 – Minimal Protection:
  - non esiste protezione per l'hardware e non ci sono autenticazioni (MS-DOS – Ms-Win – Apple – Mac)
- C1 – Discretionary Security Protection
  - Sicurezza dei sistemi UNIX, protezione HW, autenticazione degli utenti
- C2 – Controlled Access Protection
  - Aggiunge un maggior controllo, rispetto al livello superiore, nell'accesso alle risorse ed ai file
- B1 – Labelled Security Protection
  - Supporta una sicurezza multilivello
- B2 – Structured Protection
  - Ogni risorsa deve essere classificata e le possono essere assegnati diversi livelli di sicurezza
- B3 – Security Domain
  - E' presente un apposito HW per rafforzare la sicurezza del dominio
- A – Verified Design
  - Prevede l'esistenza di tutti i sottolivelli, include la verifica dei processi e controlli stringenti, inoltre l'HW ed il SW devono essere protetti durante la spedizione per evitare intrusioni al sistema

Esempio di classificazione della sicurezza dei sistemi di calcolo : **Orange Book**

- **Orange Book.** Documento pubblicato dal Dipartimento della Difesa americano (D.O.D)
- Sono specificate quattro categorie di sicurezza:A, B, C, D (in ordine decrescente).
- **Categoria D.** Non ha livelli di sicurezza.
  - Esempi MS-DOS, Windows 3.1.

Esempio di classificazione della sicurezza dei sistemi di calcolo : **Orange Book**

- **Categoria C.** Suddivisa in C1 e C2:
- **C1.** La Trusted Computing Base consente:
  - Autenticazione degli utenti (password). I dati di autenticazione sono protetti rendendoli inaccessibili agli utenti non autorizzati.
  - Protezione dei dati e programmi propri di ogni utente.
  - Controllo degli accessi a oggetti comuni per gruppi di utenti definiti
- **Esempio**: Unix
- *C2*. La TCB consente
  - oltre a quanto definito per la C1, il controllo degli accessi su una *base individuale*.
- Esempio UNIX, Windows NT, 2000,2003,2008.

Esempio di classificazione della sicurezza dei sistemi di calcolo : **Orange Book**

- **Categoria B**. Suddivisa in B1, B2 e B3
  - *B1*. La TCB consente, oltre a quanto definito in C2, l'introduzione dei livelli di sicurezza (modello Bell-La Padula). Almeno due livelli.
  - *B2*. La TCB estende l'uso di etichette di riservatezza ad ogni risorsa del sistema, compresi i canali di comunicazione.
  - *B3*. La TCB consente la creazione di liste di controllo degli accessi in cui sono identificati utenti o gruppi *cui non è consentito* l'accesso ad un oggetto specificato.

Esempio di classificazione della sicurezza dei sistemi di calcolo : **Orange Book**

- **Categoria A**. Suddivisa in A1 e classi superiori
  - *A1*. E' equivalente a B3, ma con il vincolo di essere progettato e realizzato utilizzando metodi formali di definizione e verifica.
  - Un sistema appartiene ad una classe superiore ad A1 se è stato progettato e realizzato in un impianto di produzione affidabile da persona affidabile

Politiche, classificazione e valutazione possono soddisfare queste domande?

- Riservatezza:
  - la comunicazione è stata intercettata?
- autenticazione:
  - l'utente è veramente chi dice di essere?
- Integrità:
  - i dati ricevuti sono proprio quelli spediti?
- Non ripudio:
  - il mio interlocutore può ritrattare quello che ha detto?
- Disponibilità:
  - il mezzo di comunicazione è stato reso inutilizzabile?
- Autorizzazione:
  - ogni utente può accedere solo alle risorse cui ha diritto?

IN PARTE SI MA NECESSITANO DI…. STRATEGIE

Esempi di principi e strategie 1/4

- Minimi privilegi:
  - ogni oggetto (utente, programma, ecc.) deve avere solamente i privilegi *minimi indispensabili* per quello che deve fare.
- Difesa in profondità:
  - non fare affidamento su di *un solo* meccanismo di sicurezza, per forte che possa sembrare.
- Minimizzare i punti di accesso:
  - un numero ridotto di punti di accesso (uno solo?) rende più facile il controllo.
- Cercare l'anello più debole:
  - essere coscienti dei propri punti deboli e rafforzarli fino a rendere il rischio "accettabile".

Esempi di principi e strategie 2/4

- A prova di errore (*Fail-Safe*):
  - quando si verifica un errore (prima o poi succede...) il sistema non deve permettere l'accesso agli intrusi, anche a costo di tener fuori gli utenti legittimi.
- Il non espressamente permesso è proibito (*Default Deny*):
  - *Fail-Safe*;
  - la visione dell'utenza è esattamente l'opposta;
  - i servizi vengono abilitati uno per uno sulla base delle effettive necessità, tutti gli altri sono disabilitati.
- Partecipazione universale
  - non è possibile (o almeno avrebbe costi elevatissimi) la sicurezza senza la partecipazione degli utenti.

Esempi di principi e strategie 3/4

- Diversità di difese:
  - non solo più di un meccanismo di sicurezza, ma possibilmente di tipi diversi.
- Semplicità:
  - sistemi semplici sono più facili da capire e mantenere;
  - programmi complessi sono *sicuramente* afflitti da bug, alcuni dei quali possono avere implicazioni di sicurezza.

Esempi di principi e strategie 4/4

- Sicurezza via mancanza di informazioni (*Security Through Obscurity*)?
  - Sbagliato
    - una macchina collegata ad Internet con l'unica protezione che nessuno ne è a conoscenza;
    - un server in modo che ascolta su di una porta diversa da quella di default;
  - Corretto
    - non divulgare i dettagli del proprio NID system;
    - informazioni dettagliate sul proprio firewall (protocolli ammessi, modello, ecc. ecc.)

Controlli Fisici

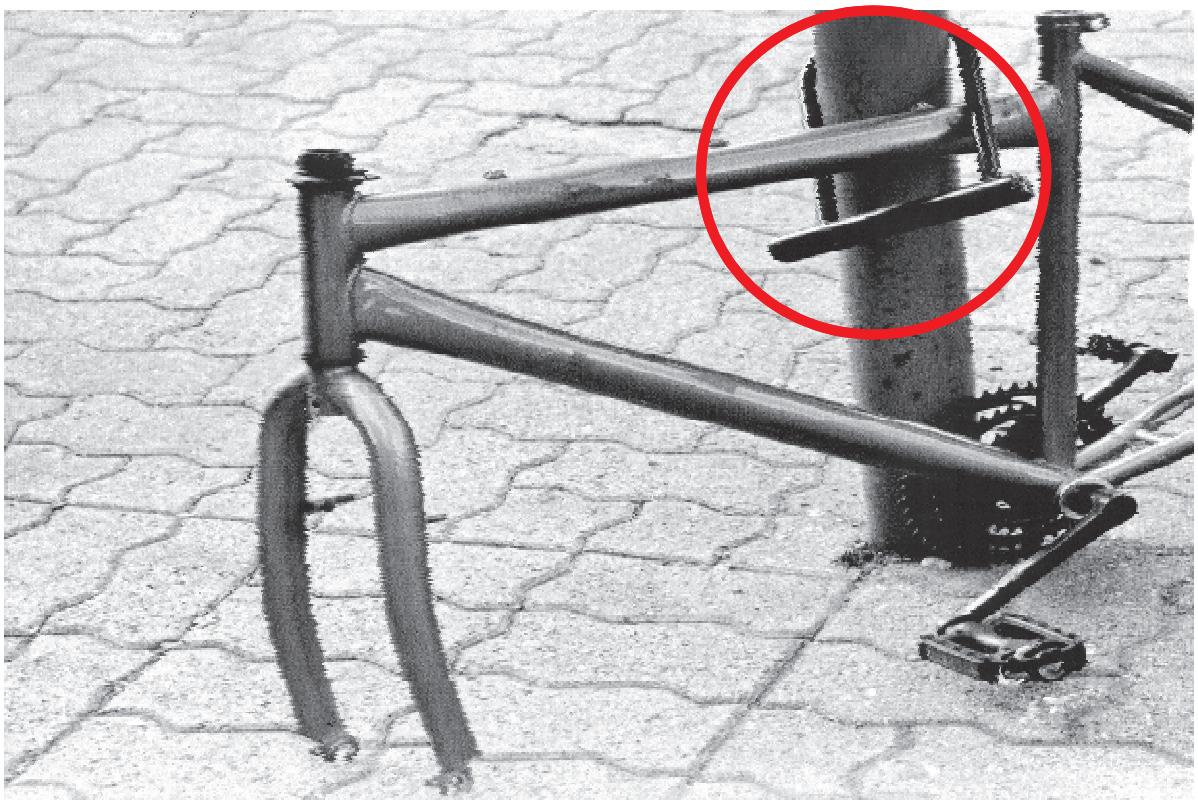
Oltre alle misure di sicurezza precedentemente elencate che possono essere utilizzate per proteggere il sistema ed i dati in esso contenuti, possono essere anche utilizzati ulteriori accorgimenti.

Le misure di sicurezza a livello fisico evitano danneggiamenti di strutture o dati.

Tra questi accorgimenti possiamo citare, ad esempio:

- **Accesso controllato ai locali dei sistemi**
- **Registrazione degli accessi**
- **Continuità elettrica**
- **Protezione dei nastri di backup (**da danneggiamenti casuali, o volontari)
- **Controllo degli accessi ai dati**
- **Autenticazione degli utenti**
- **Delimitazione degli spazi logici**
- **Tracking dell'attività**

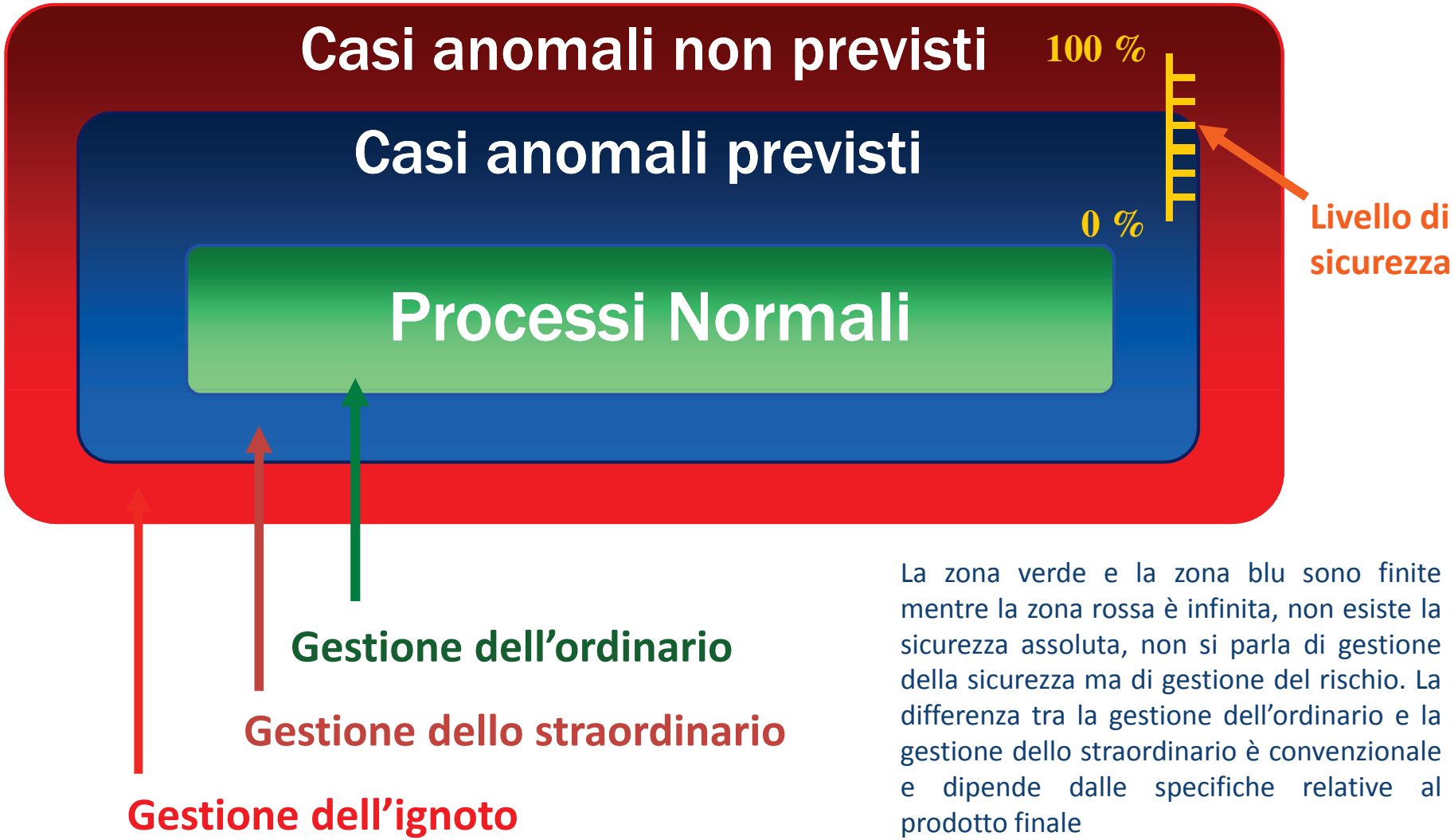
I prodotti funzionano molto spesso egregiamente….



ma da soli non bastano.

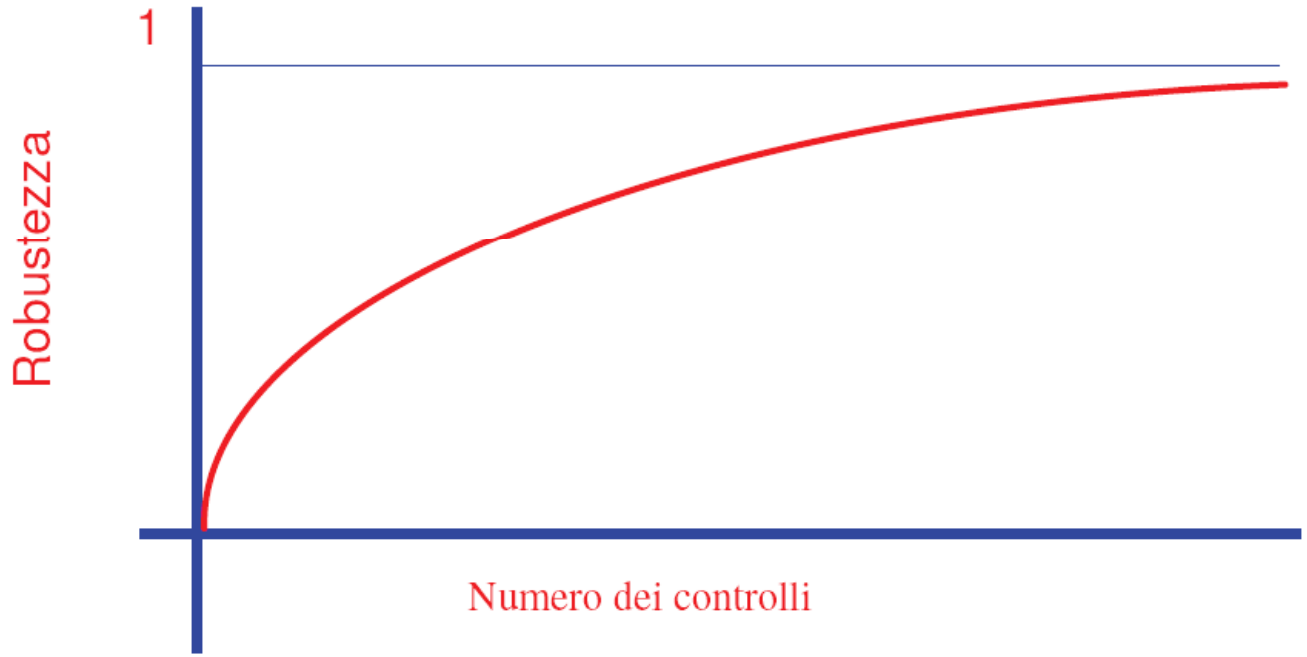
Dobbiamo sempre realizzare politiche di sicurezza che tengano conto di misure preventive in grado di gestire le anomalie ipotizzabili e contromisure per gestire le anomalie imponderabili e tener sempre conto di un rischio residuo.

Implementazione delle Politiche di Sicurezza



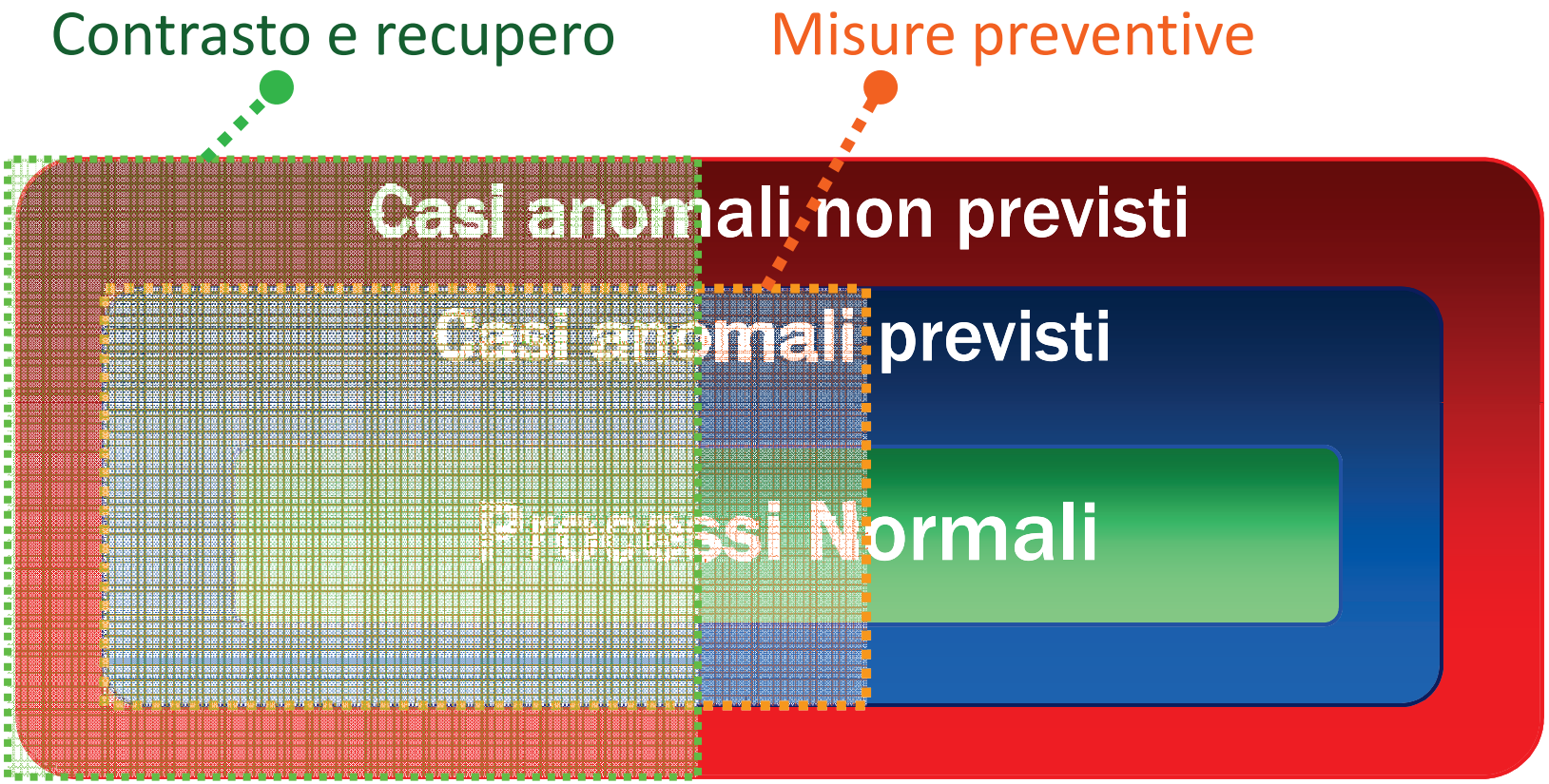
La zona verde e la zona blu sono finite mentre la zona rossa è infinita, non esiste la sicurezza assoluta, non si parla di gestione della sicurezza ma di gestione del rischio. La differenza tra la gestione dell'ordinario e la gestione dello straordinario è convenzionale e dipende dalle specifiche relative al prodotto finale

Maggiori sono i controlli maggiore è la robustezza del sistema.



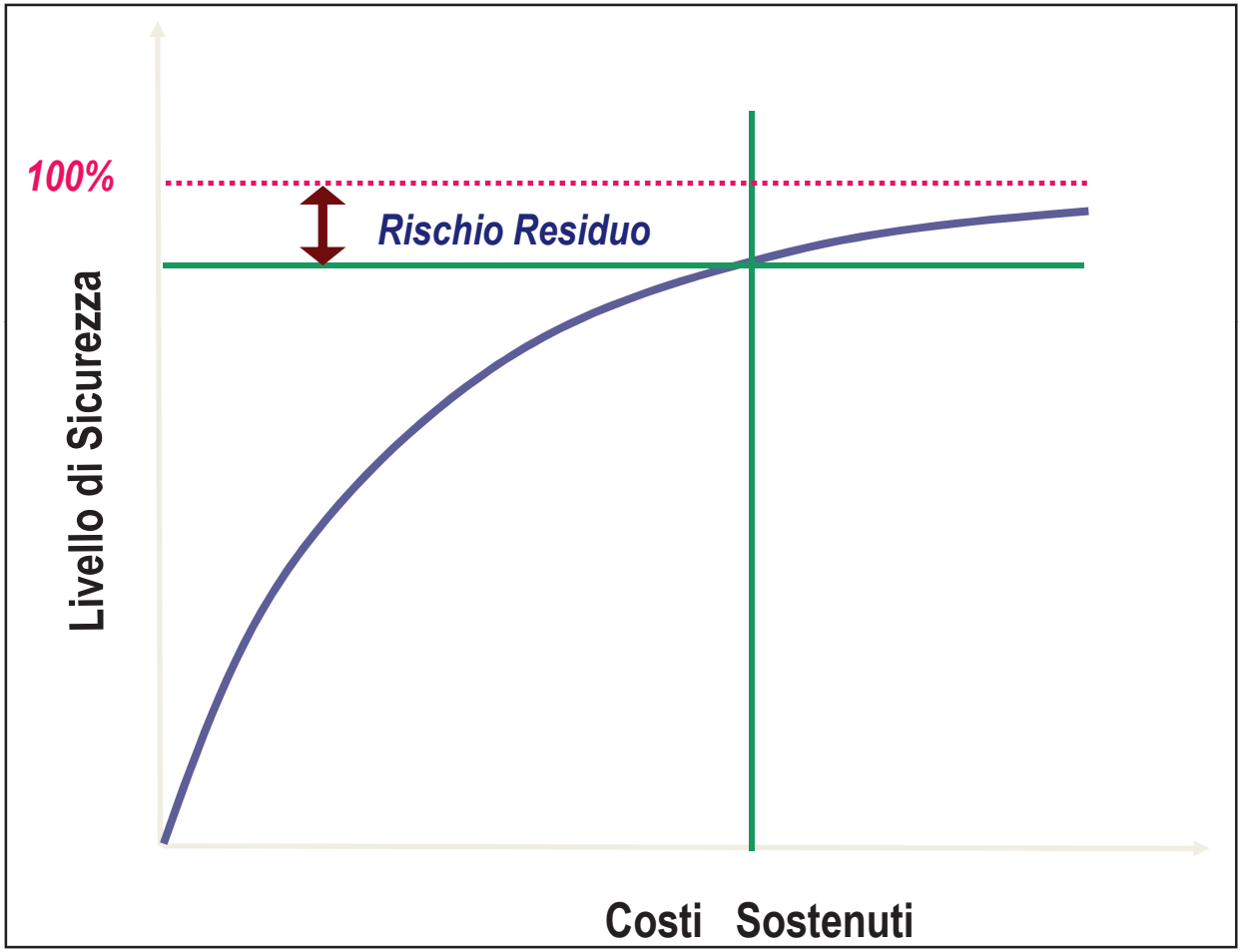
MA…PIU' I CONTROLLI INSERIAMO PIU' RISCHIAMO DI DANNEGGIARE LE PRESTAZIONI.

Implementazione delle Politiche di Sicurezza



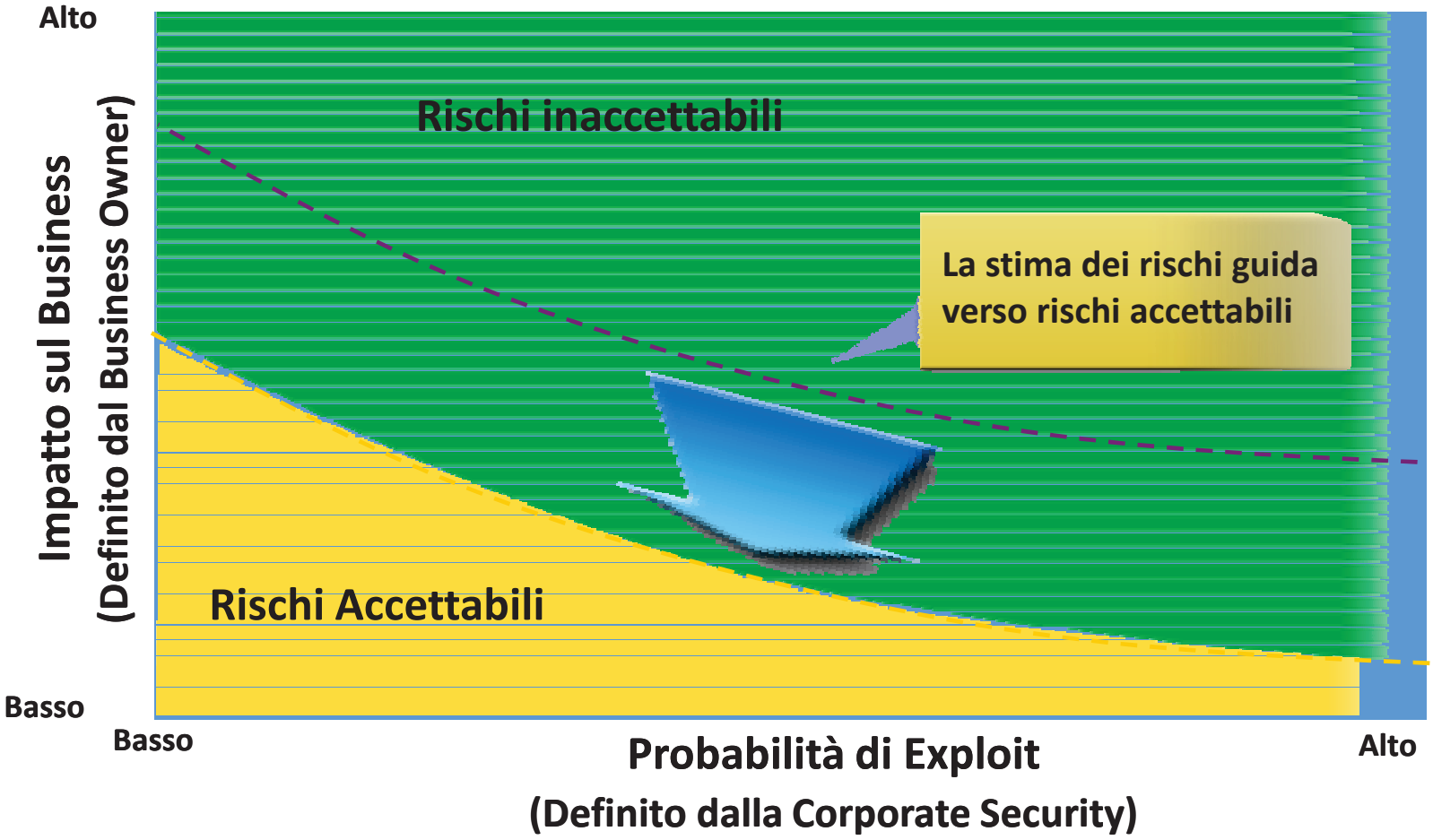
Zona trattegiata: casi anomali per i quali è stata prevista una contromisura

Rischio Residuo



Con un budget illimitato
e in un tempo illimitato,
si può costruire un
"*Security Environment* "
quasi perfetto.
Ma quello che serve è
un Security Environment
appropriato ed adeguato,
comprendente strumenti e
procedure di gestione
del **rischio residuo**

Implementazione delle Politiche di Sicurezza



GRAZIE