



NUOVI PERCORSI DI SVILUPPO  
DELLA CAPACITÀ AMMINISTRATIVA  
DELLA REGIONE SICILIANA



ASSESSORATO REGIONALE  
DELLE AUTONOMIE LOCALI E DELLA FUNZIONE PUBBLICA  
DIPARTIMENTO DELLE AUTONOMIE LOCALI

**Linea 2.5 "Rafforzamento della capacità di  
attuazione dei Fondi SIE da parte degli Enti Locali"**

**Ciclo "I Responsabili per la Transizione al Digitale e  
l'innovazione negli Enti Locali"**

**Webinar – 24 marzo 2021**

**La sicurezza informatica: proteggere il  
patrimonio informativo  
dell'Amministrazione**

**Alessandro Sinibaldi**



Unione Europea



Repubblica Italiana



Regione Siciliana

FSE FONDO SOCIALE EUROPEO  
**SICILIA 2020**  
PROGRAMMA OPERATIVO



Formez**PA**

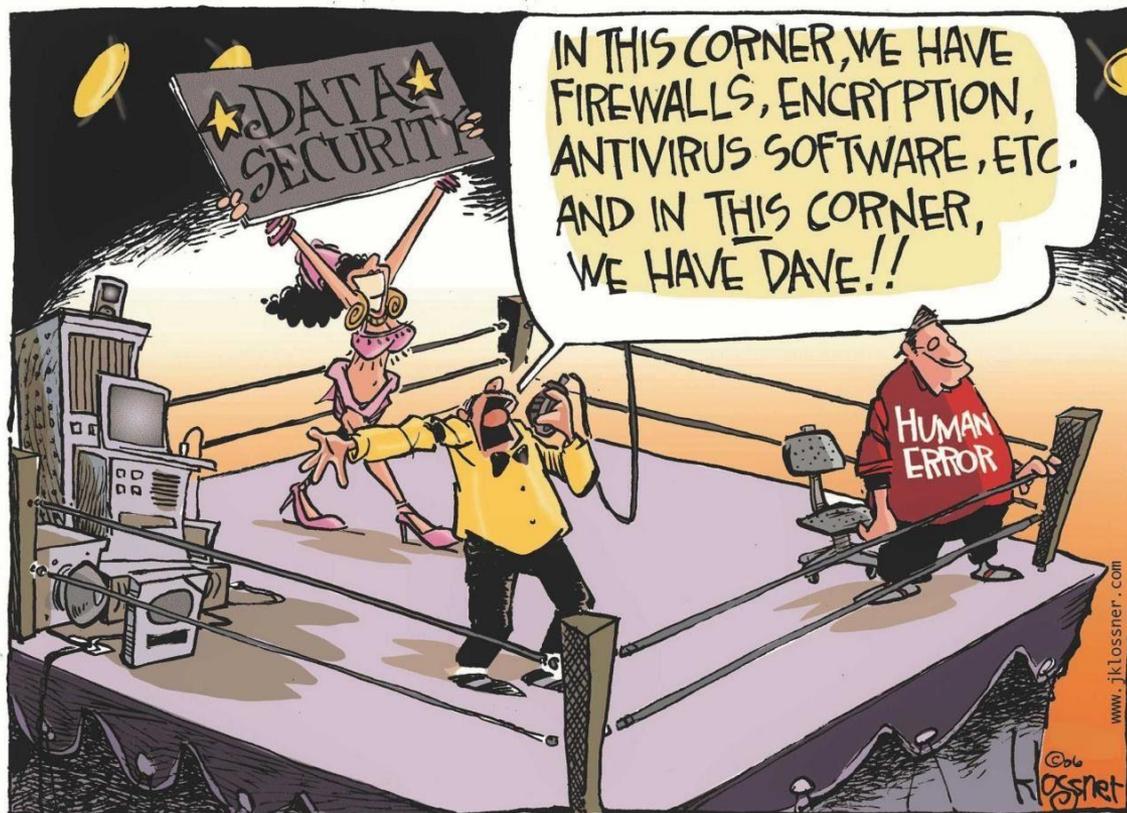
# Agenda

- 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



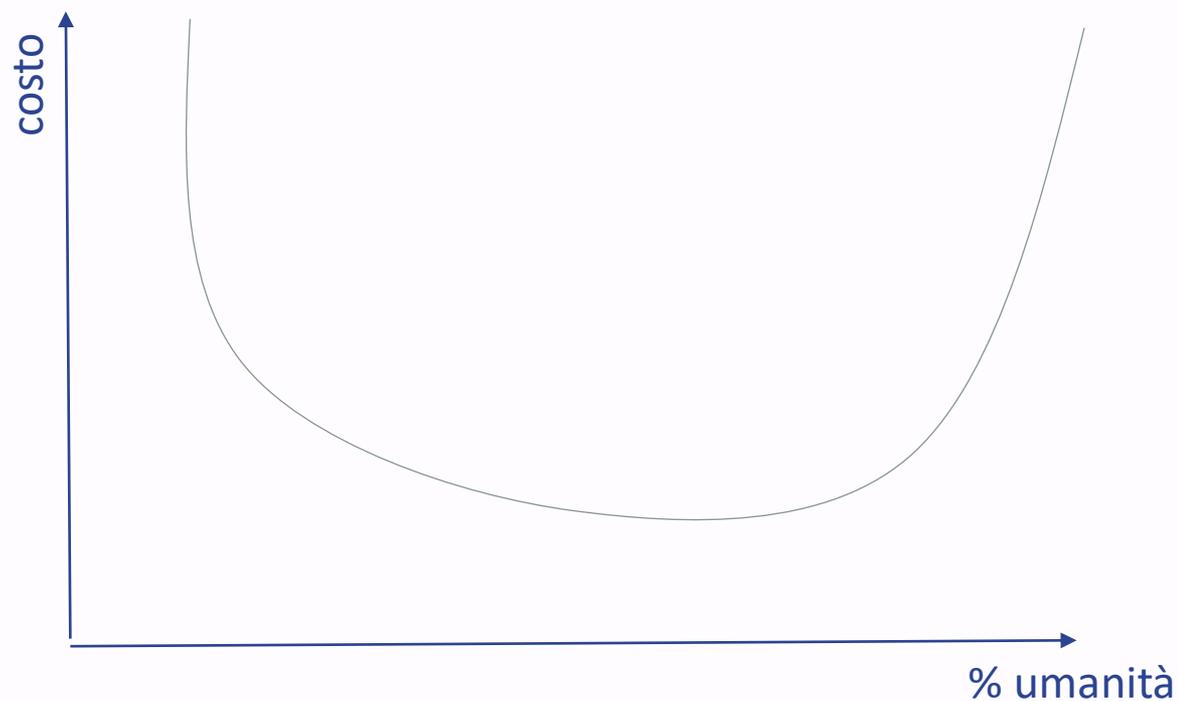
# Quattro principi fondamentali

- “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



NUOVI PERCORSI DI SVILUPPO  
DELLA CAPACITÀ AMMINISTRATIVA  
DELLA REGIONE SICILIANA

FormezPA

**Bezos: «Amazon fallirà. Il nostro compito è far sì che accada il più tardi possibile»**



# Dall'analisi del rischio al documento di visione: ecco il «metodo Cingolani» per la via italiana alla transizione ecologica

Intervenendo alla conferenza preparatoria per la revisione triennale della Strategia nazionale per lo sviluppo sostenibile, il neoministro tratteggia le sue priorità e indica la necessità di un documento di visione che potrà servire per le decisioni future

di Celestina Dominelli



dovranno essere affrontate. «Dobbiamo cominciare a guardare al futuro con un'ottica diversa che è quella della prevenzione - sottolinea ancora il titolare del nuovo ministero della Transizione ecologica -, serve l'analisi del rischio di tutto quello che facciamo. In vista del Recovery Plan, mi



# 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

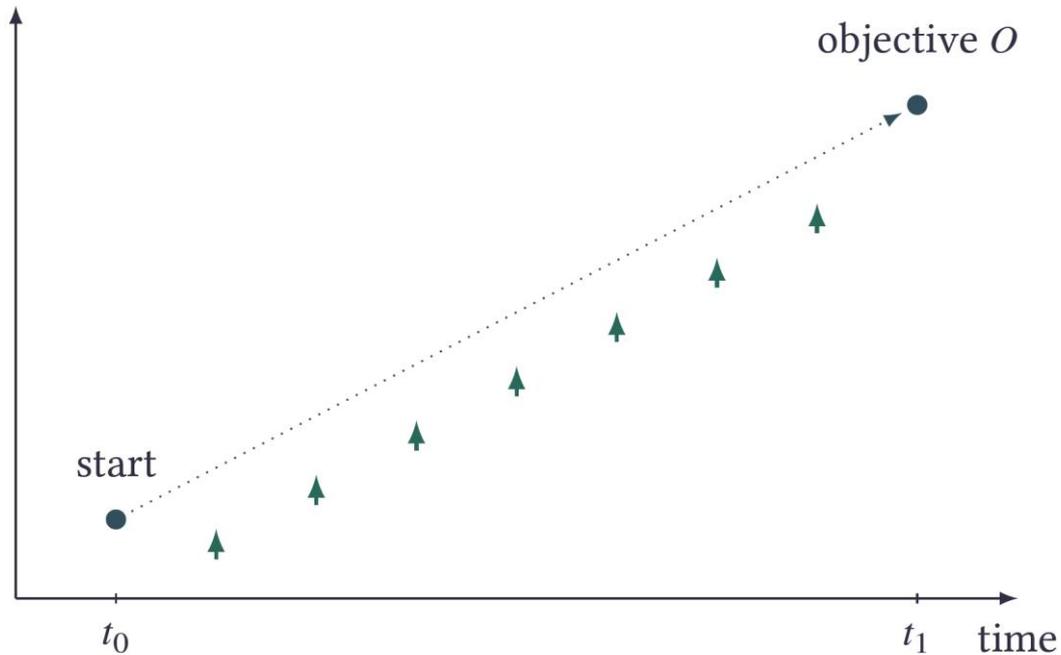
Rischio: l'effetto dell'incertezza sulla capacità di un'organizzazione di raggiungere i suoi obiettivi

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  $t_1$  vuole essere nel punto O.

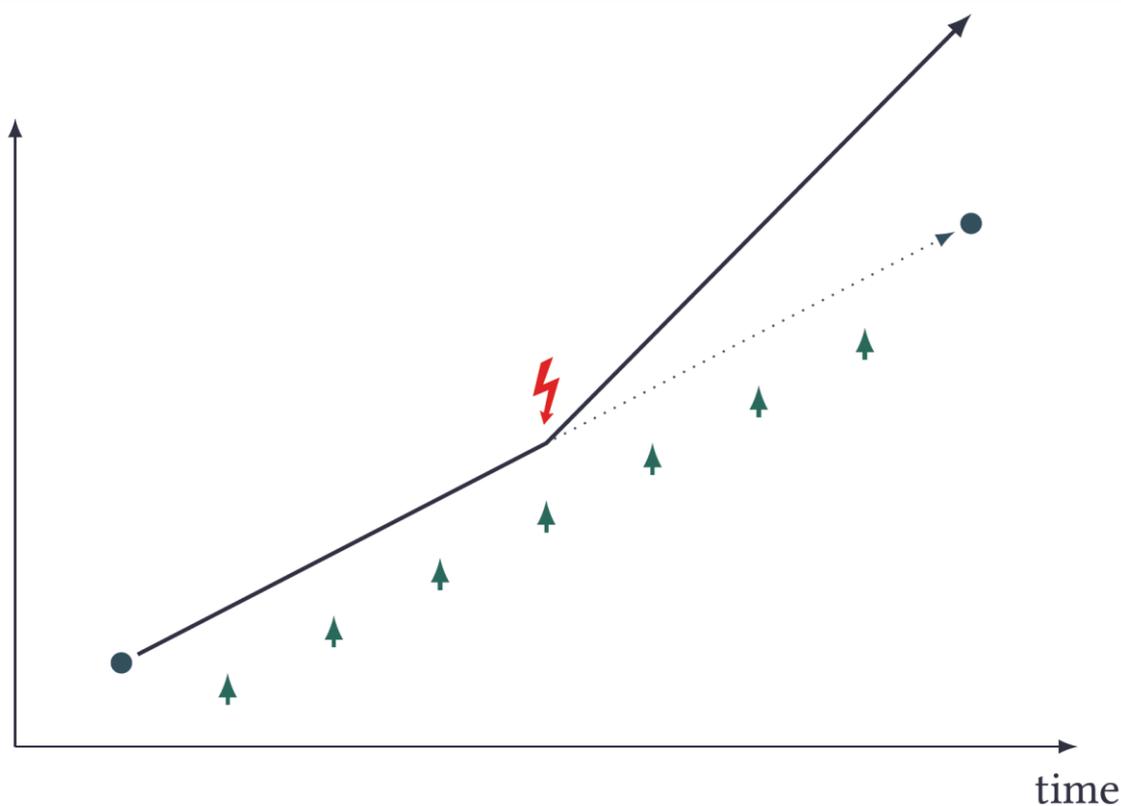
Per fare questo, stabilisce un Piano d'Azione per spostarsi dalla posizione corrente fino al punto O.



NUOVI PERCORSI DI SVILUPPO  
DELLA CAPACITÀ AMMINISTRATIVA  
DELLA REGIONE SICILIANA

FormezPA

# Il Rischio



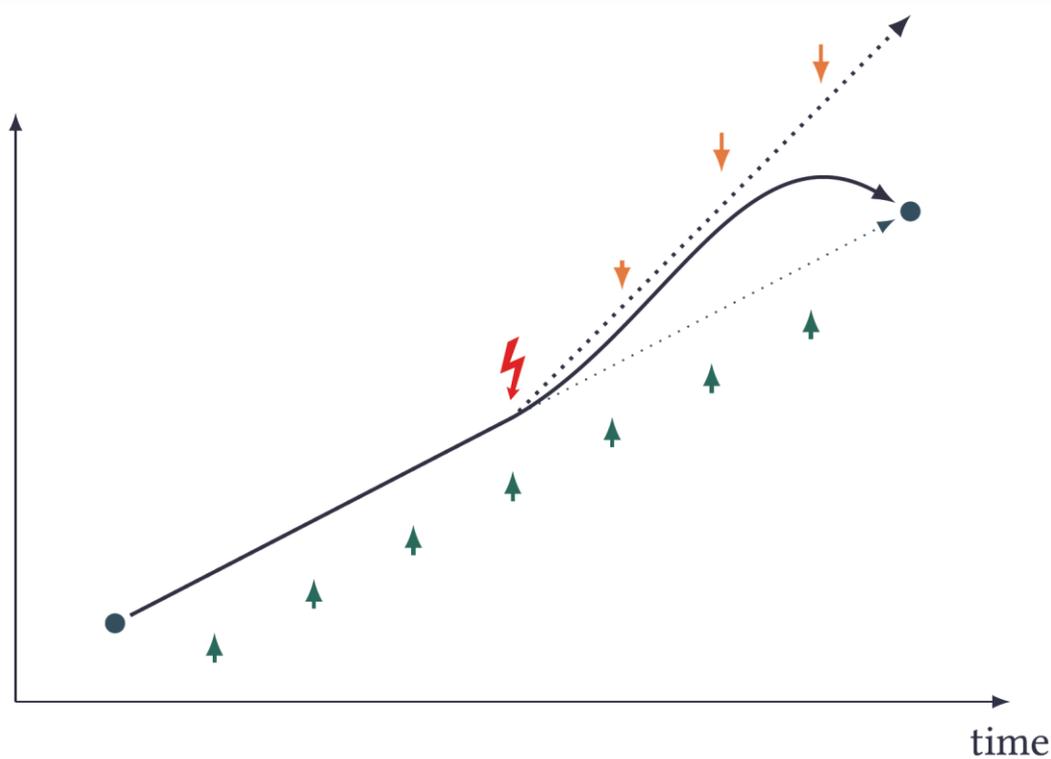
La presenza di incertezza significa che delle perturbazioni inattese possono causare deviazioni dal piano definito al tempo  $t_0$ .

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?

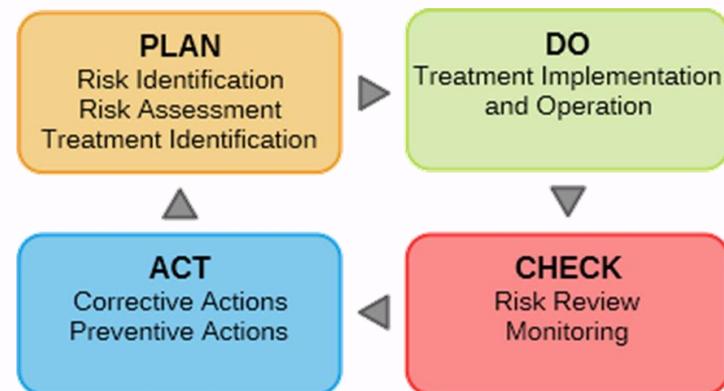


# Gestire il Rischio

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.

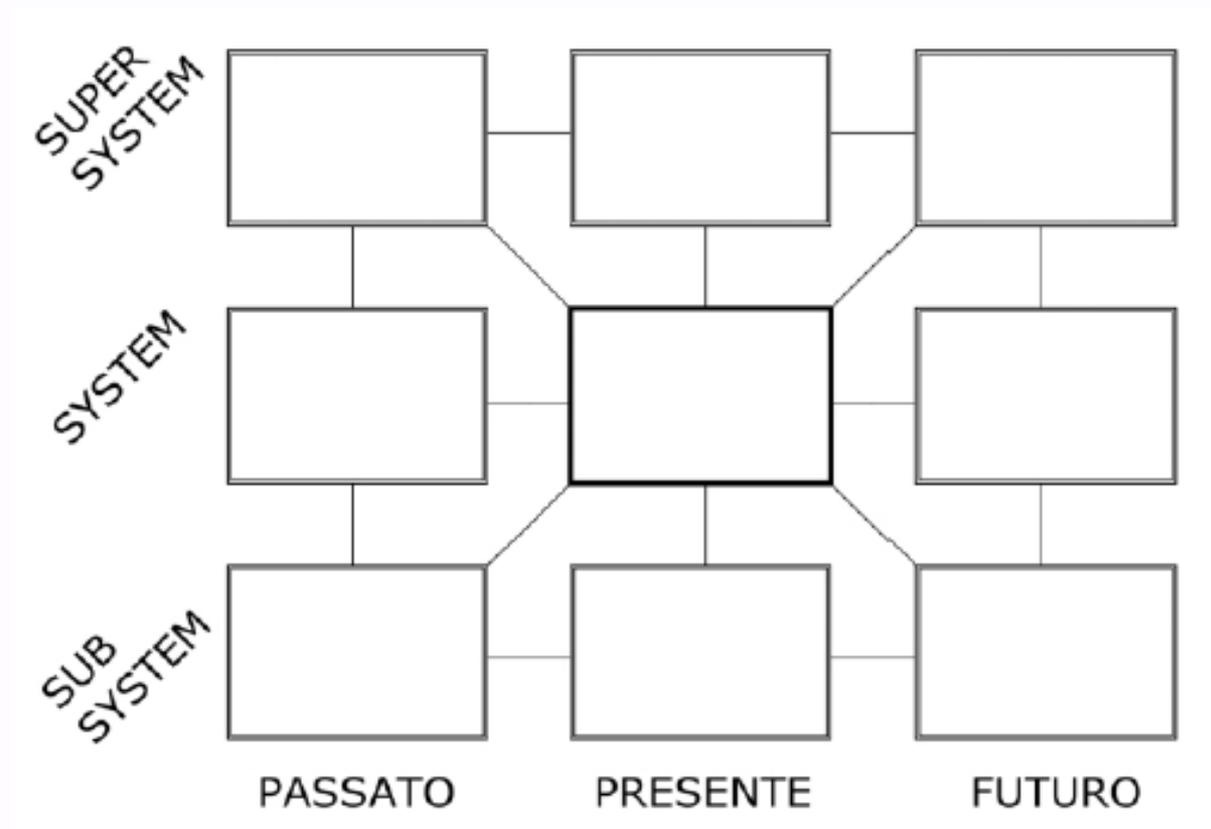


# Le domande da porsi

- 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

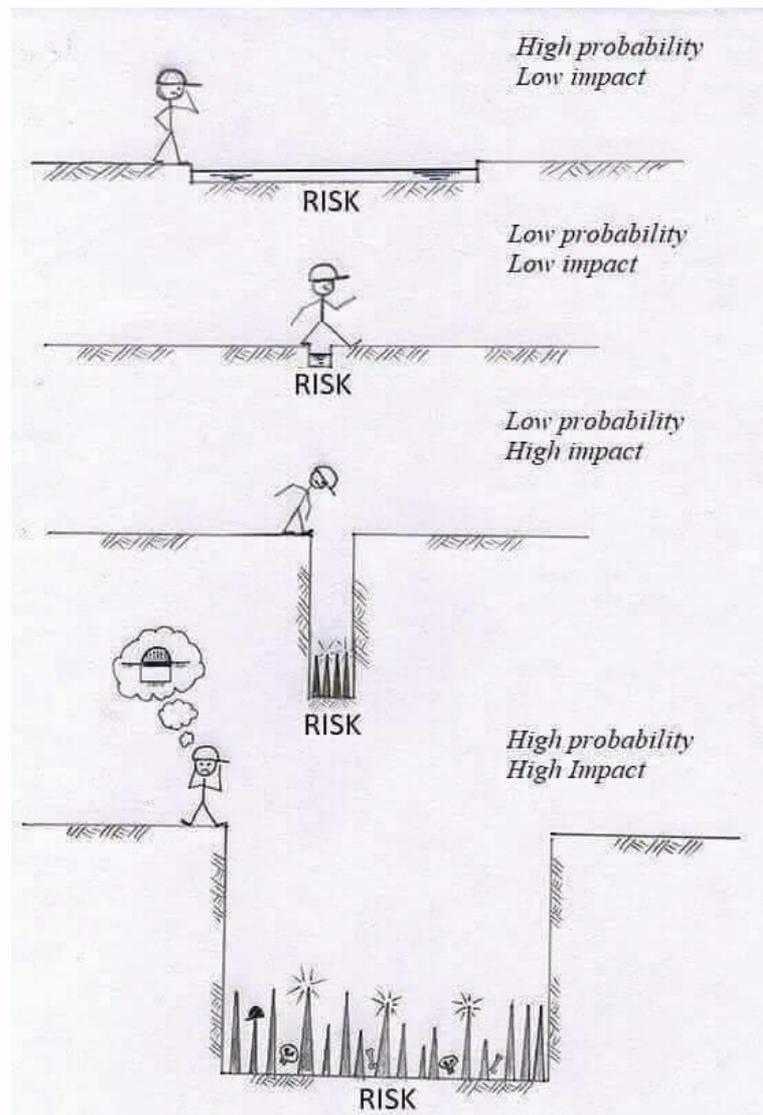


# Identificazione dei rischi

- 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 = Quanto spesso?

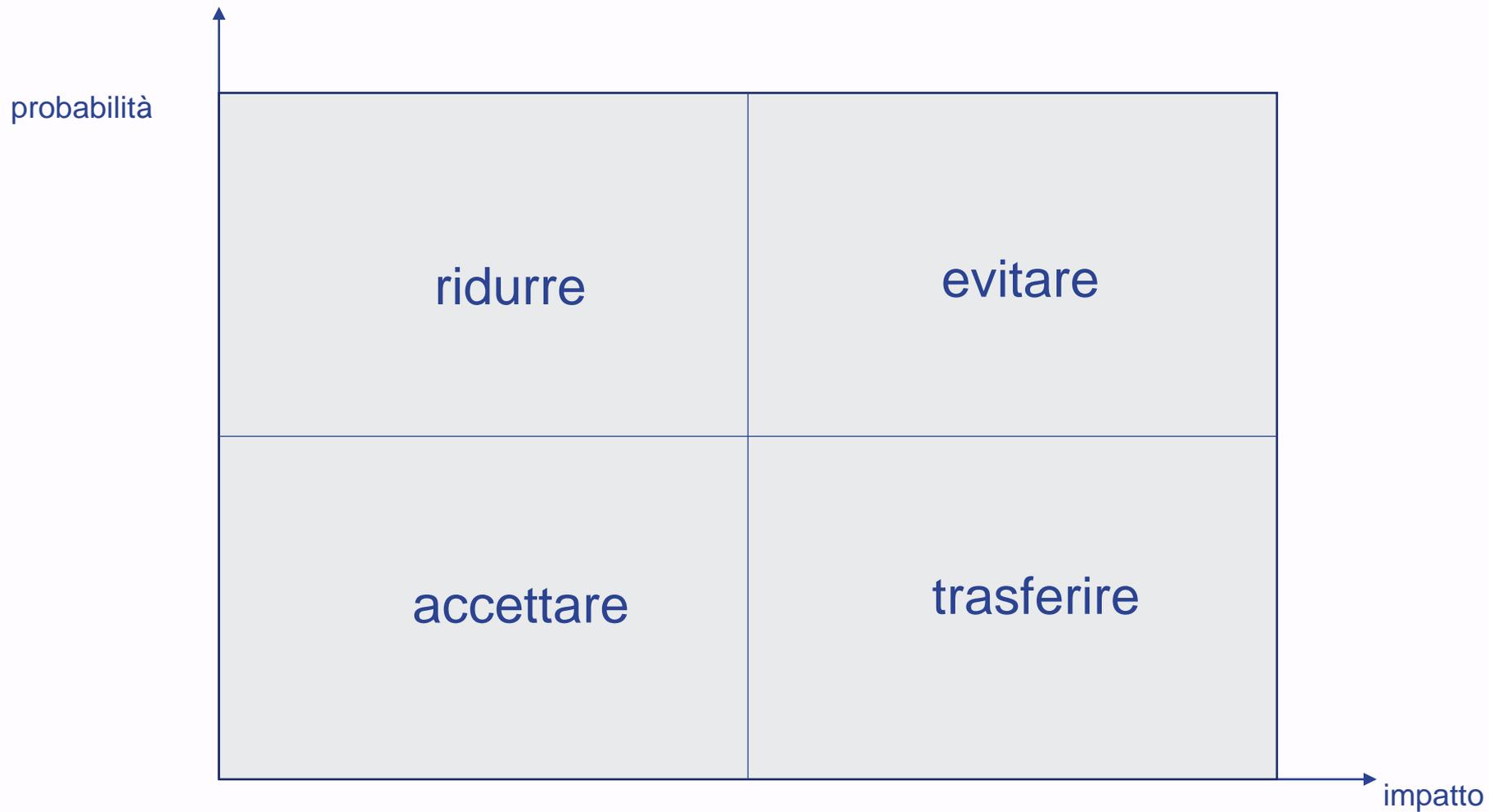


Impatto = Quanto male mi faccio?



NUOVI PERCORSI DI SVILUPPO  
DELLA CAPACITÀ AMMINISTRATIVA  
DELLA REGIONE SICILIANA

FormezPA



# Il calcolo del rischio

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

$$R = P \times I \times E$$

dove:

**P** = probabilità (della minaccia) (alta per minacce molto probabili)

**I** = impatto (gravità 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



NUOVI PERCORSI DI SVILUPPO  
DELLA CAPACITÀ AMMINISTRATIVA  
DELLA REGIONE SICILIANA

FormezPA

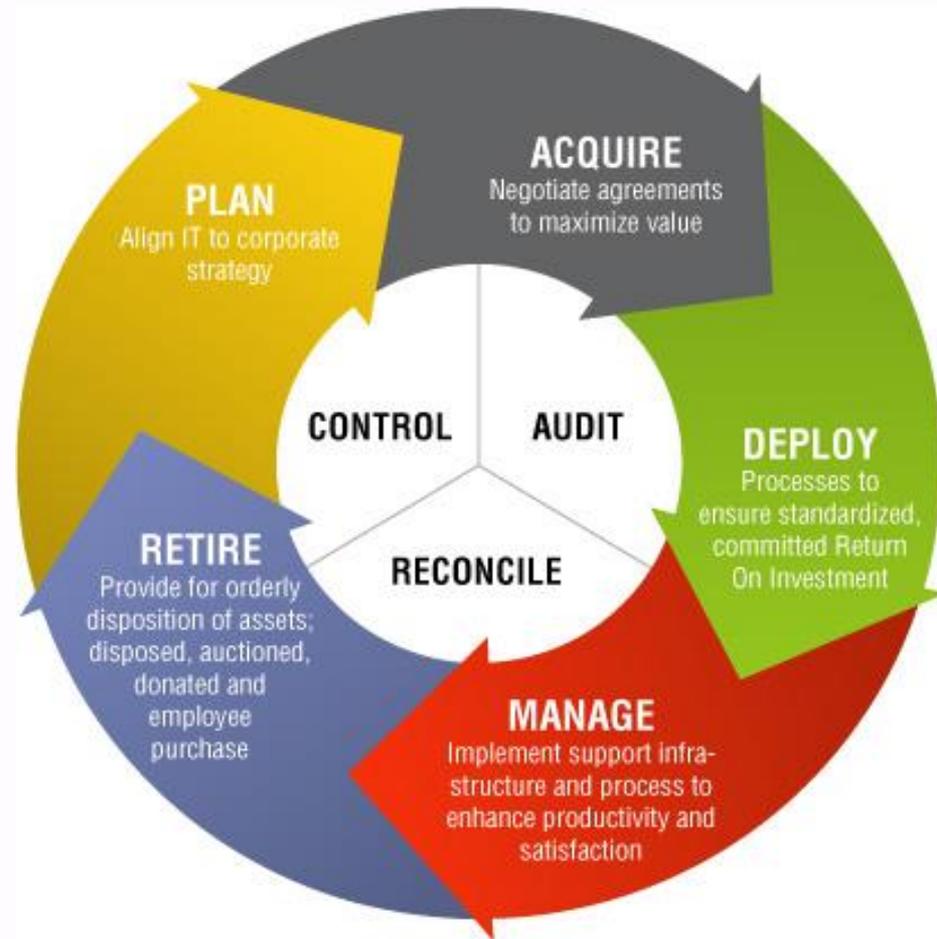
# Gli asset

"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.

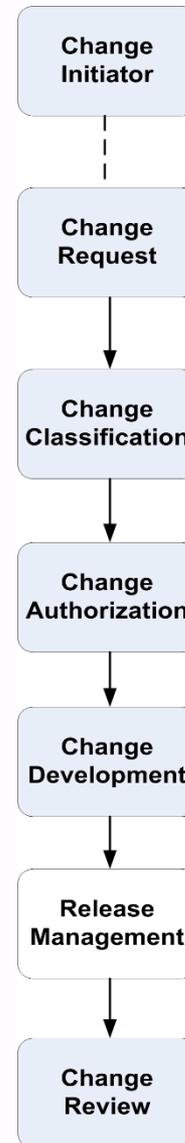
La RFC, corredata di un'analisi di impatto sul sistema e di uno studio di fattibilità, viene sottoposta a un **Change Manager**, che la discute di concerto con la **Change Advisory Board**, per l'approvazione.

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:

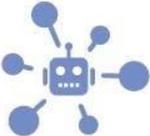
- il **Change Initiator**, colui che inserisce la RFC
- il **Change Manager**, che gestisce le attività di change management e riunisce e prepara il lavoro per la CAB
- il **Change Advisory Board (CAB)**, che è un gruppo di persone coinvolte nell'ambito IT operations e che valuta, approva e rifiuta una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



# Le minacce

## TOP 15 CYBER THREATS



1  Malware	2  Web-based attacks	3  Phishing	4  Web application attacks	5  Spam
6  DDoS	7  Identify theft	8  Data breach	9  Insider threat	10  Botnets
11  Physical manipulation, damage, theft and loss	12  Information leakage	13  Ransomware	14  Cyberespionage	15  Cryptojacking

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

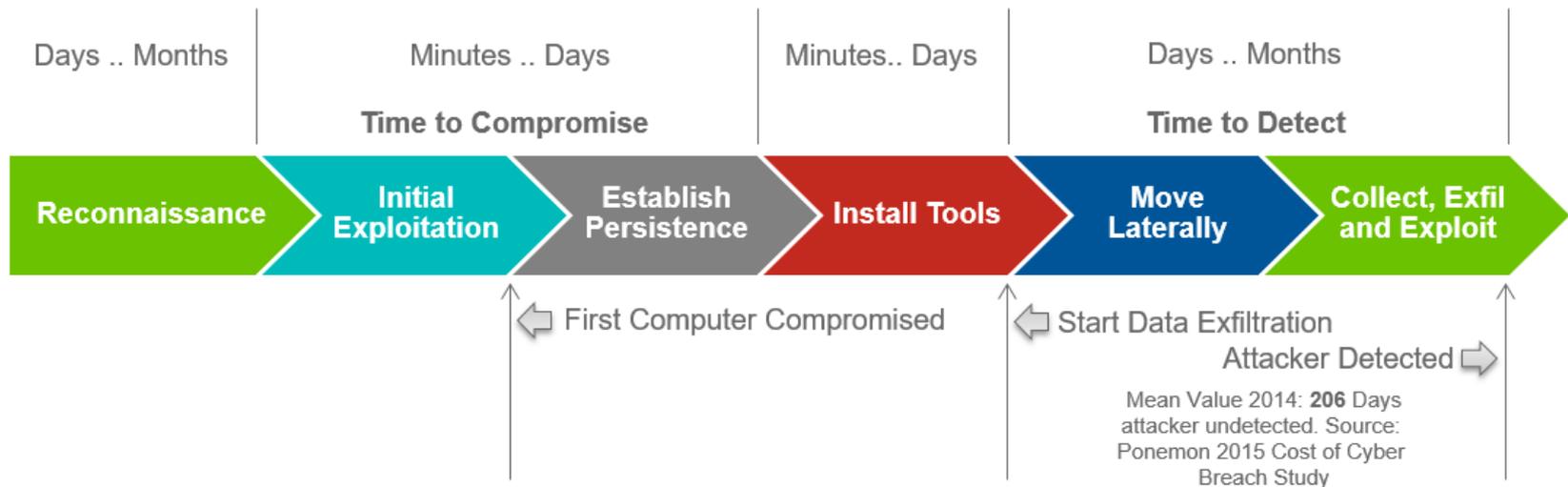


NUOVI PERCORSI DI SVILUPPO  
DELLA CAPACITÀ AMMINISTRATIVA  
DELLA REGIONE SICILIANA

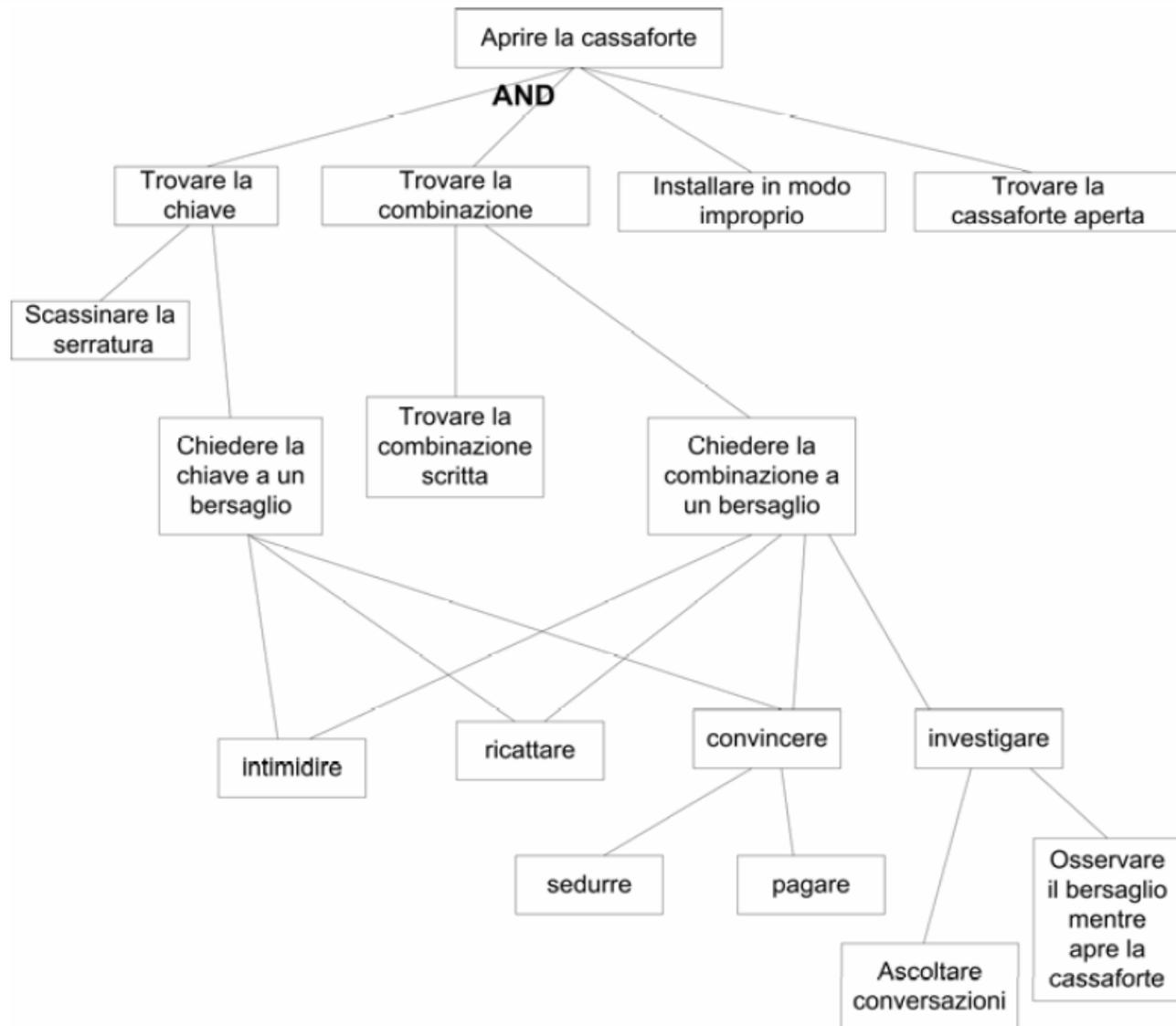
FormezPA

# Le minacce

## The Six Phases of a Cyber Attack



# 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.

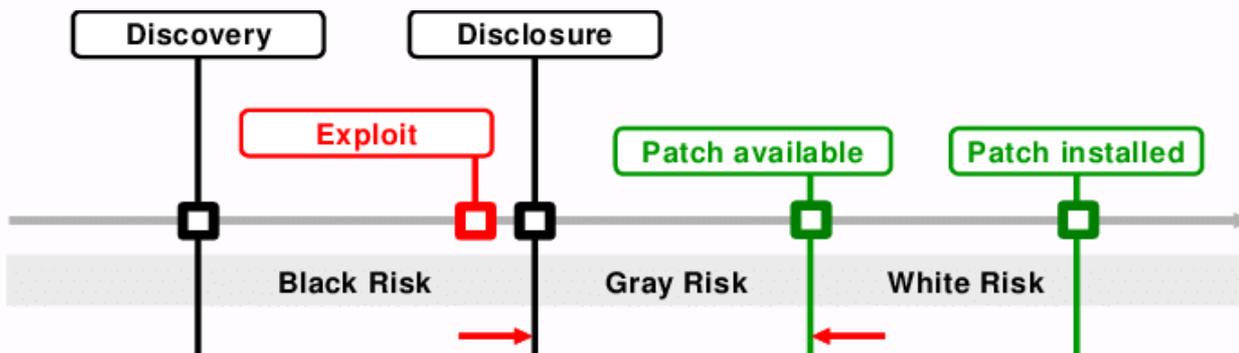
Il **potenziale d'attacco** rappresenta la “barriera” che un attaccante deve superare per poter sfruttare una vulnerabilità.

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](https://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



# March 2021

Below is a list of CVEs for the selected month.

**NOTE:** The CVEs shown below have a **release date** in the year and month chosen. The CVE ID may show a year value that does not match the release date, however, the release date will fall within the chosen year and month.

688 entries found for March 2021

CVE-2021-25122	CVE-2021-25329	CVE-2020-7929	CVE-2020-9479	CVE-2021-25829	CVE-2021-25830
CVE-2021-25831	CVE-2021-25832	CVE-2021-25833	CVE-2018-25004	CVE-2020-36240	CVE-2021-22114
CVE-2021-25914	CVE-2021-21515	CVE-2021-21517	CVE-2021-27317	CVE-2021-27318	CVE-2021-3332
CVE-2021-26475	CVE-2021-26476	CVE-2021-26702	CVE-2021-26703	CVE-2021-26704	CVE-2021-27876
CVE-2021-27877	CVE-2021-27878	CVE-2021-3342	CVE-2021-27884	CVE-2016-8001	CVE-2016-8003
CVE-2016-8004	CVE-2016-8013	CVE-2016-8014	CVE-2016-8015	CVE-2016-8028	CVE-2016-8040
CVE-2016-8041	CVE-2016-8042	CVE-2016-8043	CVE-2016-8044	CVE-2016-8045	CVE-2016-8046
CVE-2016-8047	CVE-2016-8048	CVE-2016-8049	CVE-2016-8107	CVE-2016-8108	CVE-2016-8109
CVE-2016-8110	CVE-2016-8111	CVE-2016-8112	CVE-2016-8113	CVE-2016-8114	CVE-2016-8115
CVE-2016-8116	CVE-2016-8117	CVE-2016-8118	CVE-2016-8119	CVE-2016-8120	CVE-2016-8121
CVE-2016-8122	CVE-2016-8123	CVE-2016-8124	CVE-2016-8125	CVE-2016-8126	CVE-2016-8127
CVE-2016-8128	CVE-2016-8129	CVE-2016-8130	CVE-2016-8131	CVE-2016-8132	CVE-2016-8133
CVE-2016-8134	CVE-2016-8135	CVE-2016-8136	CVE-2016-8137	CVE-2016-8138	CVE-2016-8139
CVE-2016-8140	CVE-2016-8141	CVE-2016-8142	CVE-2016-8143	CVE-2016-8144	CVE-2016-8145
CVE-2016-8146	CVE-2016-8147	CVE-2016-8148	CVE-2016-8149	CVE-2016-8150	CVE-2016-8151
CVE-2016-8152	CVE-2016-8153	CVE-2016-8154	CVE-2016-8155	CVE-2016-8156	CVE-2016-8157
CVE-2016-8158	CVE-2016-8159	CVE-2016-8160	CVE-2021-27886	CVE-2021-25306	CVE-2021-25309
CVE-2021-27731	CVE-2021-27804	CVE-2021-27888	CVE-2021-27730	CVE-2021-21320	CVE-2021-21321
CVE-2021-21322	CVE-2021-27901	CVE-2021-27904	CVE-2020-1936	CVE-2020-25902	CVE-2021-21513
CVE-2021-21514	CVE-2020-23518	CVE-2020-4719	CVE-2020-4725	CVE-2020-4726	CVE-2021-25330
CVE-2021-3384	CVE-2020-28657	CVE-2021-22187	CVE-2021-22294	CVE-2021-22296	CVE-2021-27885
CVE-2021-21255	CVE-2021-21258	CVE-2020-12527	CVE-2020-12528	CVE-2020-12529	CVE-2020-12530
CVE-2021-26412	CVE-2021-26854	CVE-2021-26855	CVE-2021-26857	CVE-2021-26858	CVE-2021-27065
CVE-2021-27078	CVE-2021-21352	CVE-2021-21353	CVE-2020-10519	CVE-2021-22861	CVE-2021-22862
CVE-2021-22863	CVE-2021-2138	CVE-2021-27921	CVE-2021-27922	CVE-2021-27923	CVE-2021-23347
CVE-2021-25315	CVE-2020-15937	CVE-2020-35296	CVE-2021-25252	CVE-2021-26813	CVE-2021-27215
CVE-2021-3419	CVE-2020-13554	CVE-2020-14372	CVE-2020-25632	CVE-2020-25647	CVE-2020-27749
CVE-2020-27779	CVE-2021-20076	CVE-2021-20225	CVE-2021-20233	CVE-2021-20441	CVE-2021-20442
CVE-2021-21979	CVE-2021-22638	CVE-2021-22662	CVE-2021-22666	CVE-2021-22670	CVE-2021-22683
CVE-2021-27927	CVE-2020-13558	CVE-2020-28591	CVE-2020-28597	CVE-2020-29047	CVE-2020-8296

<https://nvd.nist.gov/vuln/full-listing/2021/3>



# CVE-2021-25122 Detail

## Current Description

When responding to new h2c connection requests, Apache Tomcat versions 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41 and 8.5.0 to 8.5.61 could duplicate request headers and a limited amount of request body from one request to another meaning user A and user B could both see the results of user A's request.

[View Analysis Description](#)

### QUICK INFO

**CVE Dictionary Entry:**  
[CVE-2021-25122](#)

**NVD Published Date:**  
 03/01/2021

**NVD Last Modified:**  
 03/05/2021

**Source:**  
 Apache Software Foundation

Severity

CVSS Version 3.x
CVSS Version 2.0

**CVSS 3.x Severity and Metrics:**

**NIST:** NVD

Base Score: 7.5 HIGH

**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**CVSS v3.1 Severity and Metrics:**

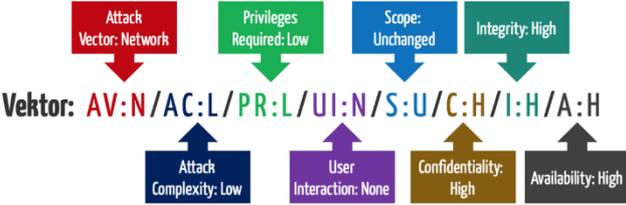
**Base Score:** 7.5 HIGH

**Vector:** AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**Impact Score:** 3.6

**Exploitability Score:** 3.9

*NVD Analysts use publicly available information to associate vector strings and CVSS scores. We do not have information from the CVE List from the CNA.*  
  
*Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information. We do not have information from this CVE List.*



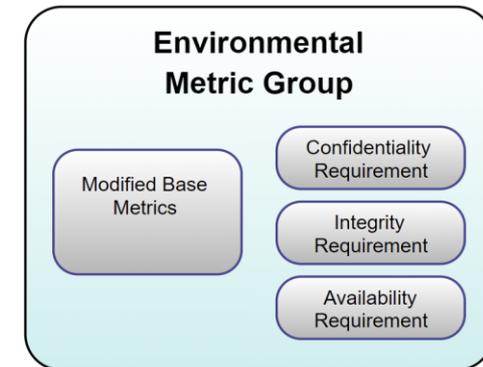
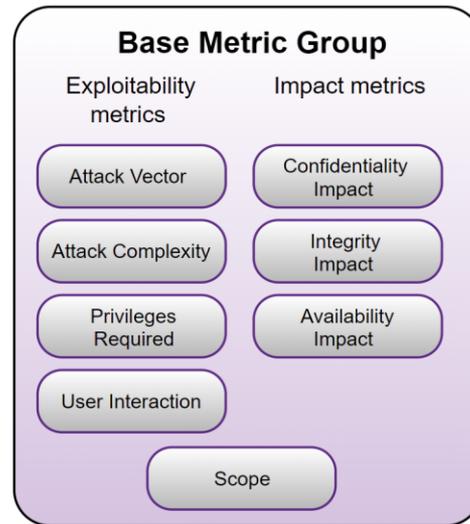
## References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to help you find more information that would be of interest to you. No inferences should be drawn on account of these links. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to [nvd@nist.gov](mailto:nvd@nist.gov).

Hyperlink	Resource
<a href="http://www.openwall.com/lists/oss-security/2021/03/01/1">http://www.openwall.com/lists/oss-security/2021/03/01/1</a>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px; background-color: #f0f0f0;">Mailing List</div> <div style="border: 1px solid #ccc; padding: 2px; background-color: #f0f0f0;">Third Party Advisory</div>
<a href="https://lists.apache.org/thread.html/r7b95bc248603360501f18c8eb03bb6001ec0ee3296205b34b07105b7%40%3Cannounce.tomcat.apache.org%3E">https://lists.apache.org/thread.html/r7b95bc248603360501f18c8eb03bb6001ec0ee3296205b34b07105b7%40%3Cannounce.tomcat.apache.org%3E</a>	<div style="border: 1px solid #ccc; padding: 2px; background-color: #f0f0f0;">Mailing List</div>

# 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

**CVSS v3.1**

ATTACK VECTOR	ATTACK COMPLEXITY	PRIVILEGES REQUIRED	USER INTERACTION
 Network	 Low	 None	 None
 Adjacent	 High	 Low	 Required
 Local		 High	
 Physical			

SCOPE	CONFIDENTIALITY	INTEGRITY	AVAILABILITY
 Changed	 High	 High	 High
 Unchanged	 Low	 Low	 Low
	 None	 None	 None

SEVERITY · SCORE · VECTOR		
Medium	5.4	CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:H

CVSS v3.1 Base Score Calculator - Copyright 2019 © Chandan

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



NUOVI PERCORSI DI SVILUPPO  
DELLA CAPACITÀ AMMINISTRATIVA  
DELLA REGIONE SICILIANA

FormezPA

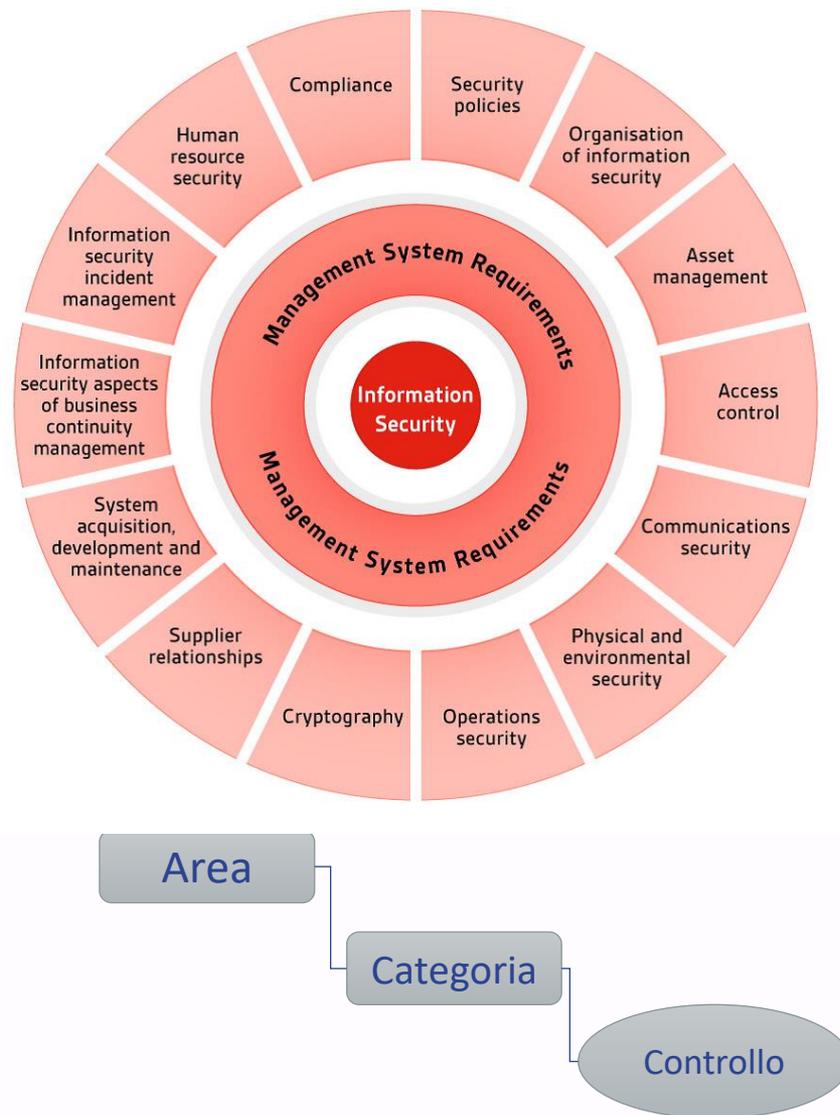
# Le contromisure

- 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

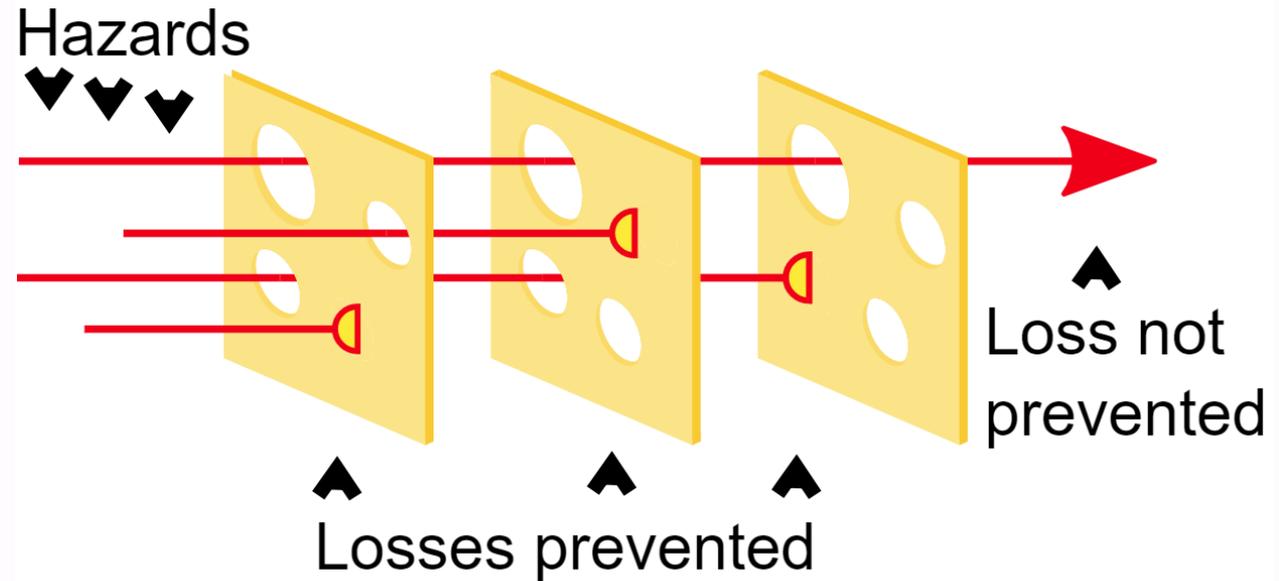
- **Controlli**:

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



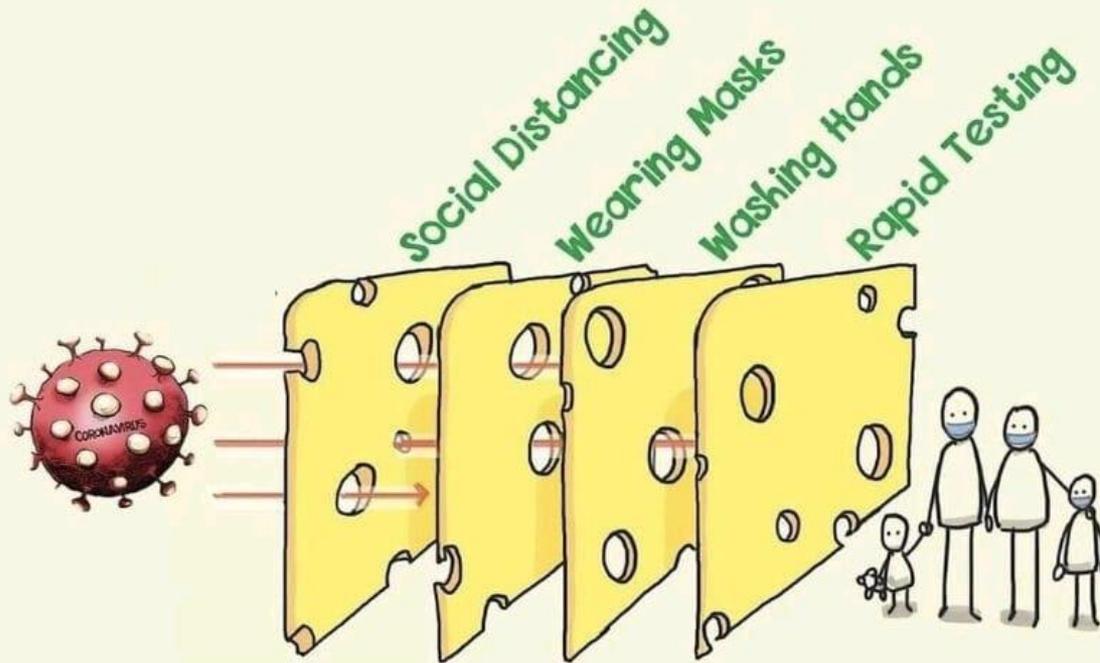
# Il modello del formaggio svizzero

**Defense in depth:**  
tutti i livelli sono importanti perché ciascuno non è perfetto



# Il modello del formaggio svizzero

## The Swiss Cheese Model



All layers are important because each layer is not perfect.

Created with sketchplanations.com



NUOVI PERCORSI DI SVILUPPO  
DELLA CAPACITÀ AMMINISTRATIVA  
DELLA REGIONE SICILIANA

FormezPA

# Analisi di uno use case

LO SAPEVI CHE?

In "Toy Story 4" (2019) si può notare per un attimo che la targa dell'auto che porta via Bo Peep è RMR F97. Questa sigla non è stata messa a caso ma ricorda un momento davvero terrificante per la Pixar.

Nel 1997 durante la produzione di "Toy Story 2" (1999) un tecnico cancellò per sbaglio praticamente tutto l'intero film spingendo i tasti RM - RF.

Quando tutto sembrava perduto, venne in soccorso della Pixar il direttore tecnico Galyn Susman, che in quel periodo era a casa in maternità e lavorava al film dalla sua abitazione.

Fortuna volle che lei aveva i file del film salvati nel suo computer e così riuscirono a recuperarlo.

Alla fine "Toy Story 2" ebbe un successo clamoroso con quasi 500 milioni di dollari di incasso a fronte di 90 milioni di spesa... e tutto grazie a Galyn e al suo bambino!



**PROTEGGI LA PIXAR!!!**



NUOVI PERCORSI DI SVILUPPO  
DELLA CAPACITÀ AMMINISTRATIVA  
DELLA REGIONE SICILIANA

FormezPA

# Analisi di uno use case

- 1) era stata fatta un'adeguata analisi dei rischi (Risposta: evidentemente no!)? Un progetto di 90 milioni di dollari dovrebbe averla
- 2) era necessario che il tecnico dovesse avere privilegi così elevati da poter distruggere tutto?
- 3) il tecnico era stato adeguatamente formato?
- 4) non si facevano backup?
- 5) il direttore tecnico era stato autorizzato a portarsi una copia del film a casa?
- 6) 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)?
- 7) avranno avuto un sistema di versioning per tenere traccia delle singole modifiche ed, eventualmente, fare rollback a un tempo definito?
- 8) se il tecnico avesse fatto lo gnorri era possibile risalire a lui (tracciabilità delle azioni)?
- 9) Per finire si potrebbe aggiungere anche un piccolo "information leak" sui sistemi operativi usati in azienda, visto che "rm -rf" è un comando Unix-like.



# 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 essere 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.
<b>il direttore tecnico era stato autorizzato a portarsi una copia del film a casa?</b>		
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 essere 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.
<b>Per finire si potrebbe aggiungere anche un piccolo "information leak" sui sistemi operativi usati in azienda, visto che "rm -rf" è un comando Unix-like.</b>		



# La PA come fornitore di servizi

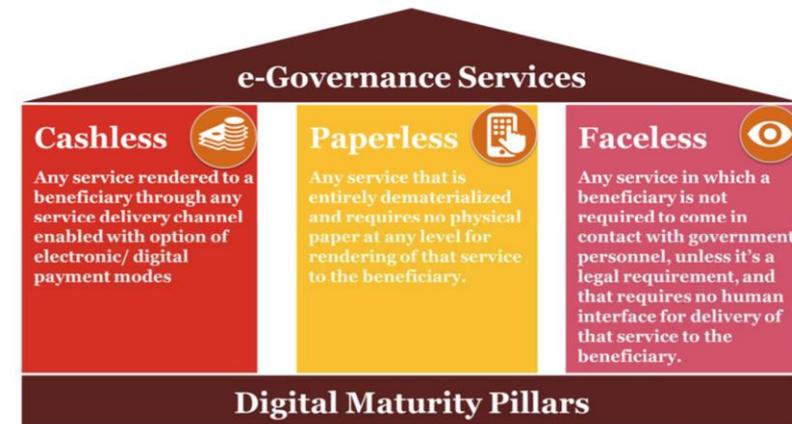
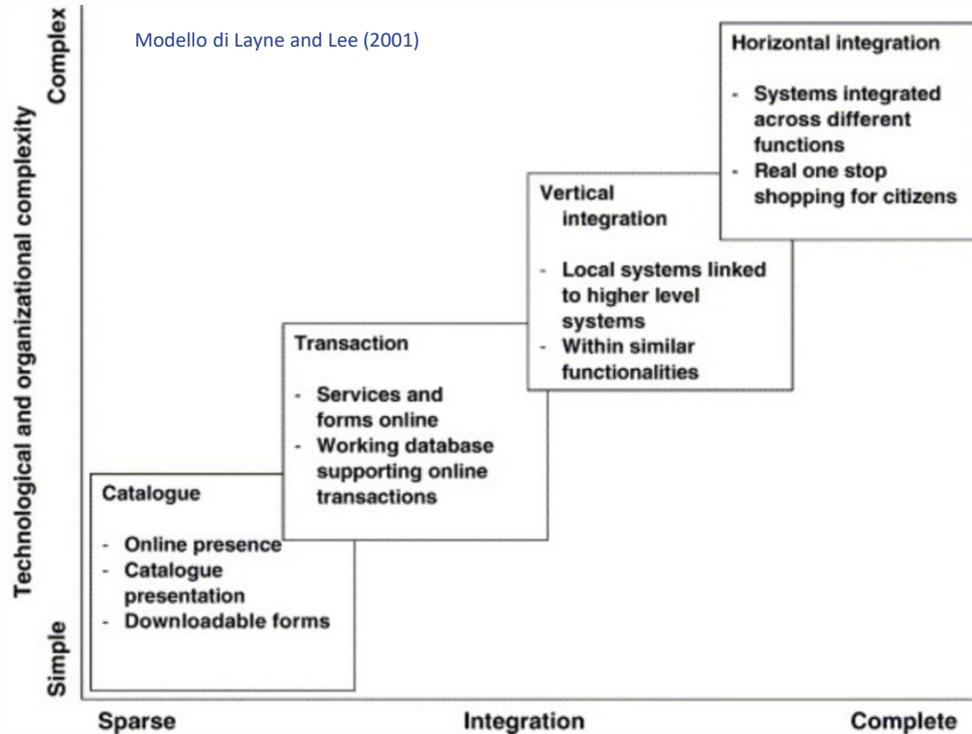
Un **servizio** è un meccanismo per abilitare l'accesso a una o più funzionalità di business attraverso un'interfaccia predefinita e in modalità coerente con vincoli e policies.

Ad esempio, l'Anagrafe è quel servizio che gestisce qualsiasi operazione sui dati anagrafici del cittadino e ci si accede nei modi e nei tempi consentiti dall'Amministrazione

- G2G (Government to Government)
- G2C (Government to Citizens)
- G2B (Government to Business)



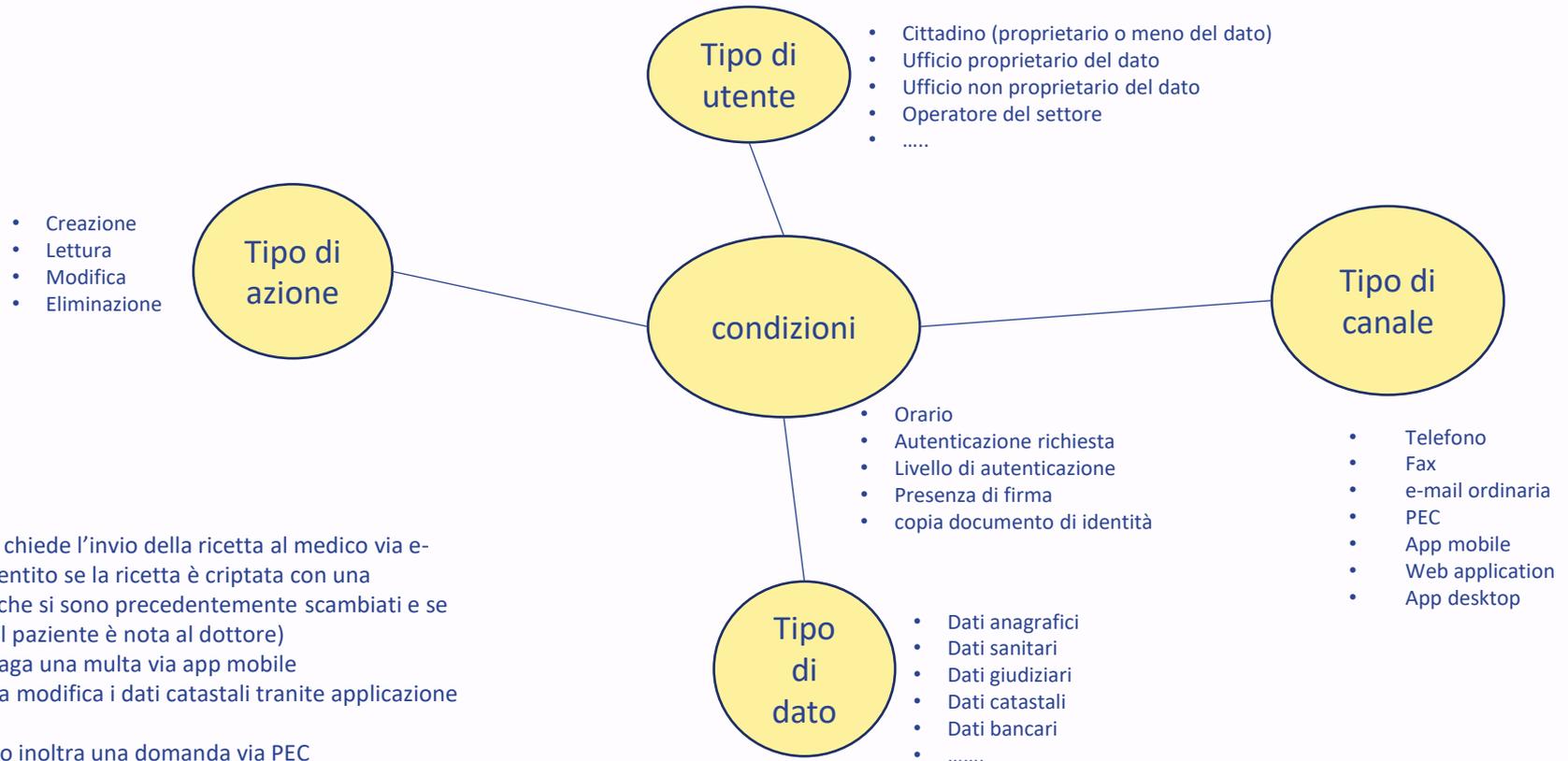
# Modelli di maturità nell'e-gov



- Gateway di pagamento
- E-wallet
- Interfacce di pagamento unificate
- Fascicolo sanitario elettronico
- Firma digitale
- Dematerializzazione
- Archivi digitali
- E-forms
- Identità digitale
- PEC
- Digital locker
- Electronic filing



# I servizi verso il cittadino



## Esempi:

- il paziente chiede l'invio della ricetta al medico via e-mail (consentito se la ricetta è criptata con una password che si sono precedentemente scambiati e se l'e-mail del paziente è nota al dottore)
- L'utente paga una multa via app mobile
- Il geometra modifica i dati catastali tramite applicazione web
- Il candidato inoltra una domanda via PEC



# 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



# Grazie dell'attenzione!

Alessandro Sinibaldi



NUOVI PERCORSI DI SVILUPPO  
DELLA CAPACITÀ AMMINISTRATIVA  
DELLA REGIONE SICILIANA

FormezPA