La sicurezza informatica nella pubblica amministrazione
- 2° Ciclo Formazione Sicurezza Informatica nella PA -

Sicurezza organizzativa

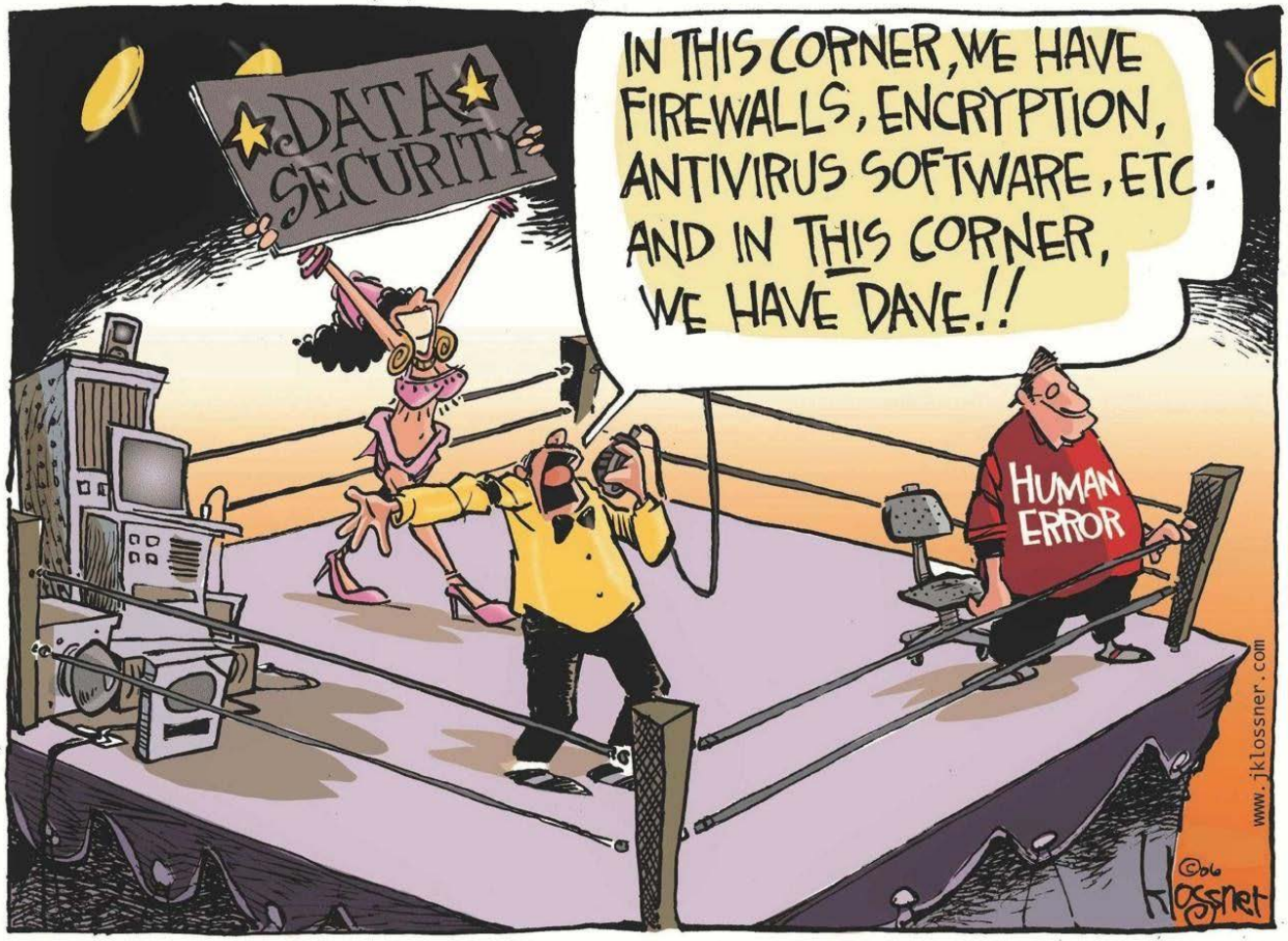
Alessandro Sinibaldi, AgID

agenda

- La gestione del Rischio
- La sicurezza organizzativa
- La sicurezza nei progetti
- La sicurezza nei processi
- La sicurezza nei servizi
- La gestione dei ruoli
- La gestione degli incidenti

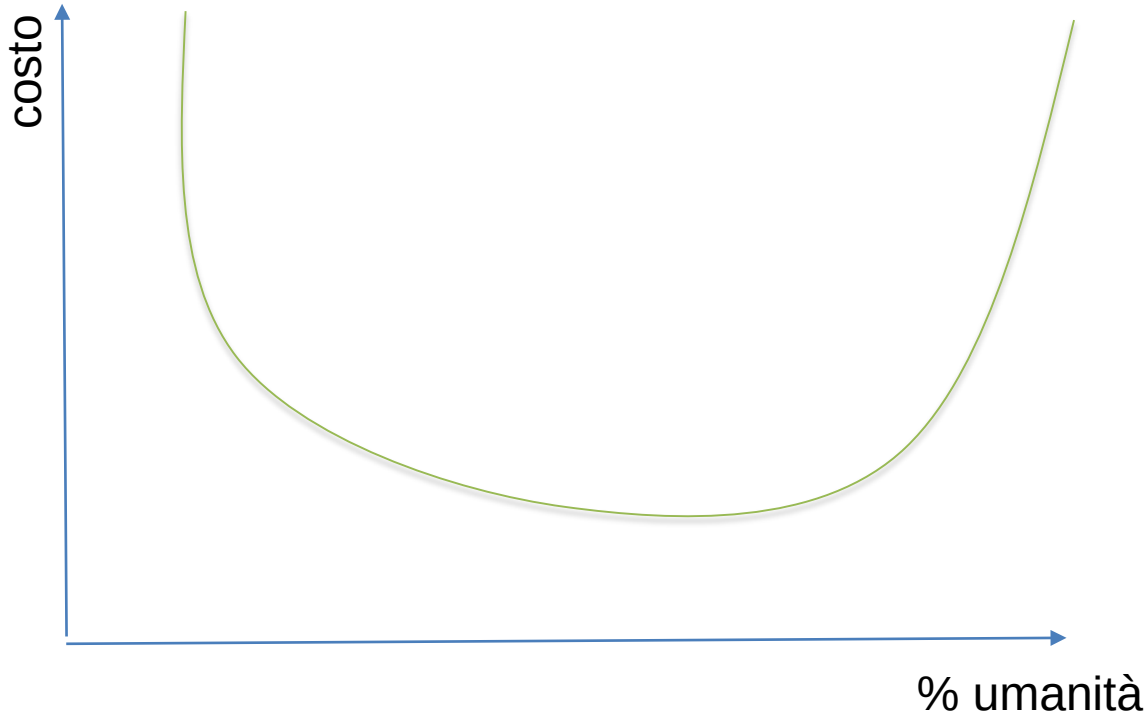
Quattro principi fondamentali

- “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”


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©06 Klossner

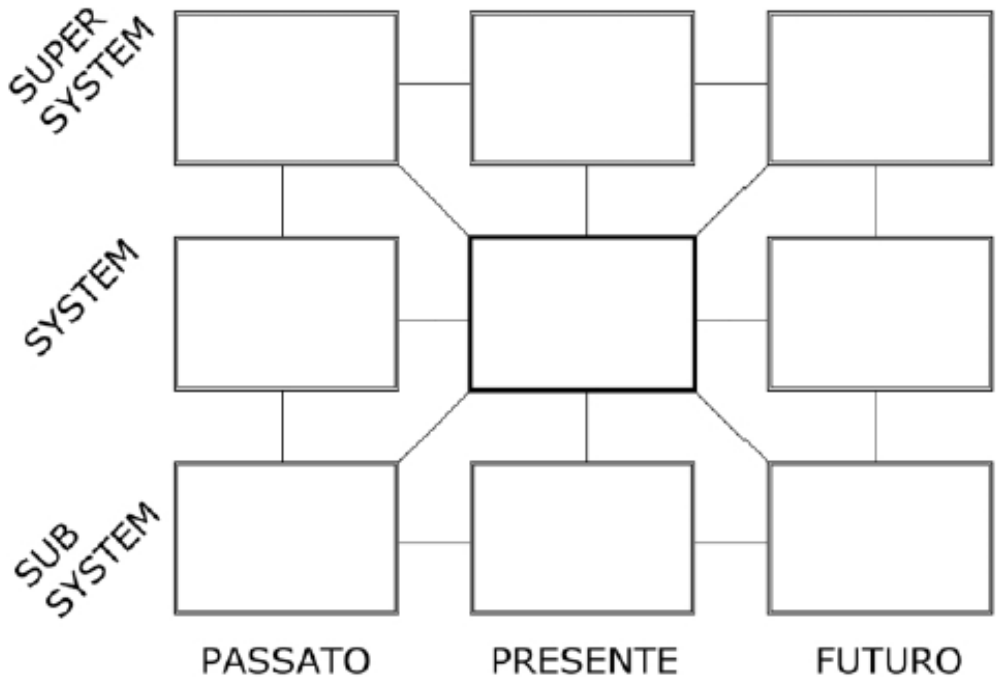
Il paradosso di Mayfield

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

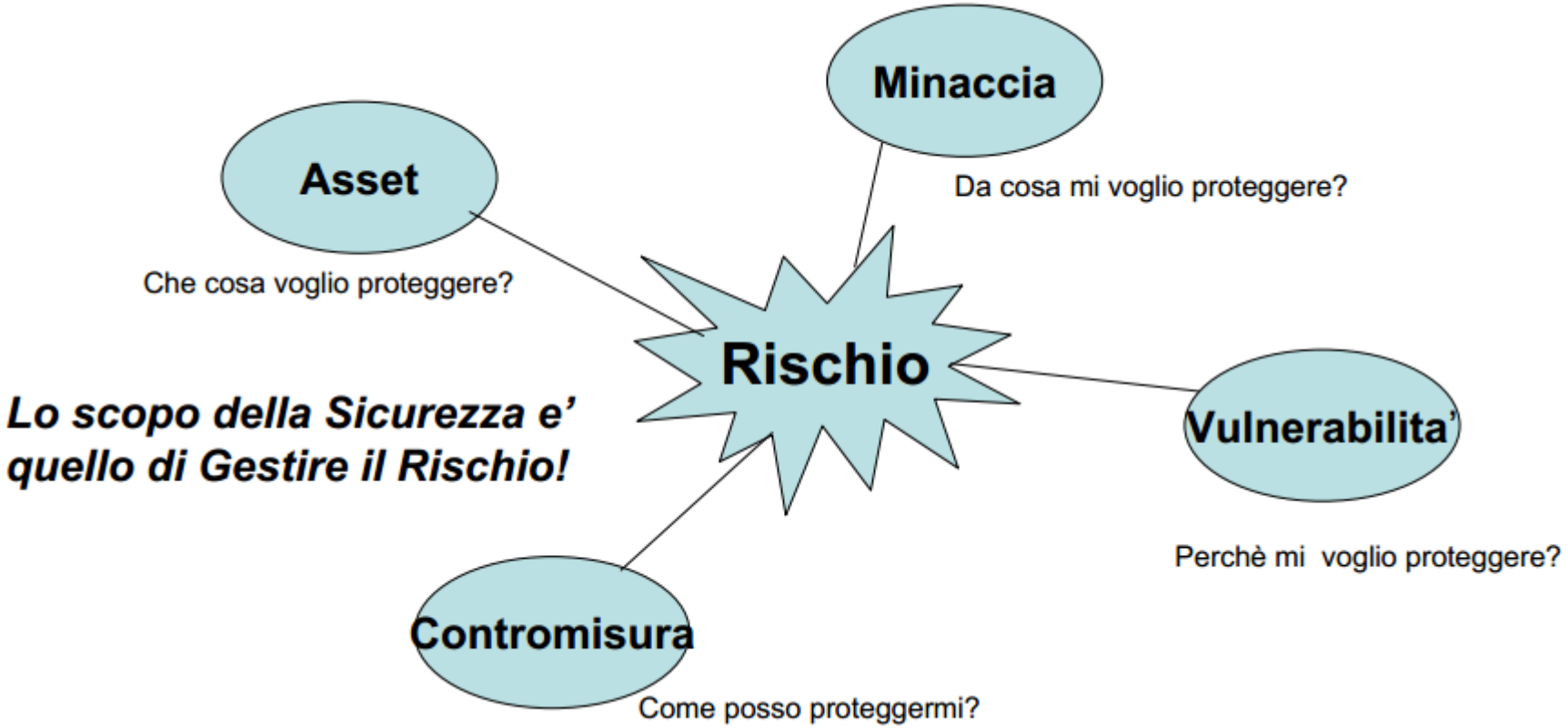


Bezos: «Amazon fallirà. Il nostro compito è far sì che accada il più tardi possibile»

Un utile strumento mentale



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:

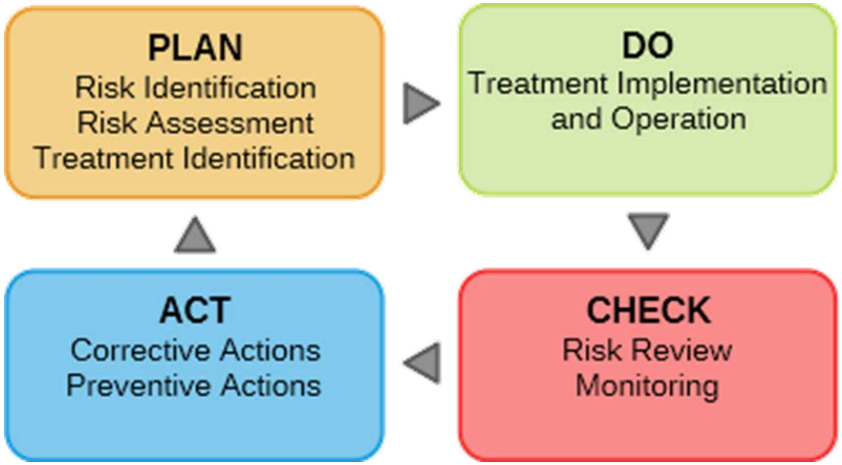
- **Identificazione** in questa fase si cerca di determinare le possibili fonti di Rischio e individuare quegli eventi che potrebbe causare l'insorgere di Pericoli

- **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

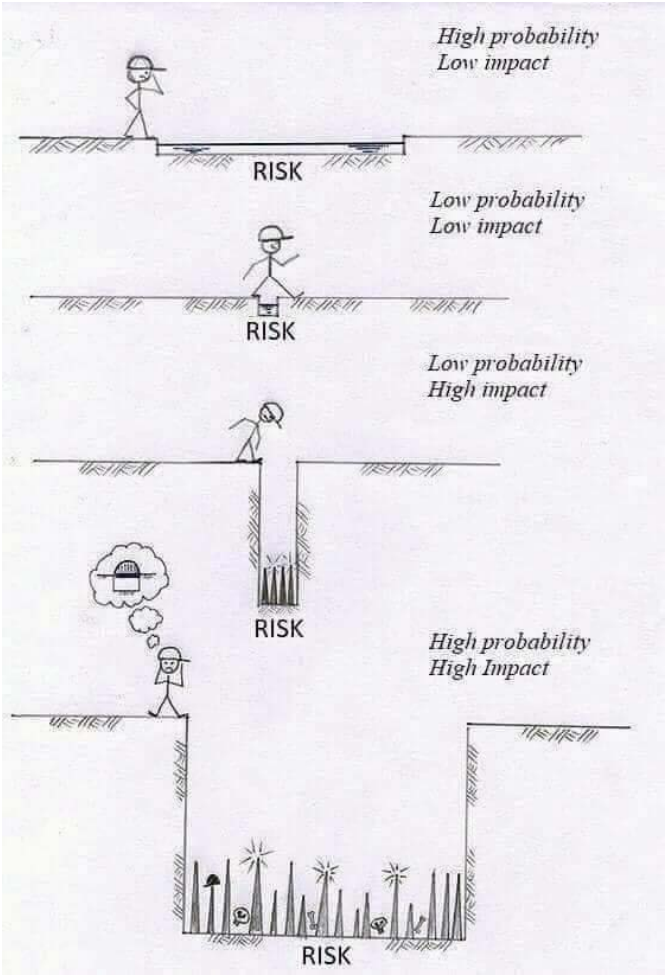
L'output di ognuna delle 4 fasi confluisce nel Piano del Rischio (Risk Plan) complessivo.



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?

Il calcolo del rischio

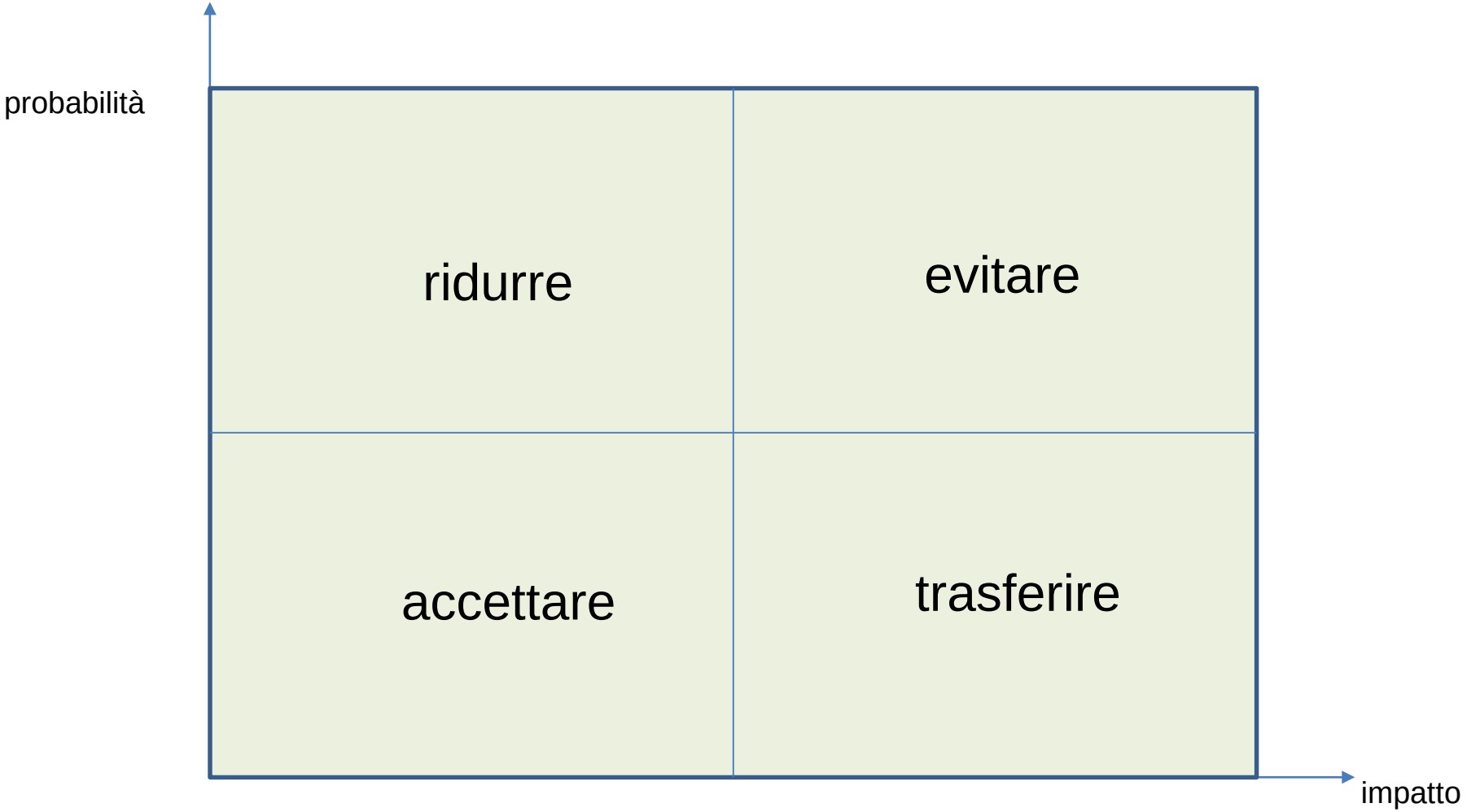
Il Rischio viene solitamente definito e calcolato come prodotto dei fattori:

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).


probabilità
ridurre
evitare
accettare
trasferire
impatto

CYBERSECURITY RISK RATING AND RELATED SERVICE LEVEL OBJECTIVES	
Extreme = range 90+	***Extreme Risk Level - Priority 1 -*** Indicates a deficiency which has been rated as an Extreme Risk /Impact on the organization's business processes which needs to be immediately corrected. Using a work around or manual process cannot reduce the impact. All involved parties, including individuals SIRT assigned employees within the organization, are expected to work continuously (24 X 7) until the incident is resolved or until the Priority is reduced. During regular business hours, the following service levels apply: • Security Incident Report (SIR) is accepted within 15 minutes; • SIR Ticket is updated within 1 hour with updates provided every hour until resolution; • Target Resolution time is 2 hours
Critical = range 80 - 89	***Critical Risk Level - Priority 2 -*** Indicates a deficiency which has been rated as a Critical Risk /Impact on the organization's business processes which needs to be immediately corrected within the agreed upon SLA /OLA terms. A limited work around or manual process is available. All involved parties, including SIRT members assigned by the organization, are expected to work during regular business hours until the incident is resolved or until the Priority is reduced. During regular business hours, the following service levels apply: • Security Incident Report (SIR) is accepted within 30 minutes; • SIR Ticket is updated within 90 minutes with updates provided every 90 minutes until resolution; • Target Resolution time is 4 hours.
High = range 60 - 79	***High Risk Level - Priority 3 -*** Indicates a deficiency which has been rated as a High Risk /Impact on the organization's business processes which needs to be immediately corrected within the SLA /OLA terms. Work is expected to continue during regular business hours until the incident is resolved or until the Priority is reduced. During regular business hours, the following service levels apply: • Security Risk Report (SRR) is accepted within 5 Business Days; • The SRR Ticket is updated within 4 hours with updates provided every 4 hours until resolution; • Target Resolution time is 10 business day.
Medium = range 30 - 59	**Medium Risk Level - Priority 4 -** Indicates a deficiency which has been rated as a Medium Risk /Impact on the organization's business processes which needs to be corrected and validated within the agreed upon SLA /OLA terms. Work is expected to continue during business hours until the incident is resolved. During regular business hours, the following service levels apply: • Security Risk Report (SRR) is accepted within 10 business days; • SRR Ticket is updated within 7 business days with updates provided every business day; • Target Resolution time is 30 business days.
Low = range 0 - 29	**Low Risk Level - Priority 5 -** Indicates a deficiency within the organization's services which cannot be rectified without a patch, fix or update assistance from outside agencies such as the software vendor. Work is expected to continue during business hours until the incident is resolved. During regular business hours, the following service levels apply: • Security Risk Report (SRR) is accepted within 30 business days; • SRR Ticket is updated within 20 business days; • Target Resolution time is 90 business days after fix, patch or resolution is received or next available scheduled change window as required.

Le minacce

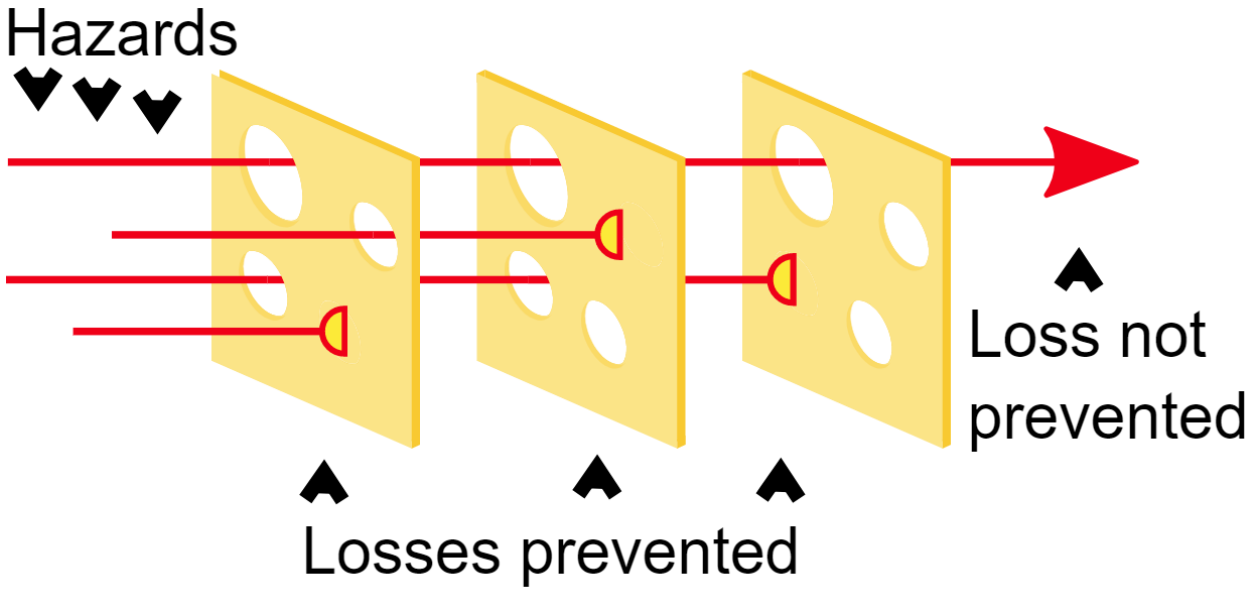
https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

Identificazione delle contromisure

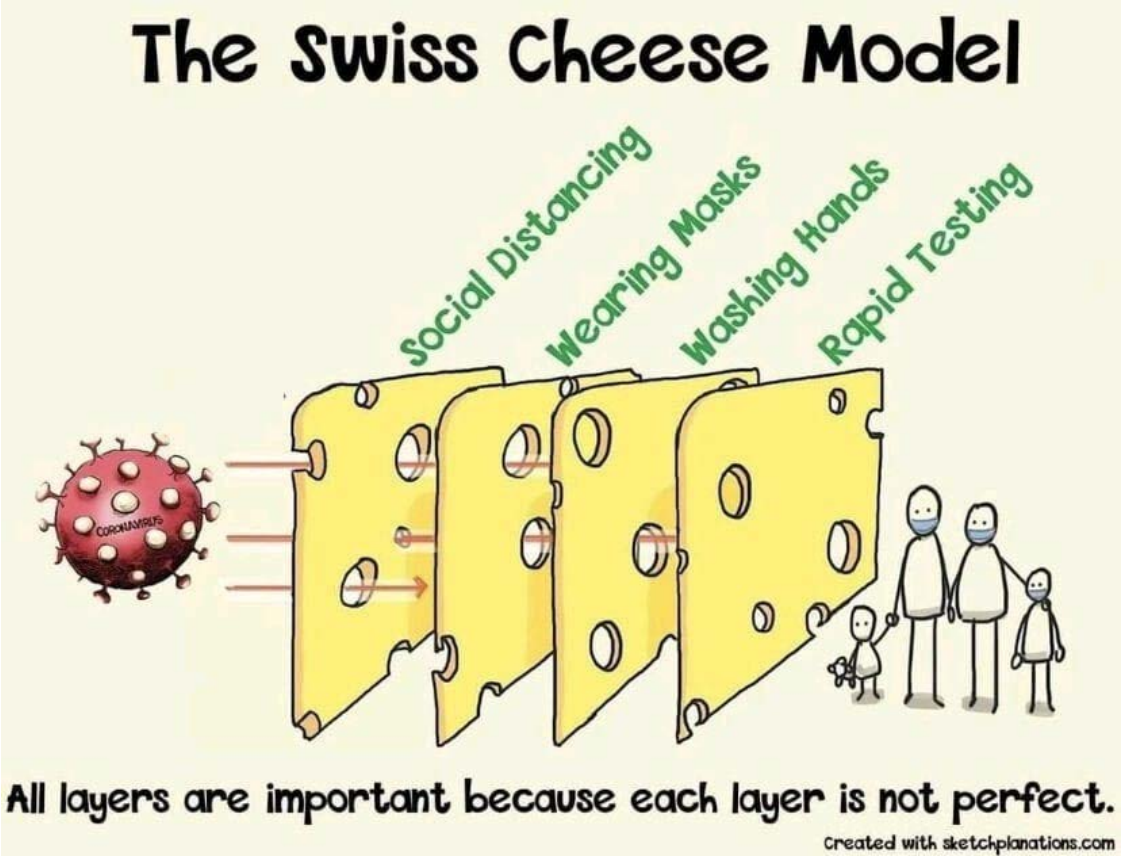
- ISO 27001 (114 controlli suddivisi in 14 aree)
- SANS 20
- Misure minime
- OWASP Proactive Controls
- ….

Il modello del formaggio svizzero

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



Il modello del formaggio svizzero



Cos’è un’organizzazione?

insieme di ruoli, processi, progetti e servizi, logicamente coordinati tra loro, atti a compiere la mission dell'ente

Cosa si intende con “sicurezza organizzativa”?

È la **gestione del rischio organizzativo**, inteso come

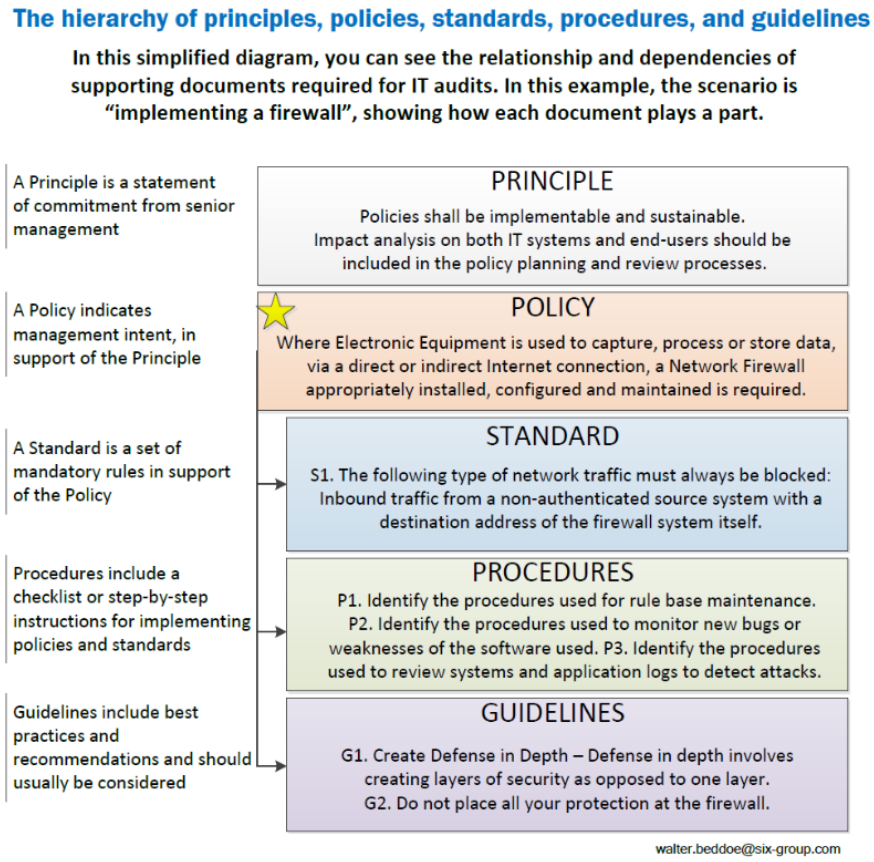
«il rischio derivante da una o più carenze dell’organizzazione, in termini gestionali, metodologici, operativi come un’insufficiente formazione, attribuzioni di responsabilità poco chiare, mancanza o inefficacia di procedure interne, scarso coinvolgimento, carenze metodologiche nell’analisi del rischio, ecc. »

I rischi organizzativi sono i rischi che dipendono dalle cosiddette “dinamiche aziendali”, cioè dall’insieme dei rapporti lavorativi, interpersonali e di organizzazione che si creano all’interno di un ambito lavorativo

Alcuni esempi di cause di rischio organizzativo

- governance carente
- ruoli poco chiari
- No accountability (Accountability = consapevoli, competenti e responsabili)
- Mancanza di policy
- processi non definiti
- formazione non adeguata
- livelli di servizio non esplicitati
- requisiti di sicurezza non elicitati
- dipendenze tra gli asset non analizzate
- gestione degli incidenti non attiva

Policy, standard e linee guida



Principi di sicurezza
https://www.youtube.com/watch?v=j1PGeUthii0

Cos’è un politica per la sicurezza delle informazioni?

E’ un documento finalizzato a definire gli indirizzi e le regole generali da applicare in materia di sicurezza all’interno di tutta l’organizzazione ed è la base di partenza di tutto il sistema di gestione. La politica, sintetica ed estremamente comprensibile nella sua stesura, deve includere:

- una definizione di cosa si intende come sicurezza delle informazioni, dei suoi obiettivi e della sua importanza, in linea con gli obiettivi aziendali e la normativa sulla privacy;
- un indirizzo generale e i principi di azione concernenti la protezione dei dati personali;
- la descrizione dei processi necessari alla gestione della sicurezza delle informazioni e dei dati personali;
- la formalizzazione di ruoli e responsabilità;
- i criteri rispetto ai quali ponderare i rischi.

Tale Politica deve essere riesaminata almeno con cadenza annuale e venire approvata dalla Direzione affinché sia garantito e visibile il necessario appoggio.
Alla Politica deve essere associato un Elenco della documentazione aziendale (procedure) rilevante sul tema.

Cosa è un progetto?

In letteratura sono state formulate varie definizioni di progetto, ma tutte concordano su quattro aspetti:

- occorre un motivo per iniziare un progetto
- deve essere esplicitato e condiviso l'obiettivo del progetto
- il progetto ha una durata finita
- ci sono dei vincoli da rispettare

Un progetto è, di fatto, un'associazione temporanea di persone che hanno un obiettivo comune.

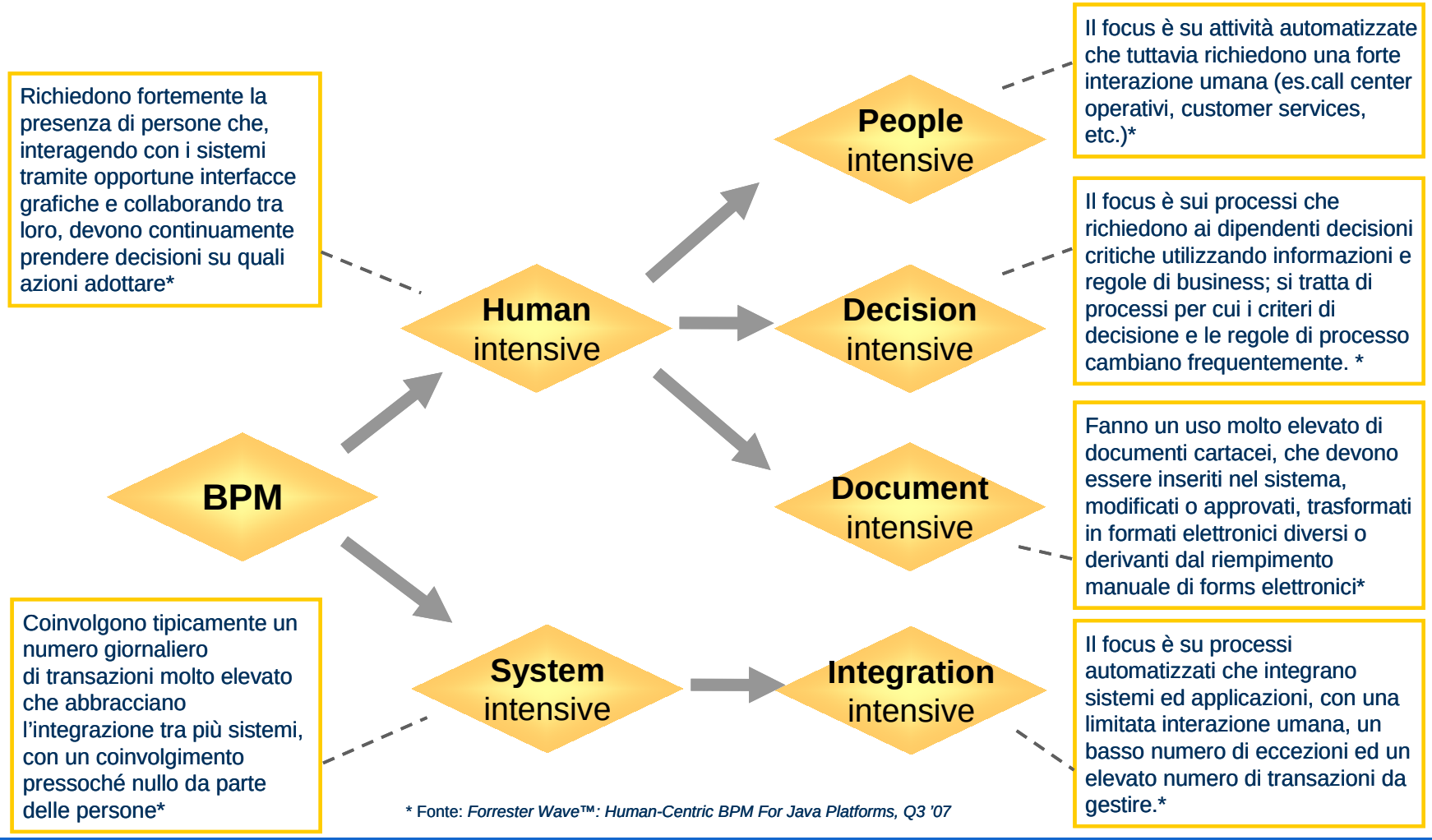
Il fatto che sia temporaneo, permette di distinguerlo da altre tipologie di attività che, invece, fanno parte dell'area di Operations (in italiano Esercizio o Produzione), e cioè le attività di gestione e manutenzione quotidiana dei sistemi.

La sicurezza nei progetti

- un membro del team di sicurezza dovrebbe essere coinvolto fin dall'inizio per valutare eventuali coinvolgimenti di sicurezza
- ambienti di sviluppo, test, collaudo e produzione separati tra loro
- team di sviluppo e test separati
- gestione delle configurazioni
- gestione del cambiamento
- gestione dei requisiti
- valutazione dei rischi
- i dati della produzione usati nell'ambiente di collaudo devono essere anonimizzati
- sistemi di gestione del ciclo di vita di software e hardware
- i membri del team dovrebbero avere tutti un livello minimo di competenze di sicurezza e comunque commisurate al loro ruolo
- Procurement sicuro (v. linee guida AGID)

Cosa è un processo?

Un processo è un insieme di attività correlate che hanno complessivamente un obiettivo comune come, ad esempio, la produzione di un bene o di un servizio o, più in generale, la creazione di valore per il cliente



* Fonte: *Forrester Wave™: Human-Centric BPM For Java Platforms, Q3 '07*

Cosa è un processo?

Un processo:

- ha uno scopo
- ha degli input specifici
- ha degli output specifici
- usa risorse
- è composto da una serie di attività che vengono eseguite in un ordine preciso
- può impattare più di un'unità organizzativa (impatto orizzontale)
- crea valore per un cliente (interno o esterno)

La sicurezza nei processi

- Costruire un catalogo dei processi
- Valutare i rischi
- Identificare i processi critici

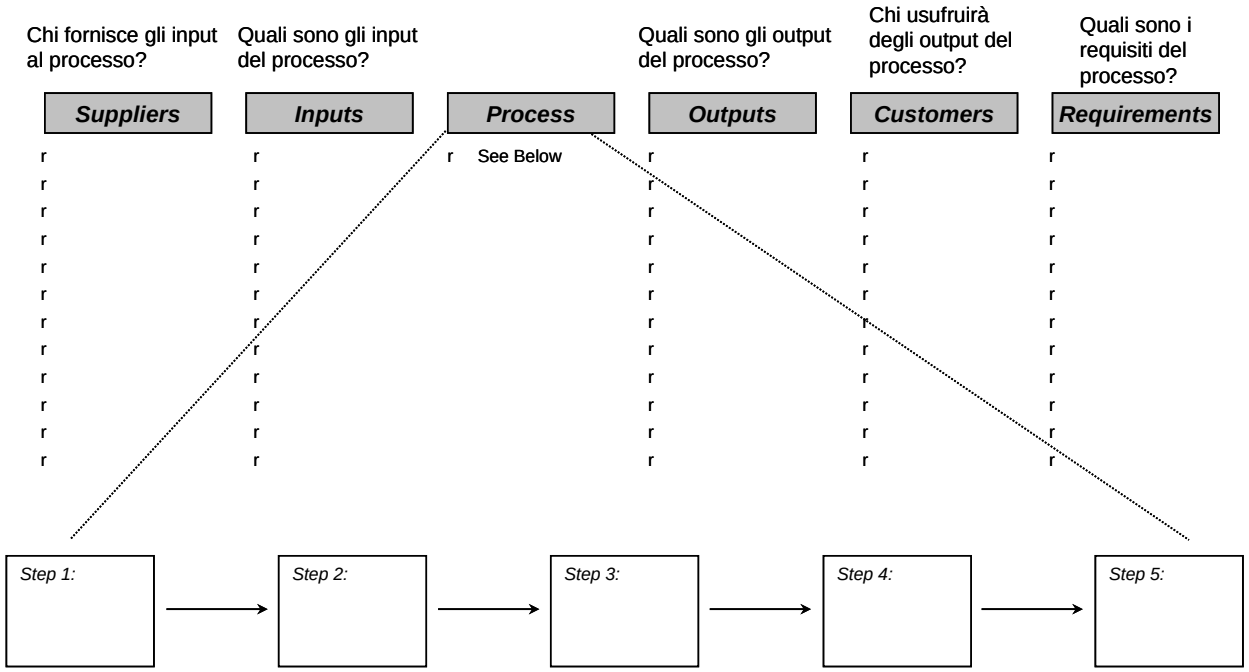
  Processi critici = Sono quei processi i cui malfunzionamenti impattano sull'efficienza e sull'efficacia dell'organizzazione

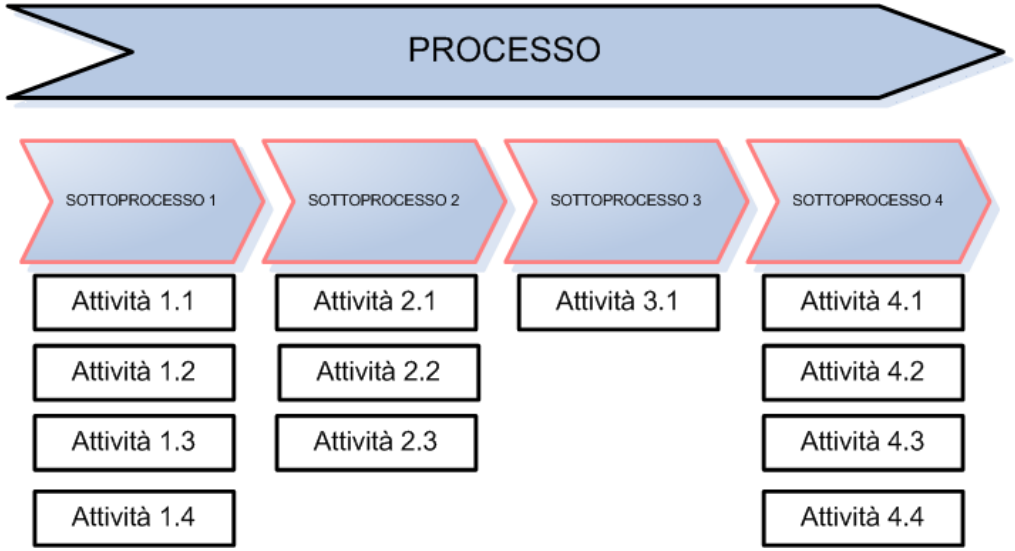
- Identificare le dipendenze tra i processi e dei processi con i servizi
- Monitorare i processi

Documentare i processi

- definire lo scopo del processo;
- definire il responsabile del processo;
- stabilire inizio e fine del processo (delimitazione del processo);
- identificare il cliente del processo;
- specificare l'output del processo;
- definire gli input del processo;
- definire i fornitori degli input;
- verificare i vincoli, le leggi e i regolamenti;
- identificare le infrastrutture necessarie per produrre l'output;
- identificare le risorse umane necessarie e i livelli di competenza richiesti;
- identificare i sottoprocessi;
- Identificare le metriche di processo;
- evidenziare se l'output del processo costituisce l'input per un altro processo.

Il diagramma SIPOC




PROCESSO
SOTTOPROCESSO 1
SOTTOPROCESSO 2
SOTTOPROCESSO 3
SOTTOPROCESSO 4
Attività 1.1
Attività 1.2
Attività 1.3
Attività 1.4
Attività 2.1
Attività 2.2
Attività 2.3
Attività 3.1
Attività 4.1
Attività 4.2
Attività 4.3
Attività 4.4


1. Ricezione Documento
2. Dematerializzazione
3. Archiviazione
4. Gestione elettronica documento
5. Conservazione sostitutiva
6. Editing/ Publishing
7. Invio Documento
Intercettazione e raggruppamento dei documenti
Ricezione di un flusso dati dal cliente
Scannerizzazione
Lettura e interpretazione dei dati
Protocollazione
Classificazione
Indicizzazione
Archiviazione elettronica
Archiviazione fisica
Applicazione di regole per il trattamento automatico del documento
Apposizione marca temporale e firma digitale
Pubblicazione su web per consultazione in remoto
Pubblicazione su portale aziendale documentale
Servizi di reporting
Spedizione del documento in formato cartaceo o elettronico

Cosa è un servizio?

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.

I principi dell’architettura a servizi

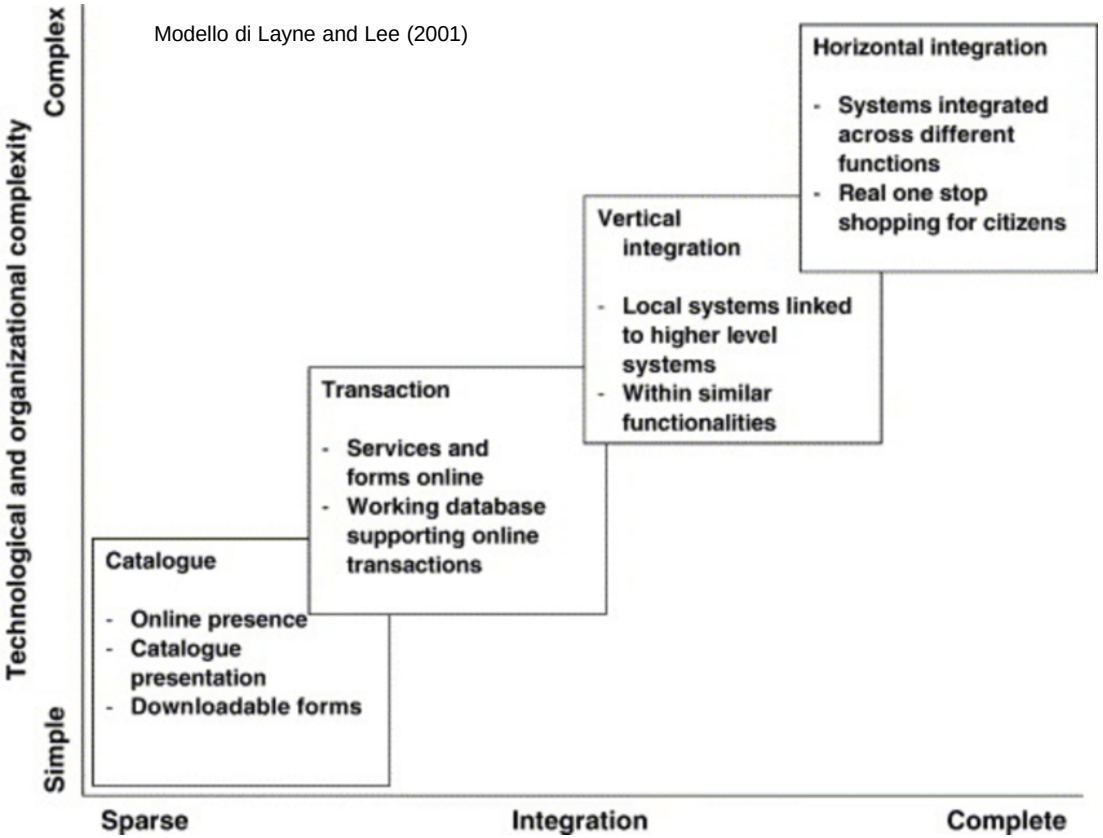
- ***Distributed Computing***
  I servizi sono rappresentati come componenti specializzati distribuiti in rete. Ogni servizio processa l’input che gli viene eventualmente fornito e elabora un output
- ***Accoppiamento debole (Loose Coupling)***
  I servizi comunicano tra loro nascondendo i dettagli implementativi. Una misura dell’accoppiamento tra due sistemi è rappresentata dal numero di cambiamenti che uno qualsiasi dei due sistemi può sopportare senza che la loro interconnessione venga interrotta. Alcuni dei vantaggi principali dell’accoppiamento debole sono la possibilità di isolare meglio i problemi quando si verificano e quello di sostituire un servizio con un altro senza riscrivere l’intera applicazione
- ***Interoperabilità***
  I servizi sono in grado di cooperare tra loro, indipendentemente dalla tecnologia utilizzata per costruirli
- ***Trasparenza di rete***
  È possibile utilizzare un servizio indipendentemente da dove esso sia fisicamente localizzato sulla rete
- ***Asincronismo***
  Un servizio è in grado di utilizzarne un’altro inviando alle sue interfacce pubbliche la richiesta di elaborazione, disconnettersi e ricevere successivamente la notifica dell’avvenuta elaborazione con l’eventuale output
- ***Trasparenza rispetto al vendor*** (e quindi utilizzo di Standard riconosciuti)
  L’interoperabilità, l’accoppiamento debole e la trasparenza di rete sono possibili solo se i servizi usano metodi standard per comunicare tra loro. L’unica cosa che necessita di essere definita e standardizzata è l’interfaccia, mentre l’implementazione può essere tranquillamente proprietaria.
- ***Separation of Concerns***
  Rappresenta la separazione della logica di business dalla logica dei computer. L’informatica è un mezzo, non un fine e il business, che invece è l’obiettivo, deve essere in grado di evolvere senza vincoli tecnologici.

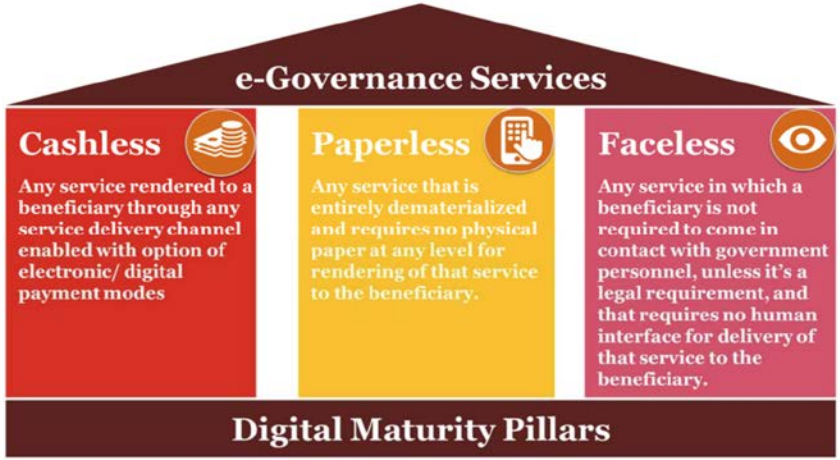
I principali servizi nella PA

- G2G (Government to Government)
  - Linee guida sull’interoperabilità
  - Linee guida sulla sicurezza dell’interoperabilità
- G2C (Government to Citizens)
- G2B (Government to Business)
  - Linee guida sul procurement

Modelli di maturità dell'e-gov

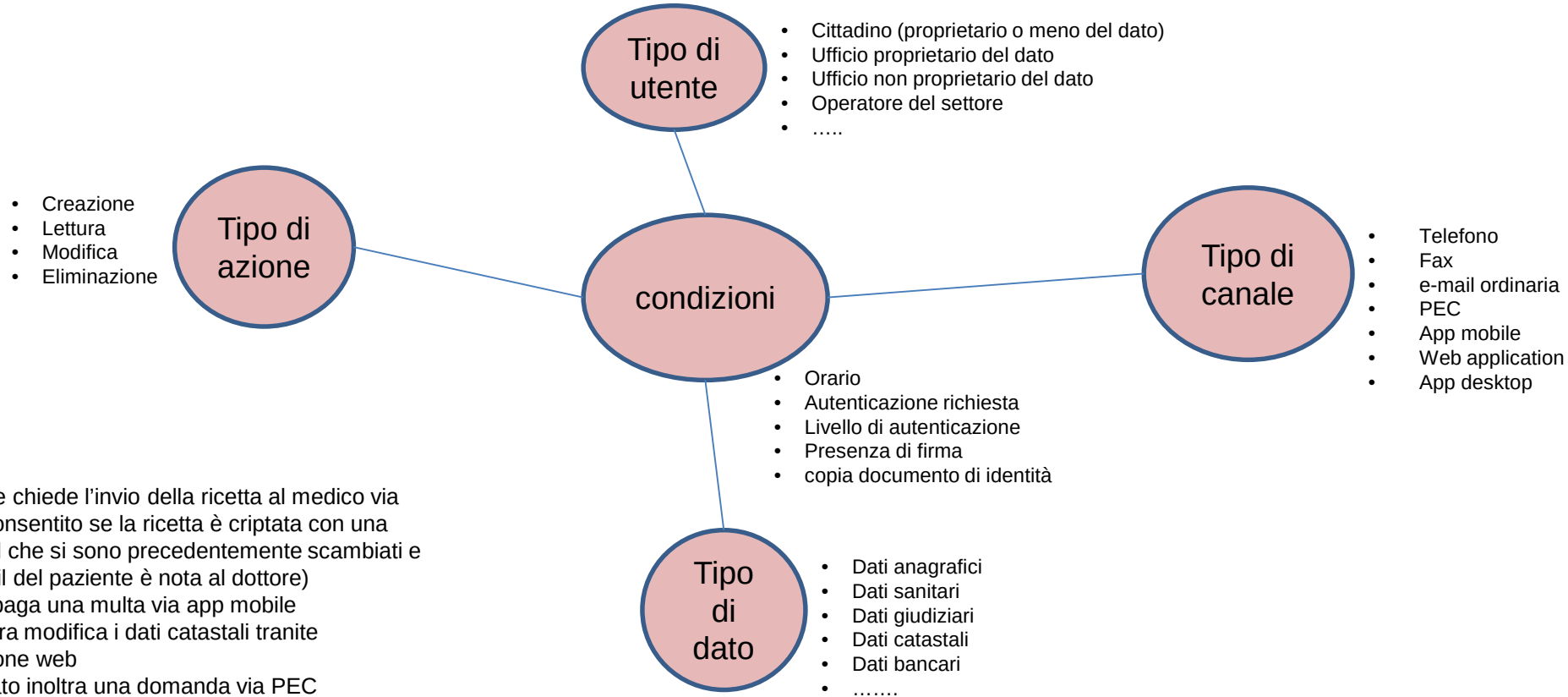
Modello di Layne and Lee (2001)





- 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

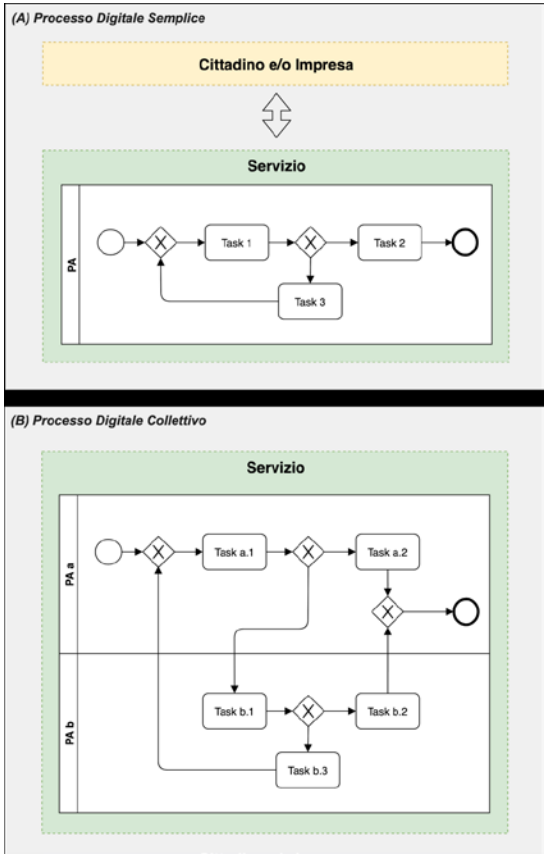
I servizi verso il Cittadino (G2C)

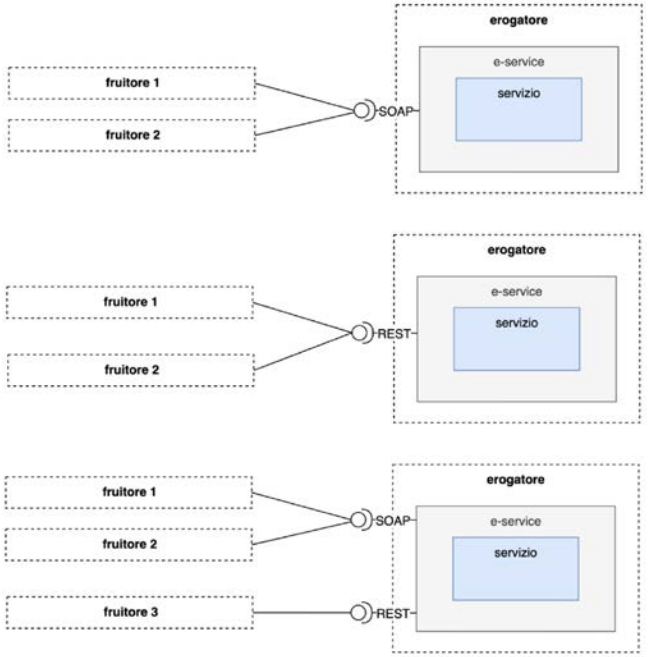


Esempi:

- 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 tranite applicazione web
- Il candidato inoltra una domanda via PEC

I servizi della PA verso se stessa (G2G)





Linee guida AGID sull'Interoperabilità

I servizi verso le imprese (G2B)

OPEN DATA

acquistinretepa.it

mercato elettronico della pubblica amministrazione

pagoPA

QUALIFIED TRUST SERVICE PROVIDER

SUAP Sportello Unico Attività Produttive

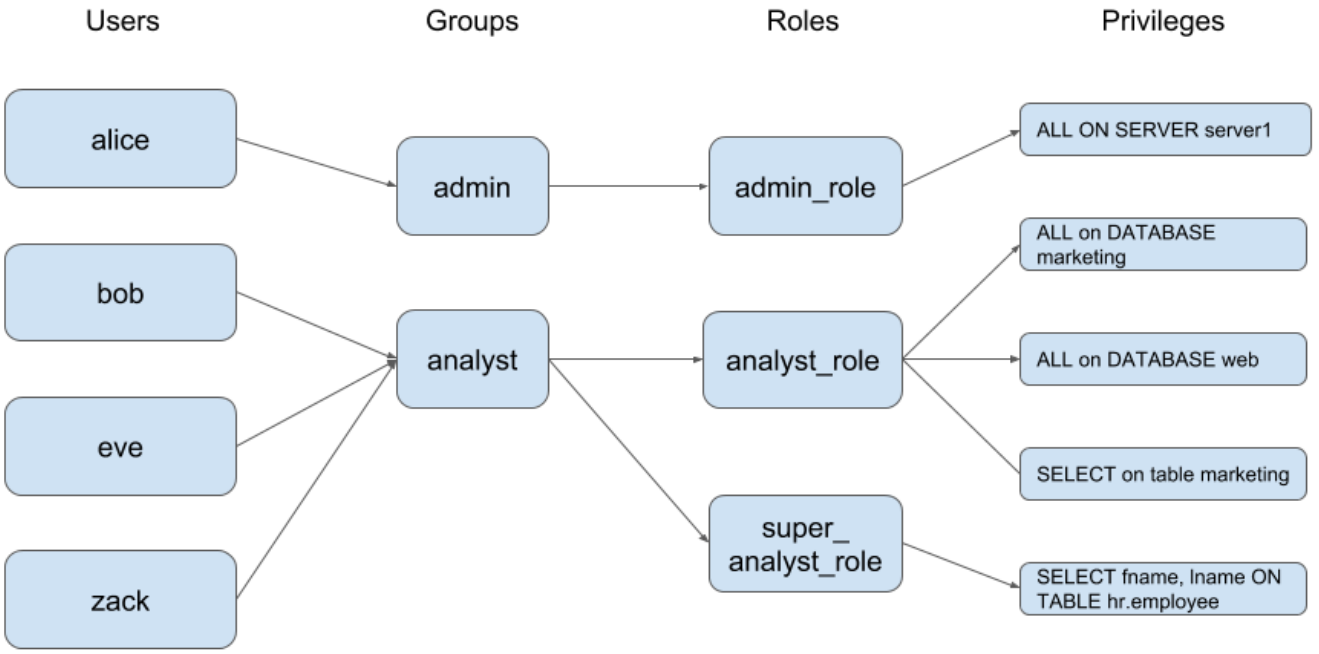
La sicurezza nei servizi

- 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

La sicurezza nei ruoli

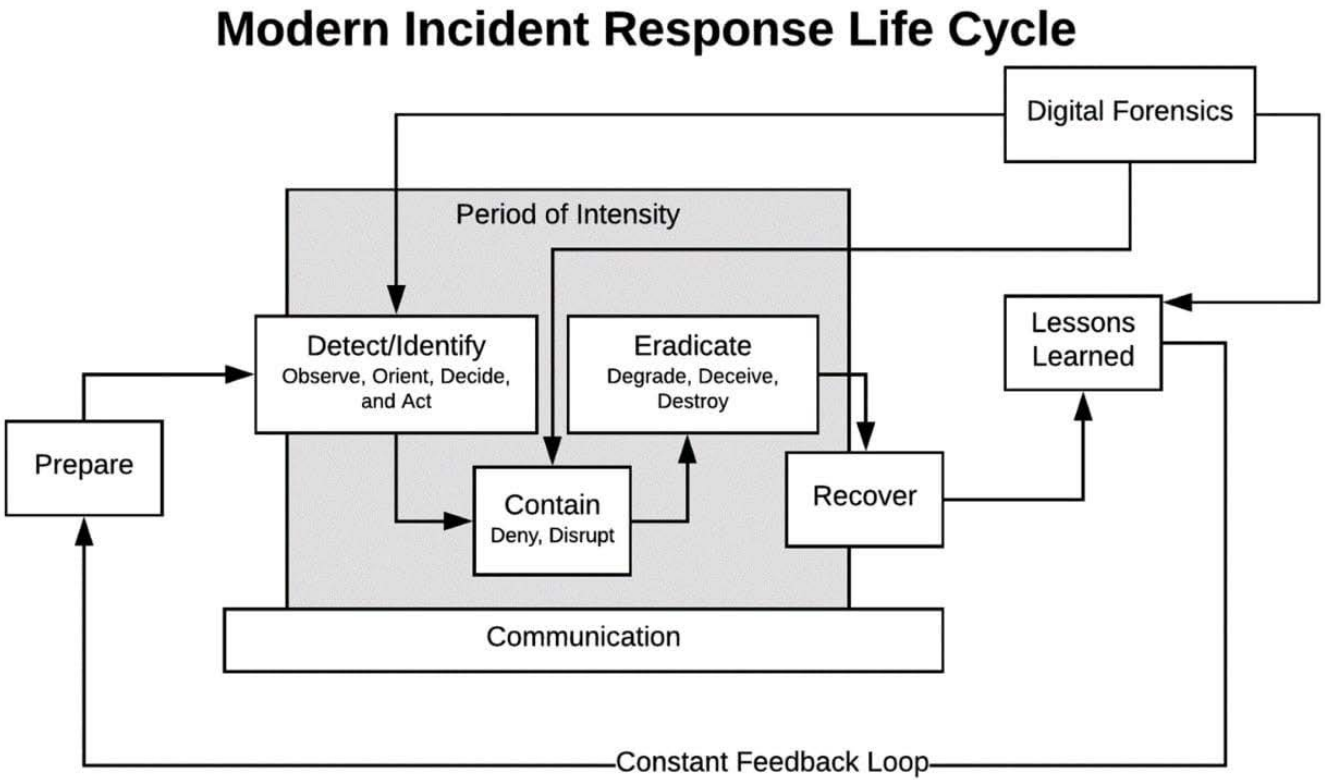
- Identificare i responsabili degli uffici e dei servizi
- Identificare i responsabili dei procedimenti
- Identificare i responsabili dei processi
- Identificare i responsabili dei contratti
- Identificare i responsabili dei progetti
- Identificare l’ambito di responsabilità e le competenze per ogni singolo ufficio
- Assegnare ruoli e responsabilità alle singole persone accertandosi che ognuno abbia solo quelli necessari alle proprie mansioni da svolgere
- Identificare i ruoli applicativi
- Utilizzare il meccanismo RBAC per fare il mapping tra ruoli organizzativi e ruoli applicativi
- Associare utenti a ruoli

RBAC (Role Based Access Security)



La gestione degli incidenti

Obiettivo : assicurare un approccio coerente ed efficace per la gestione degli incidenti relativi alla sicurezza delle informazioni, incluse le comunicazioni relative agli eventi di sicurezza ed ai punti di debolezza



Imprese, PA e perimetro di sicurezza

Introdotto dal **decreto-legge 21 settembre 2019, n. 105** convertito con modificazioni dalla L. 18 novembre 2019, n. 133 (in G.U. 20/11/2019, n. 272) «al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attivita' civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale».

1. Stabilire cosa sta dentro e cosa sta fuori
2. Fare la lista di chi sta dentro e aggiornarla con continuità
3. Stabilire a che tipo di obblighi deve ottemperare chi sta dentro
4. Cosa succede alla filiera di produzione? Che succede quando «chi sta dentro» comunica/scambia dati con «chi sta fuori»?
5. Chi controlla? -> audit e assessment, certificazioni (?)

L’Agenzia per la Cybersicurezza Nazionale (ACN)

ha personalità giuridica di diritto pubblico ed è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria

- coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale
- realizzazione di azioni comuni dirette ad assicurare la sicurezza e resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle PA, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore

Grazie!

Alessandro Sinibaldi

alessandro.sinibaldi@agid.gov.it