MISURE MINIME DI SICUREZZA ICT E TRATTAMENTO DATI

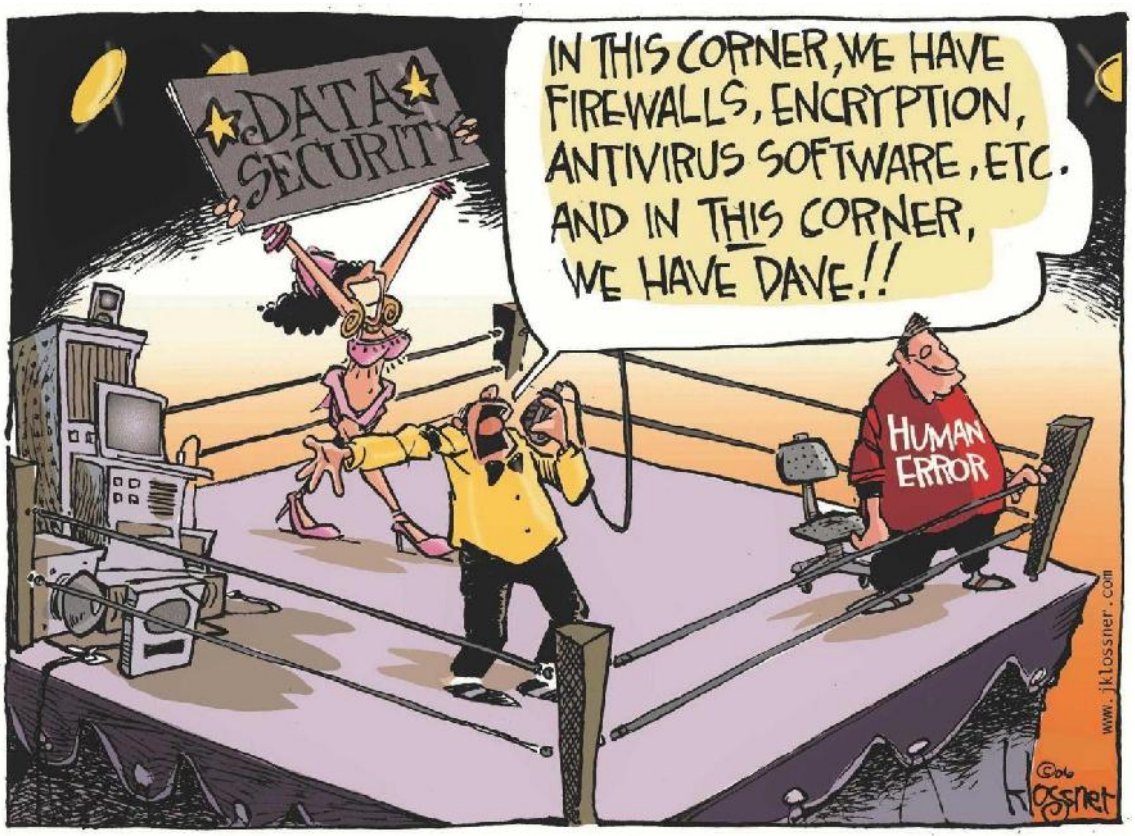
Implementare le misure minime di sicurezza ICT

Agenda

- Rischi, minacce e vulnerabilità in un mondo connesso: come difendersi?
- La sicurezza informatica in un Ente Pubblico
- Le misure minime di sicurezza ICT per le Pubbliche Amministrazioni

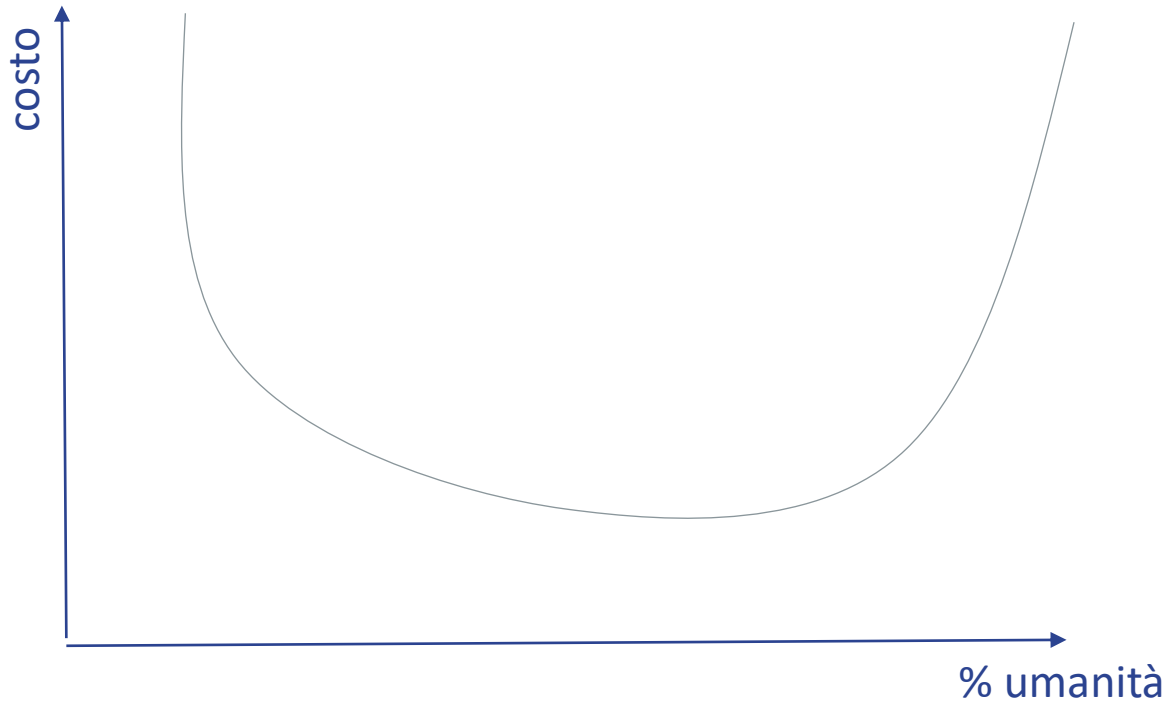
Quattro principi fondamentali

- “la sicurezza è un processo”
- “la sicurezza di una catena è pari a quella del suo anello più debole”
- “non si può gestire ciò che non si può misurare”
- “You Don’t Have To Be a Target To Become a Victim”



Il paradosso di Mayfield

Costa una quantità infinita di denaro sia aprire un sistema a tutti che chiuderlo a tutti



→ La sicurezza è sempre un compromesso

Il rischio nel GDPR

- ***Articolo 25 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita***
  *1.Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei **rischi** aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento,…*

- ***Considerando 75***
  *I **rischi** per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, …*

- ***Considerando 76***
  *La probabilità e la gravità del **rischio** per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.*

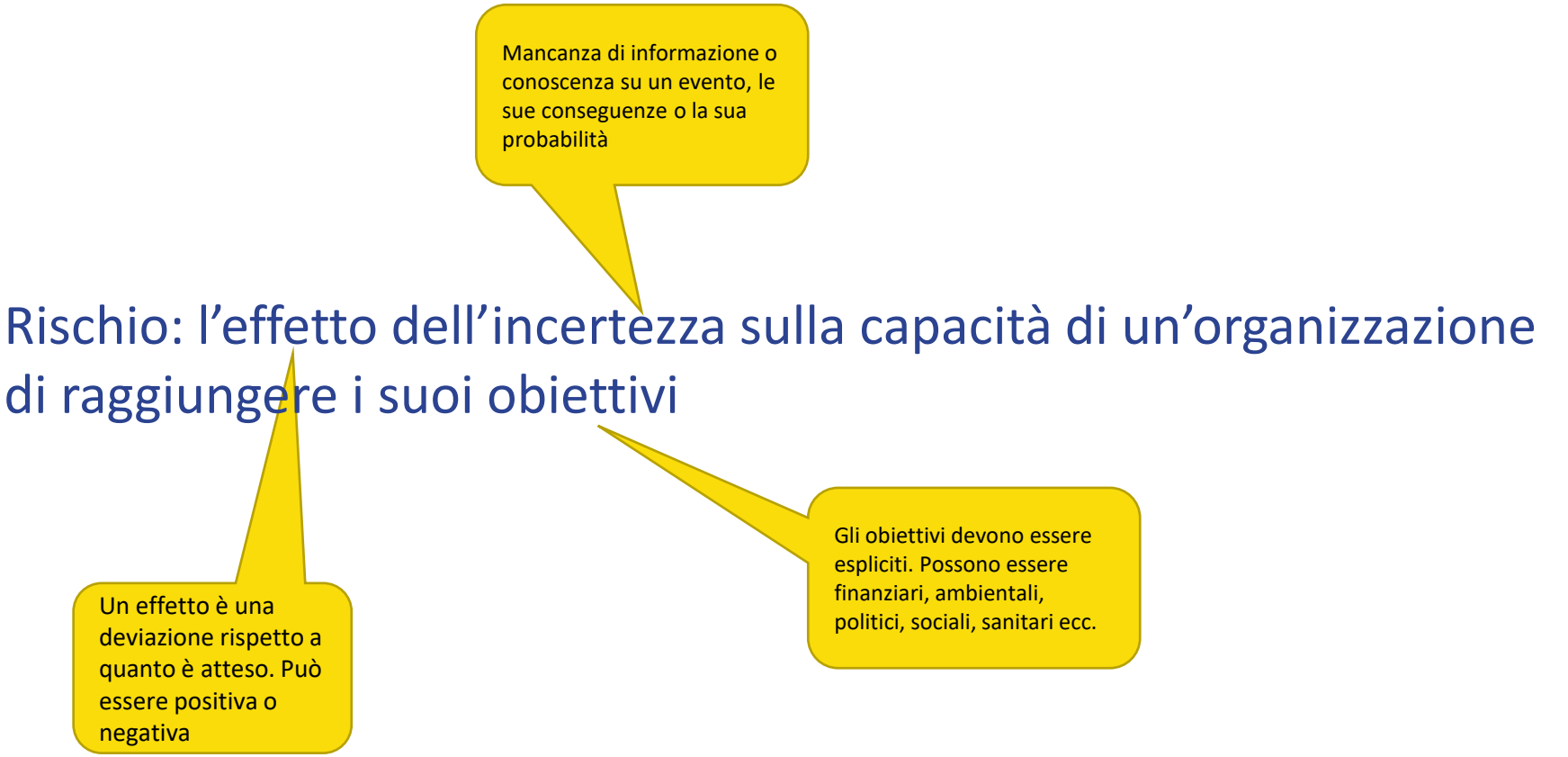
Il rischio nella Direttiva NIS

1. *Tanto gli OSE (Operatori di Servizi Essenziali) che gli FSD (Fornitori di Servizi Digitali):*

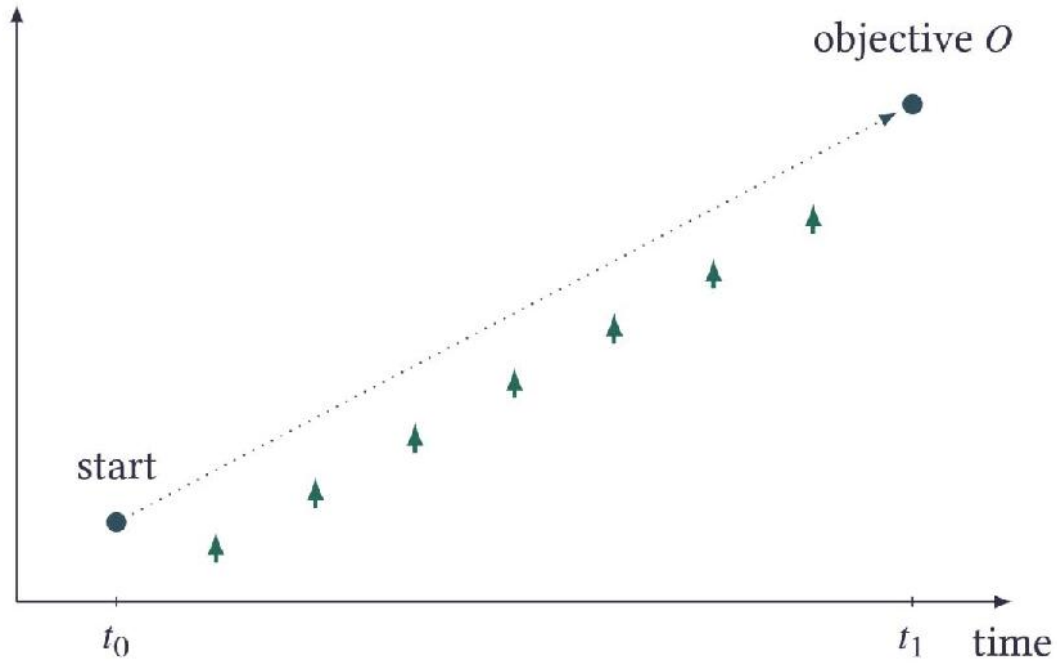
   - *sono chiamati ad adottare misure tecniche e organizzative adeguate e proporzionate alla **gestione dei rischi** e a prevenire e minimizzare l'impatto degli incidenti a carico della sicurezza delle reti e dei sistemi informativi, al fine di assicurare la continuità del servizio*

   - *hanno l'obbligo di notificare, senza ingiustificato ritardo, gli incidenti che hanno un impatto rilevante, rispettivamente sulla continuità e sulla fornitura del servizio, al Computer Security Incident Response Team (CSIRT) italiano, informandone anche l'Autorità*

Il Rischio


Mancanza di informazione o conoscenza su un evento, le sue conseguenze o la sua probabilità
Rischio: l'effetto dell'incertezza sulla capacità di un'organizzazione di raggiungere i suoi obiettivi
Un effetto è una deviazione rispetto a quanto è atteso. Può essere positiva o negativa
Gli obiettivi devono essere espliciti. Possono essere finanziari, ambientali, politici, sociali, sanitari ecc.

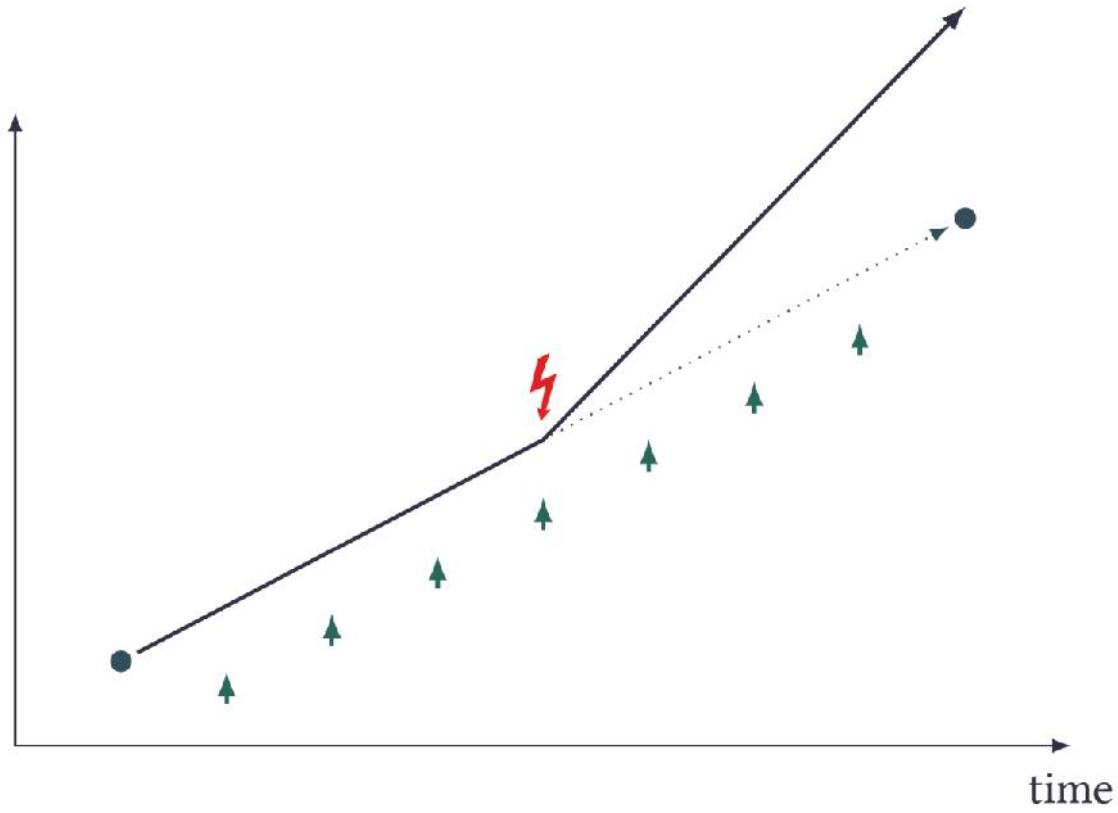
Il Rischio



L'organizzazione stabilisce i suoi obiettivi: al tempo t1 vuole essere nel punto O.

Per fare questo, stabilisce un Piano d'Azione per spostarsi dalla posizione corrente fino al punto O.

Il Rischio

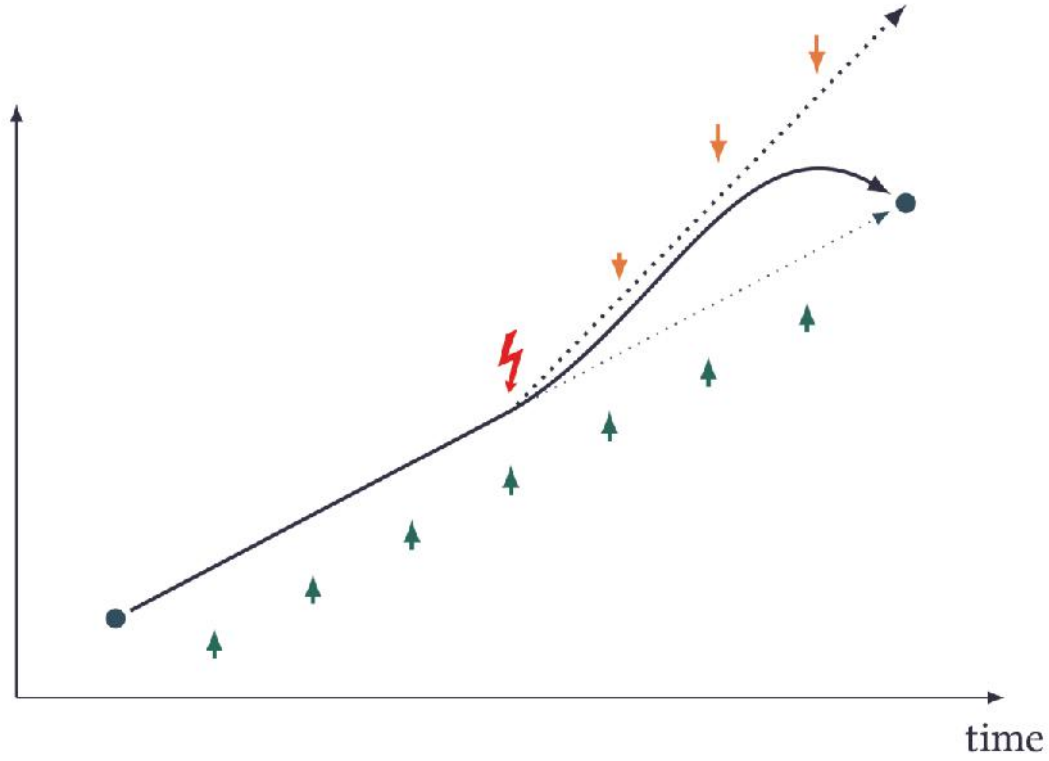


La presenza di incertezza significa che delle perturbazioni inattese possono causare deviazioni dal piano definito al tempo t0.

Se non vengono gestite l'organizzazione non raggiungerà il suo obiettivo.

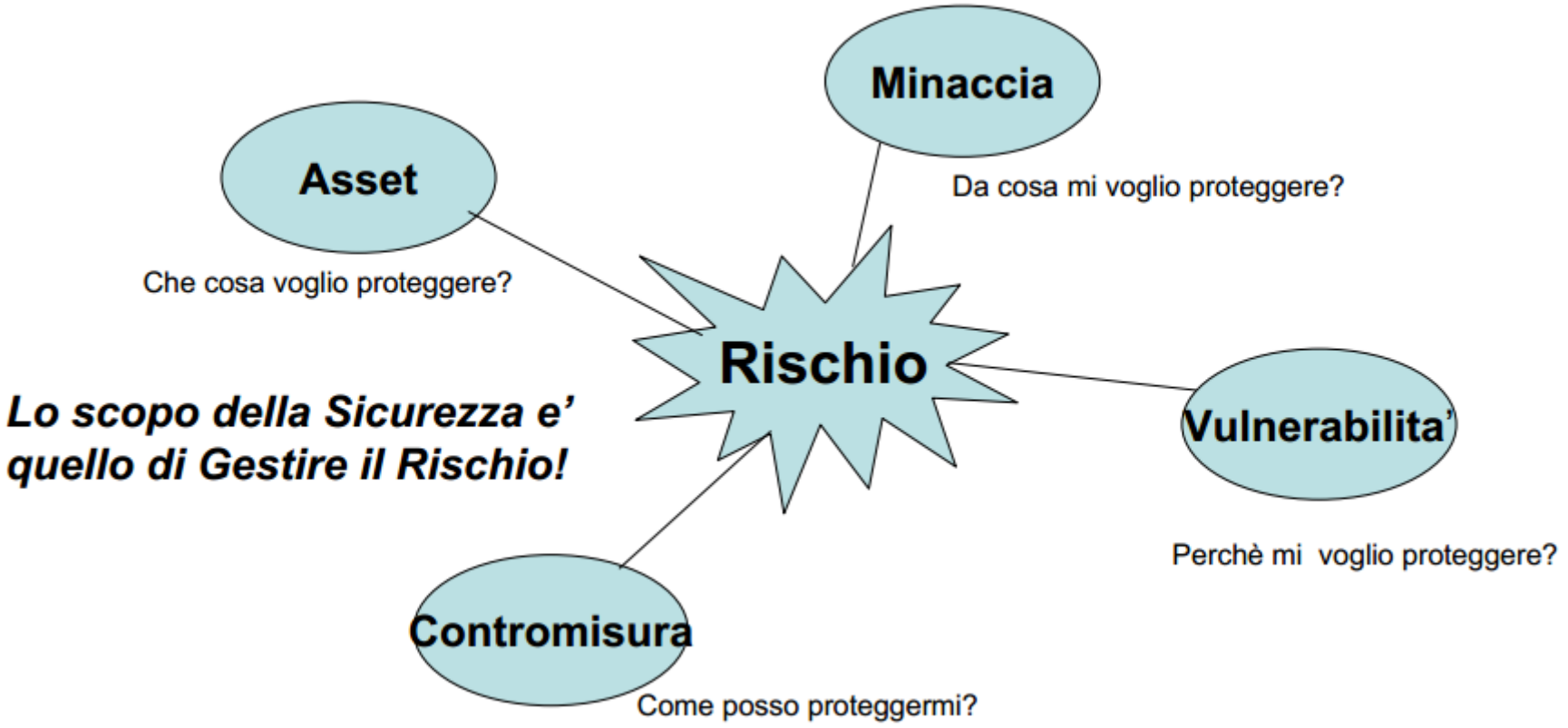
Questo è il Rischio, l'effetto dell'incertezza sulla possibilità di raggiungere gli obiettivi.

Il Rischio



Gestire il Rischio significa cercare di anticipare e far attenzione alle deviazioni dal piano e implementare opportune **misure correttive** affinché l'obiettivo sia comunque raggiunto.

Cos’è la sicurezza?

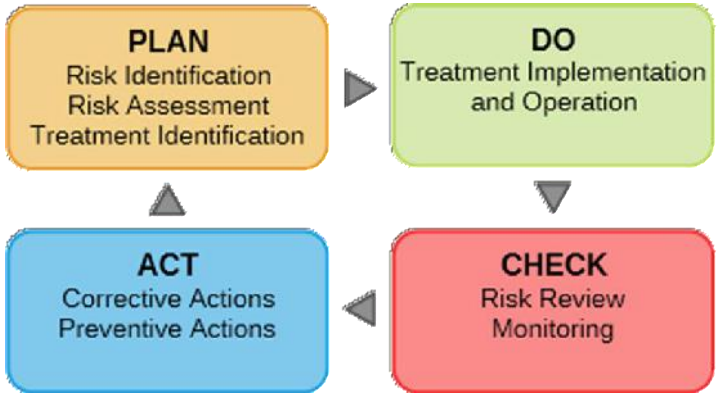


Lo scopo della Sicurezza e’ quello di Gestire il Rischio!

Gestire il Rischio

Il Risk Management si compone di quattro fasi:

- **Identificazione** in questa fase si cerca di determinare le possibili fonti di Rischio e individuare quegli eventi che potrebbe causare l'insorgere di Pericoli
- **Valutazione qualitativa e quantitativa** consiste nel determinare impatto e probabilità di un Pericolo e nell'assegnare, in modo qualitativo o quantitativo, un ordine di priorità (o, se si preferisce, un indice di pericolosità) dei Rischi
- **Pianificazione** in questa fase si passa a identificare l'insieme delle contromisure applicabili ad un certo rischio. Si fa l'analisi costi/benefici di ognuna di esse e si passa a selezionare quelle da applicare
- **Controllo** anche dopo che sono state poste in essere le contromisure, bisogna continuare a monitorare i rischi per capire se le contromisure stanno effettivamente funzionando e valutare l'insorgere di nuovi rischi

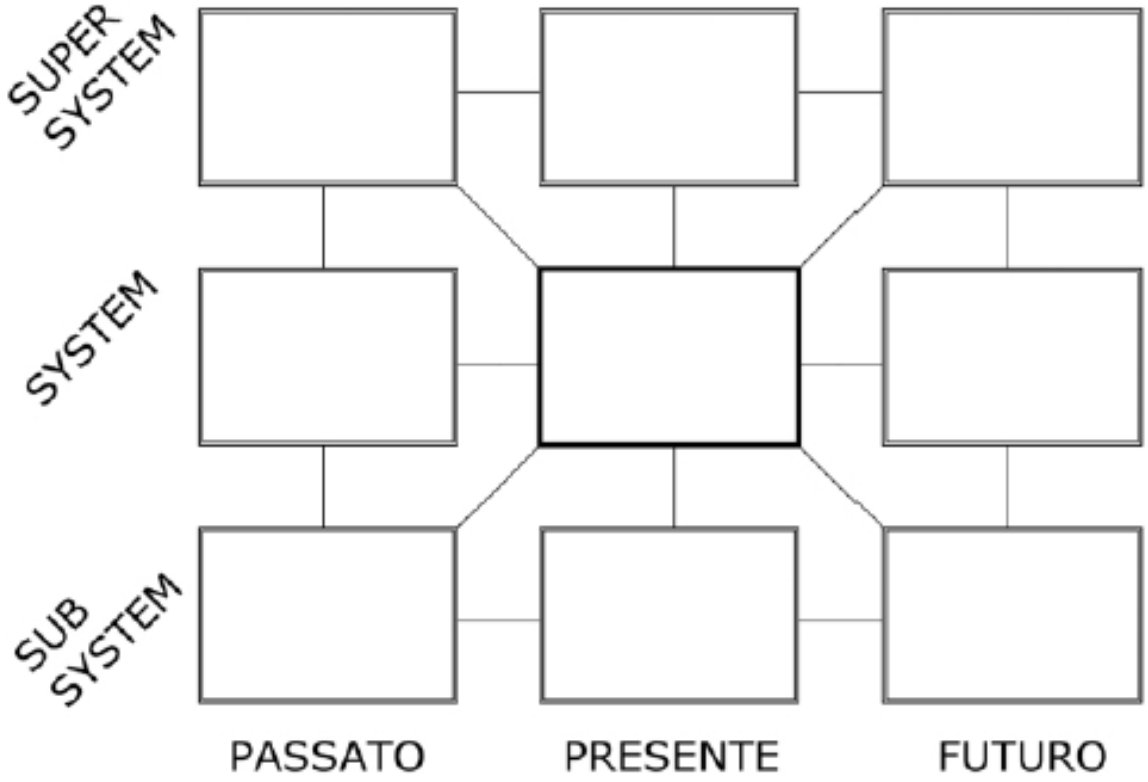


L'output di ognuna delle 4 fasi confluisce nel Piano del Rischio (Risk Plan) complessivo.

Le domande da porsi

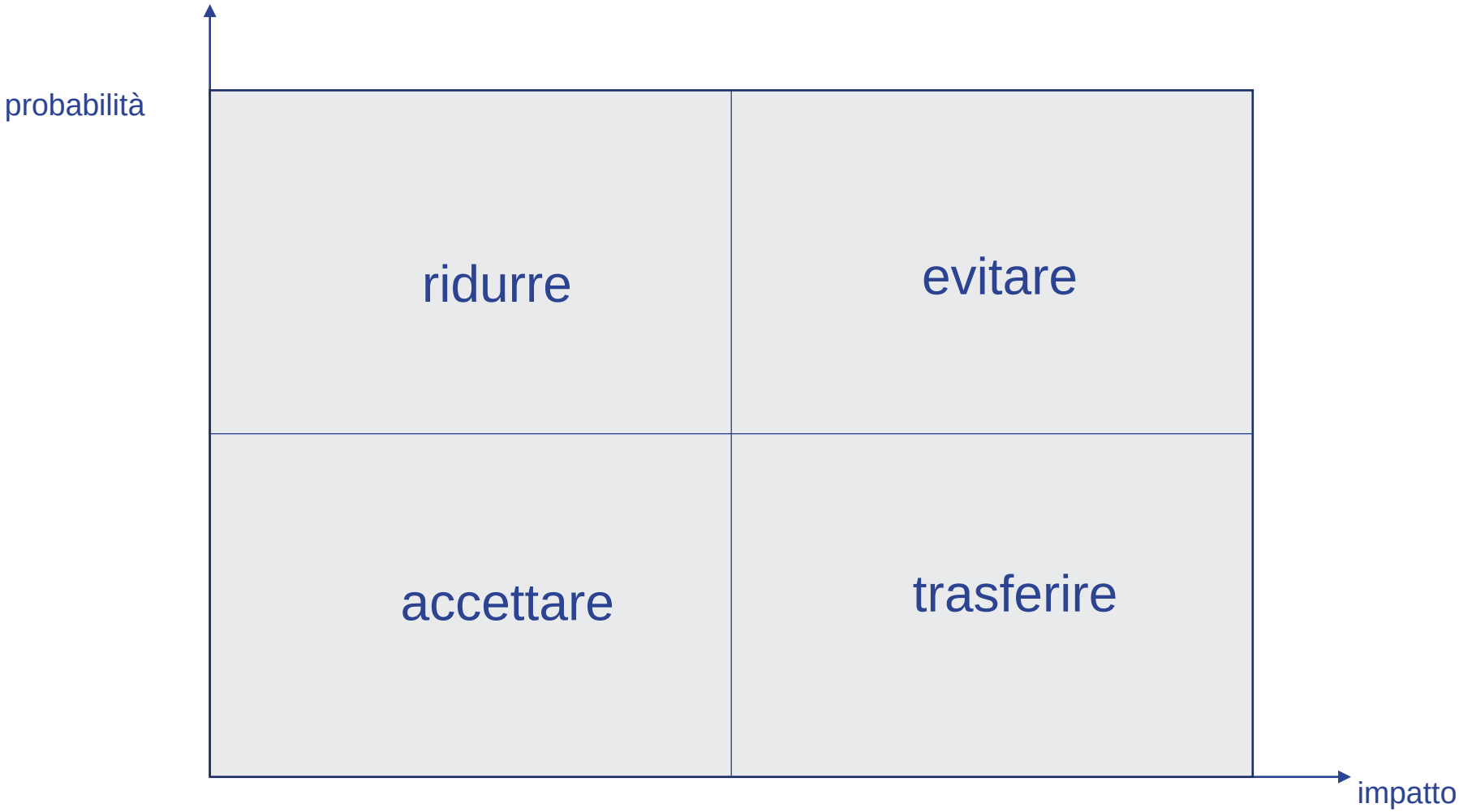
- Cosa potrebbe andare storto?
- Ci sono funzionalità nascoste nel Sistema?
- Ci sono modi alternativi (indesiderati) con cui il Sistema può funzionare?
- Come posso far sì che il Sistema si comporti in modo diverso da come dovrebbe?

Un utile strumento mentale



Identificazione dei rischi

- Risk 1: Perdita di riservatezza (ad es. consultazione di un documento fatta da una persona senza i diritti per farlo)
- Risk 2: Perdita di integrità (ad es. modifica di un dato fatta da una persona senza i diritti per farlo)
- Risk 3: mancanza di tracciabilità (chi ha richiesto cosa e chi ha materialmente compiuto l'azione)
- Risk 4: Impersonamento
- Risk 5: Perdita di disponibilità (ad es. un dato non più accessibile, un servizio non funzionante ecc.)
- Risk 6: incapacità di ricondurre un'azione a data e ora certe
- Risk 7: …..


probabilità
ridurre
evitare
accettare
trasferire
impatto

Il calcolo del rischio

Il Rischio viene solitamente definito e calcolato come prodotto dei fattori:

R = P x I x E

dove:

P = probabilita' (della minaccia) (alta per minacce molto probabili)

I = impatto (gravita' del danno / dell'effetto) (alto per danni consistenti)

E = efficacia (dei controlli) (alto per controlli poco efficaci)

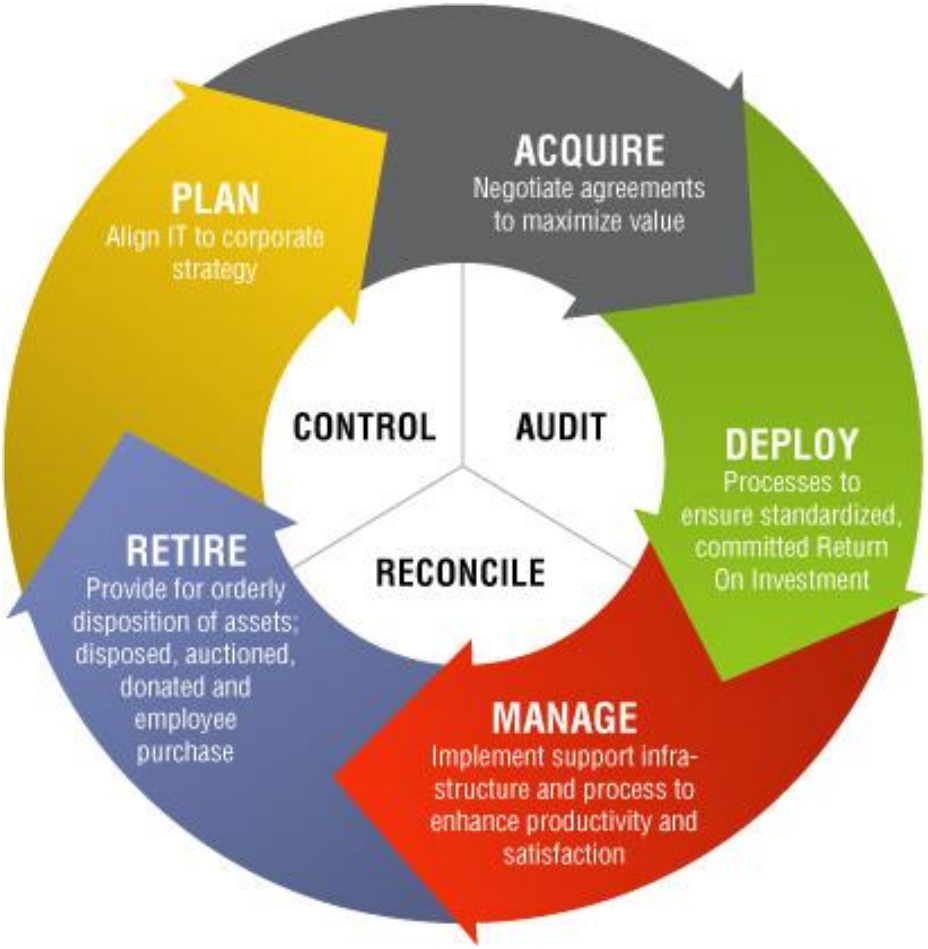
In pratica il rischio viene definito come la probabilità che una minaccia sfrutti una vulnerabilità per generare un impatto nocivo (senza che esista una contromisura che lo impedisca).

10	500000	50.0	500.0	500.0	1500.0	1500.0	1500.0	10000.0	10000.0	50000.0	50000.0
9	100000	10.0	100.0	100.0	300.0	300.0	300.0	2000.0	2000.0	10000.0	10000.0
8	30000	3.0	30.0	30.0	90.0	90.0	90.0	600.0	600.0	3000.0	3000.0
7	10000	1.0	10.0	10.0	30.0	30.0	30.0	200.0	200.0	1000.0	1000.0
6	5000	0.5	5.0	5.0	15.0	15.0	15.0	100.0	100.0	500.0	500.0
5	2000	0.2	2.0	2.0	6.0	6.0	6.0	40.0	40.0	200.0	200.0
4	500	0.0	0.5	0.5	1.5	1.5	1.5	10.0	10.0	50.0	50.0
3	100	0.0	0.1	0.1	0.3	0.3	0.3	2.0	2.0	10.0	10.0
2	10	0.0	0.0	0.0	0.0	0.0	0.0	0.2	0.2	1.0	1.0
1	1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1	0.1
O/D		99.99%	99.90%	99.90%	99.70%	99.70%	99.70%	98.00%	98.00%	90.00%	90.00%
		1	2	3	4	5	6	7	8	9	10

Source: Fraunhofer IPA

Gli asset

"An asset is an item, thing or entity that has potential or actual value to an organization" (ISO 55000)



Asset: A capability or resource that is used in the delivery of a service. Also called service asset. There are many types of assets, including management assets, organization assets, process assets, knowledge assets, people assets, information assets, application assets, infrastructure assets, and financial assets.

Asset management

Systematic and coordinated activities and practices through which an organization optimally and sustainably manages its assets and asset systems, their associated performance, risks and expenditures over their life cycles for the purpose of achieving its organizational strategic plan

Change management

Una ***Change Request*** (CR) o anche **Request for Change** (RFC) è un documento di dettaglio in cui si richiede una modifica alle specifiche.

La RFC viene, generalmente, presentata con alcuni attributi, come la priorità e un tipo o categoria, ad es. richiesta di modifica software, hardware, architetturale e così via.

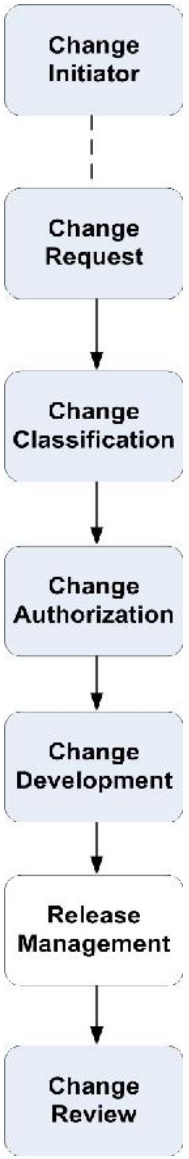
La RFC, corredata di un'analisi di impatto sul sistema e di uno studio di fattibilità, viene sottoposta a un **Change Manager**, che la discute di concerto con la **Change Advisory Board**, per l'approvazione.

La modifica, a questo punto, se approvata, deve essere schedulata per la messa in opera.

Dopo ciò, il sistema, ormai dotato del cambiamento richiesto, deve essere monitorato per verificare un eventuale impatto negativo nell'ambiente in esercizio con un conseguente rollback della modifica effettuata.

Le figure coinvolte nel processo di change management sono:

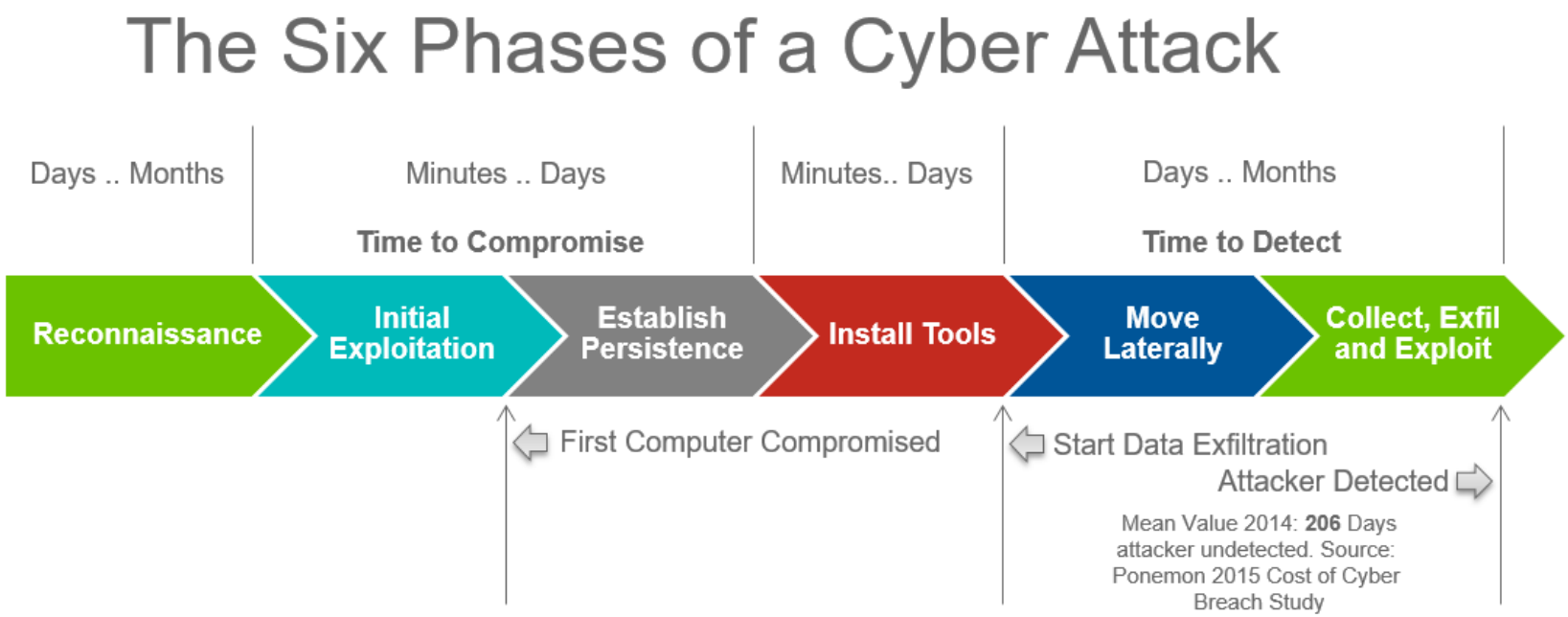
- il ***Change Initiator***, colui che inserisce la RFC
- il ***Change Manager***, che gestisce le attività di change management e riunisce e prepara il lavoro per la CAB
- il ***Change Advisory Board*** **(CAB),** che è un gruppo di persone coinvolte nell'ambito IT operations e che valuta, approva e rifiuta una RFC
- il ***Change Owner***, è nominato dal Change Manager ed ha la responsabilità operativa del cambiamento



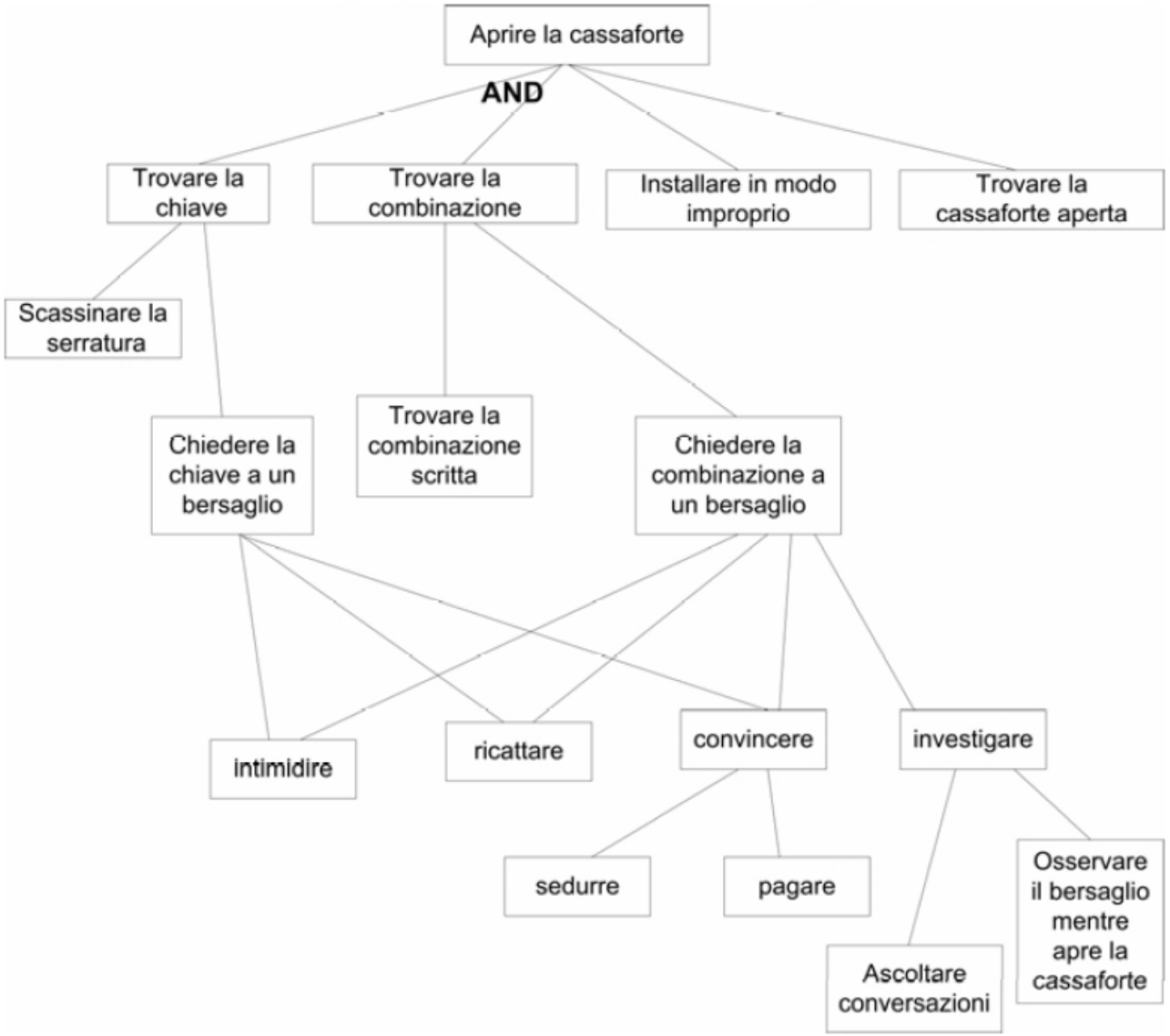
Le minacce

https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

Le minacce


The Six Phases of a Cyber Attack
Days .. Months
Minutes .. Days
Minutes.. Days
Days .. Months
Time to Compromise
Time to Detect
Reconnaissance
Initial Exploitation
Establish Persistence
Install Tools
Move Laterally
Collect, Exfil and Exploit
First Computer Compromised
Start Data Exfiltration
Attacker Detected
Mean Value 2014: 206 Days attacker undetected. Source: Ponemon 2015 Cost of Cyber Breach Study

Un utile strumento: gli attack tree



Le vulnerabilità

Una vulnerabilità è

una debolezza in un asset che un Threat Agent può impiegare per modificare a suo vantaggio la posizione di sicurezza dell'asset, con impatto sugli attributi che ne costituiscono il valore, come la riservatezza, l'integrità, la disponibilità ecc.

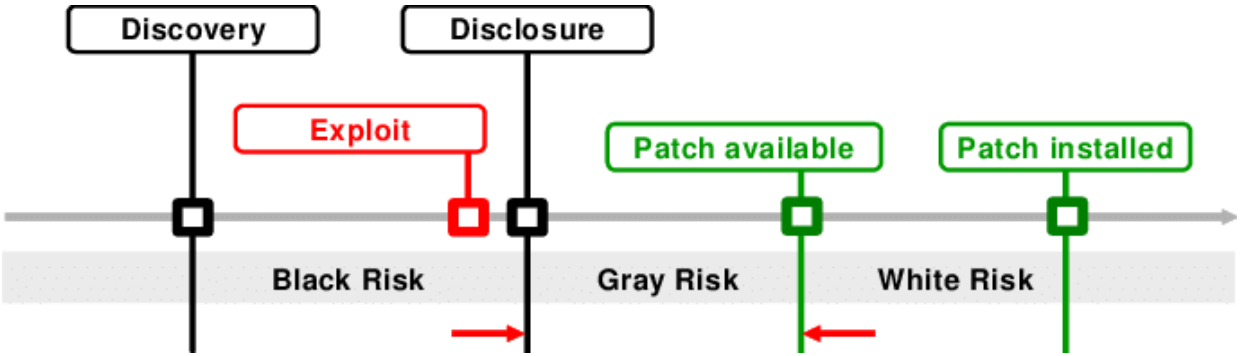
Le vulnerabilità possono essere di tre tipi:

- **Amministrative** - sono relative alle policies e alle procedure di sicurezza
- **Fisiche** - sono le vulnerabilità relative alle persone, ai luoghi geografici e agli apparati fisici
- **Tecniche** - sono relative all'aspetto tecnologico, cioè errori di configurazione di apparati, backdoor, password deboli ecc.

Il **potenziale d'attacco** rappresenta la "barriera" che un attaccante deve superare per poter sfruttare una vulnerabilità.
Esso dipende tipicamente da alcuni fattori come:

- Il Tempo necessario per sfruttare la vulnerabilità
- L'Equipaggiamento necessario
- Le Capacità necessarie dell'attaccante
- La Conoscenza del sistema
- L'Accesso al sistema

Le vulnerabilità



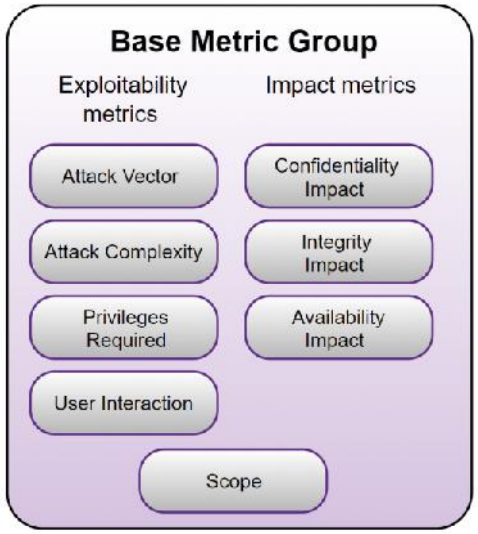
La disclosure è fatta ad opera di quelli che vengono chiamati **Security Information Providers** quali:

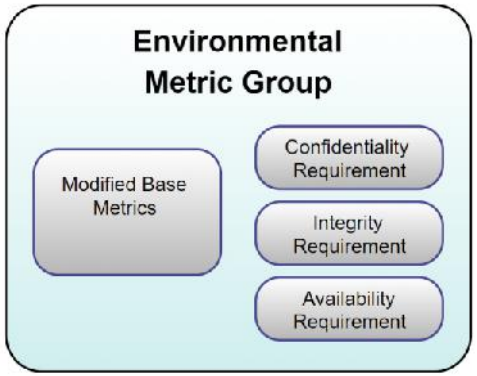
- **CERT** (Computer Emergency Response Team, USA) https://www.kb.cert.org/vuls/
- **NIST** (National Institute of Standards and technology) https://nvd.nist.gov/
- **Securityfocus** (Symantec, USA) https://www.securityfocus.com
- **Mitre** (Mitre, USA) cve.mitre.org
- **NVD** https://nvd.nist.gov/vuln

1. La vulnerabilità viene scoperta (discovery)
2. Il primo exploit viene rilasciato
3. Il grande pubblico viene a conoscenza della vulnerabilità (disclosure)
4. Viene sviluppata la patch che chiude la vulnerabilità

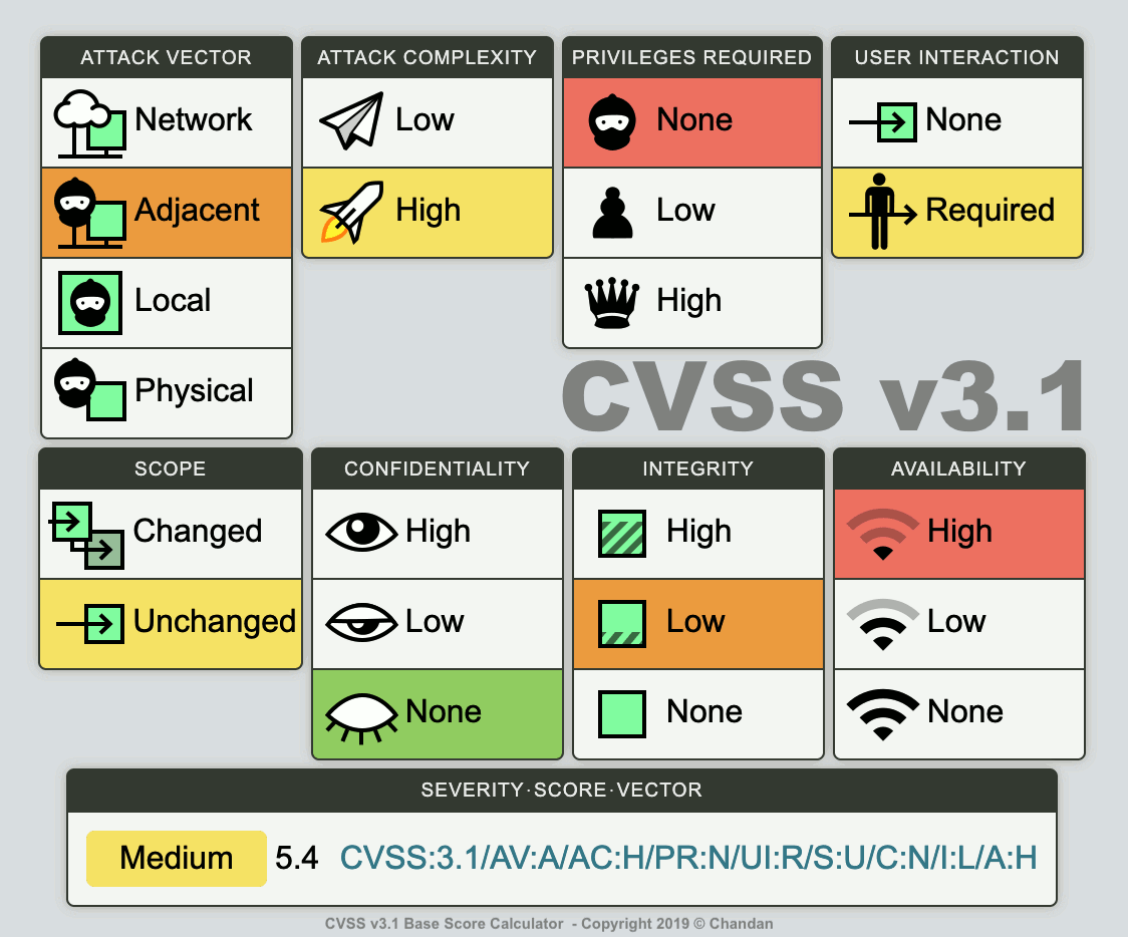
Le metriche delle vulnerabilità

CVSS è nato come linguaggio universale per indicare la severità di una vulnerabilità e aiutare a determinare l'urgenza e la priorità della risposta.
Il punteggio **Base** rappresenta la severità della vulnerabilità, il punteggio **Temporale** la sua urgenza, il punteggio **Ambientale** la priorità nella risposta entro l'ambiente dell'utente finale.





Il punteggio base



https://www.first.org/cvss/calculator/3.1

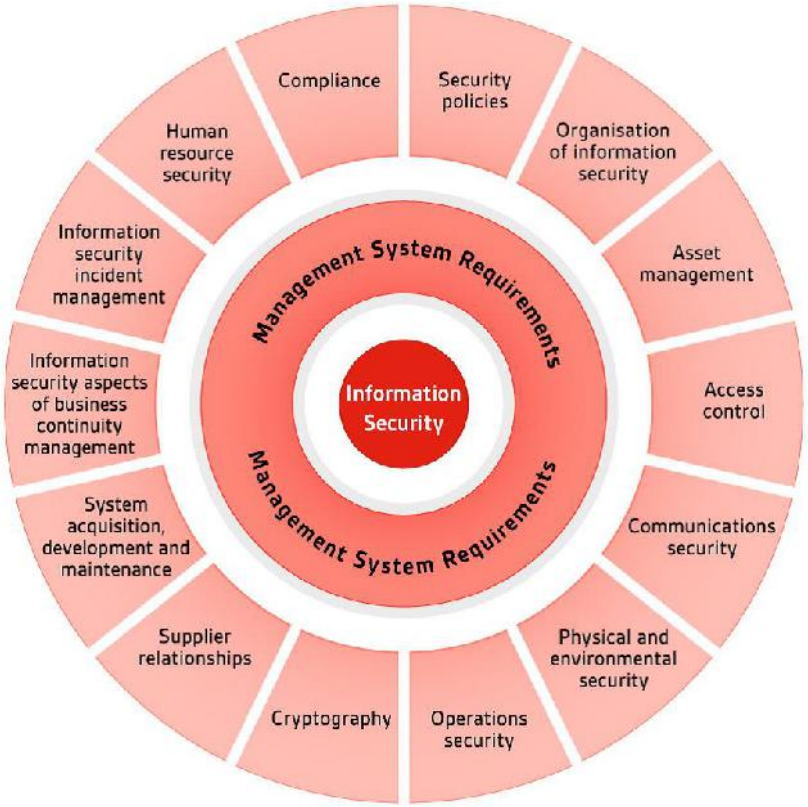
Le contromisure

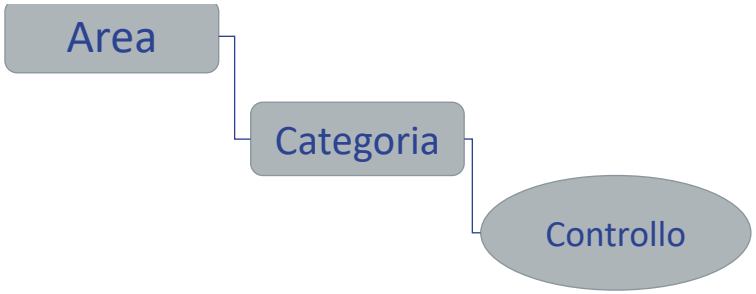
- ISO 27001 (114 controlli suddivisi in 14 aree)
- SANS 20
- Misure minime
- OWASP Proactive Controls
- ….

La struttura di ISO 27001

- Ciascuna delle **14 aree** include una o più categorie per un totale di **35 diverse categorie** (la versione 2005 39)

- Ogni categoria ha un **obiettivo** associato, che dichiara ciò che si vuole raggiungere. L'obiettivo, viene raggiunto attraverso l'implementazione di uno o più controlli. In totale ci sono **114 controlli** (la versione 2005 133).





La gestione degli asset secondo ISO 27001

- ***Categoria***: Responsabilità per gli asset
  - ***Obiettivo*** : identificare gli asset dell'organizzazione e definire adeguate responsabilità per la loro protezione
  - ***Controlli***:
    1. **Inventario degli asset**– tutti gli asset associati alle informazioni e alle strutture di elaborazione delle informazioni devono essere identificati; un inventario di questi asset deve essere compilato e mantenuto aggiornato
    2. **Responsabilità degli asset** – gli asset censiti nell'inventario devono avere un responsabile
    3. **Utilizzo accettabile degli asset** – le regole per l'utilizzo accettabile delle informazioni e degli asset associate alle strutture di elaborazione delle informazioni devono essere identificate, documentate e attuate
    4. **Restituzione degli asset** – tutto il personale e gli utenti di parti esterne devono restituire gli asset dell'organizzazione in loro possesso al termine del periodo di impiego, del contratto o dell'accordo stipulato

La gestione degli asset secondo ISO 27001

Categoria: Classificazione delle informazioni

Obiettivo : assicurare che le informazioni ricevano un adeguato livello di protezione, in linea con la loro importanza per l'organizzazione

Controlli:

1. **Classificazione delle informazioni**– le informazioni devono essere classificate in relazione al loro valore, ai requisiti cogenti e alla criticità in caso di divulgazione o modifica non autorizzate
2. **Etichettatura delle informazioni**– deve essere sviluppato e attuato un appropriato insieme di procedure per l'etichettatura delle informazioni in base allo schema di classificazione adottato dall'organizzazione
3. **Trattamento degli asset** – deve essere sviluppato e attuato un insieme di procedure per il trattamento degli asset in base allo schema di classificazione adottato dall'organizzazione

La gestione degli asset secondo ISO 27001

- ***Categoria***: Trattamento dei supporti
  - ***Obiettivo*** : prevenire la divulgazione non autorizzata, la modifica, la rimozione o la distruzione delle informazioni archiviate sui supporti
  - ***Controlli***:
    1. **Gestione dei supporti rimovibili**– devono essere sviluppate procedure per il trattamento dei supporti rimovibili in base allo schema di classificazione adottato dall'organizzazione
    2. **Dismissione dei supporti**– la dismissione dei supporti non più necessari deve avvenire in modo sicuro, attraverso l'utilizzo di procedure formali
    3. **Trasporto dei supporti fisici**– I supporti che contengono informazioni devono essere protetti da accessi non autorizzati, utilizzi impropri o manomissioni durante il trasporto

Le misure minime di sicurezza

- ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI
- ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI
- ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER
- ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ
- ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE
- ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE
- ABSC 10 (CSC 10): COPIE DI SICUREZZA
- ABSC 13 (CSC 13): PROTEZIONE DEI DATI

- https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict
- Circolare AGID **18 aprile 2017, n. 2/2017 (pubblicata in G.U.** Serie Generale n.103 del 05-05-2017)

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	
1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	
1	4	3	A	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	
1	5	1	A	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	
2	2	1	S	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.	
2	2	2	S	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).	
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	
2	3	2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	
2	3	3	A	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	
3	1	2	S	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.	
3	1	3	A	Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco.	
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	
3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	
3	5	2	A	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.	
3	5	3	A	Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.	
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	

Analisi di uno use case

era stata fatta un'adeguata analisi dei rischi (Risposta: evidentemente no!)? Un progetto di 90 milioni di dollari dovrebbe averla	ABSC 4.8.1	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).
era necessario che il tecnico dovesse avere privilegi così elevati da poter distruggere tutto?	ABSC 5.1.3	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.
il tecnico era stato adeguatamente formato?	ABSC 5.1.1	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.
non si facevano backup?	ABSC 10.1.1	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.
il computer del direttore tecnico di casa era sufficientemente protetto da evitare rischi di esfiltrazione di dati o di inclusione di malware (che poi avrebbero potuto essere portati in azienda)?	ABSC 2.3.1	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.
	ABSC 2.4.1	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.
	ABSC 3.1.1	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.
	ABSC 3.1.2	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.
	ABSC 4.5.1	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.
	ABSC 8.1.1	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.
	ABSC 8.1.2	Installare su tutti i dispositivi firewall ed IPS personali.
avranno avuto un sistema di versioning per tenere traccia delle singole modifiche ed, eventualmente, fare rollback a un tempo definito?	ABSC 2.3.3	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.
	ABSC 3.2.3	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.
	ABSC 3.7.1	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.
	ABSC 3.5.3	Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.
se il tecnico avesse fatto lo gnorri era possibile risalire a lui (tracciabilità delle azioni)?	ABSC 5.1.2	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.
	ABSC 5.1.4	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.
	ABSC 5.10.2	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.
	ABSC 5.10.3	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.

La sicurezza dei servizi

- Costruire un catalogo dei servizi
- Valutare i rischi (es. tool di risk assessment AGID)
- Identificare i servizi critici
- Identificare le dipendenze fra i servizi
- Definire i livelli di servizio
- Monitorare i servizi