UNIBO
Gestione dei rischi integrata e conformità

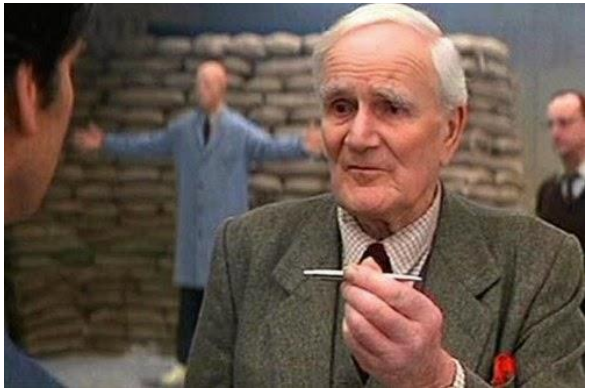
Andrea Foschi
Net Studio S.p.A.
13/12/2017

AGENDA

1	**Contesto di riferimento**
2	Approccio alla sicurezza & Compliance
3	Analisi dei rischi
4	ISO27001 e ISO27002
5	Conclusioni

IL PARADIGMA DELLA SICUREZZA NEGLI ANNI

Anni 60



2015

“..oso dire che faccio molti più danni io, con il mio portatile in pigiama seduto davanti alla prima tazza di Earl Grey, di quanti ne fai tu in un anno sul campo…”

LA SICUREZZA AD OGGI

Le minacce dovute ad attacchi volontari stanno sempre più aumentando affiancando alle da logiche di attacchi massivi le logiche mirate e personali (es. Social Engineering)

Ora come non mai il crimine informatico ha un ben preciso obiettivo : **quello economico**. Meno rumore per una pericolosità decisamente maggiore

Non vengono coinvolti "solo" i dati, le minacce riguardano anche aspetti infrastrutturali critici, quali rete elettriche, gasdotti, sistemi idrici, ecc.

In questo scenario spesso si sfrutta anche l'opportunità : **il più vulnerabile** (a volte per arrivare ad altri)

Sempre più si richiamano le aziende ad una responsabilità "sociale" condivisa : "…il problema non è più solo mio"

I GRANDI PERICOLI

New York, 13 feb 2013. Il Presidente Americano ha firmato l'ordine esecutivo sulla sicurezza informatica, sottolineando che gli attacchi dei pirati informatici "rappresentano una minaccia in rapida crescita"

l Decreto invita a partecipare, in modo 'volontario', all'azione di contrasto al crimine informatico che potrebbe riguardare le **infrastrutture critiche**, dall'**energia elettrica** agli **oleodotti**, ai **sistemi idrici**

Il principio importante che emerge, forse per la prima volta in modo così forte, è quello della "Responsabilità Sociale nella Sicurezza Informatica" che tutti devono sostenere.

LA QUOTIDIANITÀ

Se i grandi rischi sono "statisticamente" **meno probabili** (ma con maggiori impatti) , è la quotidianità a portarci un insieme di rischi (ad impatti meno rilevanti) ma invece **assai probabili**

- Non rare le azioni dolose apportate da persone molto vicini alle organizzazioni, spesso avvantaggiate dalla conoscenza del contesto (asset e vulnerabilità) e dalle facili opportunità

- Non sempre i pericoli sono legati ad azione dolose e volontarie; altrettanto pericolosa è la non corretta gestione dell'elevata complessità tecnologica (sempre più in ascesa).

SOCIAL ENGINEERING

Tradizionalmente, il mondo della sicurezza dei sistema si concentra soprattutto sui metodi utilizzati per verificare le minacce, spesso attraverso la valutazione delle stesse vulnerabilità

Questo metodo è principalmente tecnologico

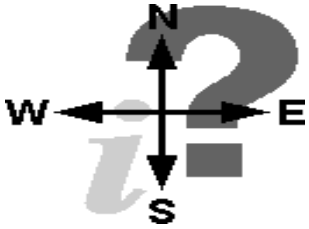
Tuttavia, un sistema informativo non è costituito soltanto da fattori tecnologici, ma soprattutto fattori umani.

E' necessario approccio alla sicurezza a più livelli considerando il Social Eng. come una potenziale minaccia, concependo quindi contromisure di sicurezza anche in tal senso

Social Engineering può essere definita come l'arte e la scienza di ottenere informazioni attraverso tecniche d'inganno, facendo leva sui comportamenti della psicologia umana di base

L'IMPORTANZA E L'AUMENTO DELL'INFORMAZIONE

L'informazione è oggi un elemento "cruciale" per poter svolgere qualsiasi tipo di attività; tutte le Organizzazioni trattano oramai un numero di informazioni che è aumentato in modo esponenziale nel tempo … forse fin troppe.



E' pertanto cresciuta la consapevolezza di quanto l'informazione (*parte degli Asset "intangibili" di ogni Organizzazione*) siano un **valore strategico**

La distruzione o la divulgazione non consentita di una informazione di business produce sempre e comunque un danno all'azienda.

I 3 paradigmi

- **Smart production**: nuove tecnologie produttive che creano collaborazione tra operatore, macchine e strumenti.
- **Smart services**: tutte le “infrastrutture informatiche” e tecniche che permettono di integrare fra sistemi e aziende (fornitore – cliente)
- **Smart energy**: sistemi più performanti riducendo gli sprechi di energia secondo i paradigmi tipici dell'Energia sostenibile.

Industry 4.0 si fonda sui sistemi ciberfisici (CPS) ovvero sistemi fisici **strettamente connessi con i sistemi informatici** e che possono interagire e collaborare con altri sistemi CPS (decentralizzazione e collaborazione tra i sistemi)

IOT (INTERNET OF THINGS)

Gli oggetti (le "cose") si rendono riconoscibili e acquisiscono intelligenza grazie al fatto di poter comunicare dati su se stessi e accedere ad informazioni aggregate da parte di altri.

Per "cosa" si può intendere : dispositivi, apparecchiature, impianti e sistemi, materiali e prodotti tangibili, opere e beni, macchine e attrezzature.

L'obiettivo dell'internet delle cose è far sì che il mondo elettronico tracci una mappa di quello reale, dando un'identità elettronica alle cose e ai luoghi dell'ambiente fisico. Gli oggetti e i luoghi muniti di sistemi di identificazione (etichette, Rfid, Codici QR, ecc.) comunicano informazioni in rete o a dispositivi mobili.

INDUSTRY 4.0 E IOT IN OTTICA DI SICUREZZA

Industry 4.0 e IOT : due chiavi di lettura delle medesime opportunità... ma dei medesimi problemi

Maggiore volumi di dati trattati

Scambio ed elaborazione automatico di dati

Maggior numero di device (punti di ingresso) e complessità

Minor presidio e controllo umano

Maggiori vulnerabilità e Rischi

CONFORMITÀ DI LEGGE VS SICUREZZA

Art. 32 - Sicurezza del trattamento (reg. UE 2016/679)

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del **contesto e delle finalità del trattamento**, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto **misure** tecniche e organizzative **adeguate** per garantire un livello di sicurezza **adeguato** al **rischio**, che comprendono, tra le altre, se del caso:

   a) la capacità di assicurare su base permanente la **riservatezza**, **l'integrità**, **la disponibilità** e la resilienza dei sistemi e dei servizi di trattamento;
   b) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
   c) una procedura per **testare, verificare e valutare** regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Nel valutare **l'adeguato livello di sicurezza**, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, ……..

rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche

misure tecniche e organizzative **adeguate** per garantire un livello di sicurezza **adeguato** al **rischio**

Assicurare la **riservatezza**, **l'integrità**, **la disponibilità**

testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative

l'adeguato livello di sicurezza

Rischi: dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso

SOLO COMPLIANCE ?

- Un azienda che ha la necessità di implementare soluzioni di conformità legislative sul fronte della sicurezza delle informazioni (es. GDPR) avrà, quasi sicuramente, anche problematiche di sicurezza di Business.
- Nell'ambito della compliance non esiste solo l'aspetto del GDPR collegato alla sicurezza delle informazioni ... non ultimo il D.Lgs 231 (ma anche altro).
- I costi di adeguamento ad aspetti di conformità (es. PIA e AR per GDPR; Protocolli 231, ecc) spesso non hanno ordini di grandezza differenti rispetto ad affrontare il tema della sicurezza delle informazioni in modo più esteso.
- Include valenze anche di Business nella gestione della sicurezza delle informazioni rende più efficace anche la parte di compliance.

AGENDA

1 Contesto di riferimento

2 Approccio alla sicurezza & Compliance

3 Analisi dei rischi

4 ISO27001 e ISO27002

5 Conclusioni

GARANTIRE LA SICUREZZA

Garantire la sicurezza delle proprie informazioni significa quindi garantire il **proprio patrimonio** da potenziali **danni** … anche se a riguardo le imprese maggiormente sensibili sono proprio quelle **che hanno subito rilevanti perdite di dati** e, di conseguenza, gravi perdite economiche

Questo accade perché le imprese spesso tendono a sottovalutare i rischi connessi ad una non corretta gestione e tutela delle informazioni

Il tema della "Security" non passa solo dal governare e tutelare il proprio Sistema Informativo bensì dal:

- *conoscere l'intera "mappa" delle informazioni aziendali (cartacee, informatiche, vocali, audio, video, ecc…)*
- *comprendere il valore delle diverse tipologie di dati gestiti*
- *prevedere opportune azioni a tutela degli stessi in base ad una corretta analisi dei rischi*

E SE NON CI SUCCEDE NULLA ?

La scarsa propensione al rischio fa si che le funzioni che si occupano di IT e Security in azienda abbiano spesso problemi a giustificare le spese inerenti la sicurezza delle informazioni

a peggiorare questa considerazione il fatto che la dimensione economica della sicurezza si fonda su una regola apparentemente poco logica contro la quale i CISO e CIO devono lottare quotidianamente :

più un investimento in sicurezza è adeguato
meno visibili e misurabili sono i suoi risultati !

LA MISURA DELL'EFFICACIA

Si può dare una metrica a quello che potenzialmente potrebbe accadere (analisi dei rischi)…

ma misurare ciò che "realmente" non è accaduto per via di una adozione di corrette contromisure di sicurezza … beh è estremamente difficile

E quindi non rimane che affidarsi a **metodi** ed adeguati strumenti (di analisi, organizzativi, tecnici, ecc.)…e misurare la loro efficacia nel tempo

In breve l'unica strada è **Governare la Sicurezza** in tutti i suoi processi fondamentali e in tutte le dimensioni in modo integrato

LA SICUREZZA E LE DOMANDE DA PORSI

Si parla di sicurezza tutte le volte che esiste un bene (Asset) da proteggere.

Questo vale sia per gli asset tangibili sia per quelle **intangibili**…come le **informazioni**

Quindi la prima domanda da porsi è sempre :

- ✓ **Cosa devo proteggere ... e quanto vale** ? (asset)

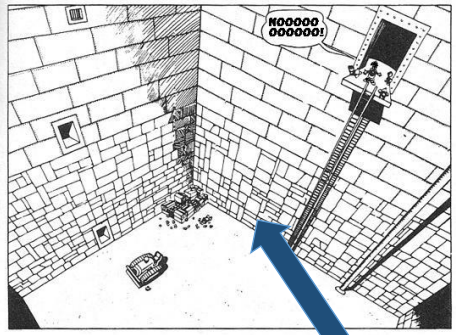
Seguono immediatamente :

- ✓ Perché e da chi lo devo proteggere ? (vulnerabilità e minacce)
- ✓ Come lo posso proteggere ? (Contromisure)

ELEMENTI DELL'ANALISI DEL RISCHIO

ASSET

AGENTI



RISCHIO

MINACCIA

VULNERABILITA'

CONTROMISURE

IL VALORE DELL'INFORMAZIONE : INTERNO ED ESTERNO

Ma qual è il valore di un asset informativo ?

- Valore interno alla mia organizzazione
- Valore per il mondo esterno

Entrambi, in maniera differente, hanno una influenza sull'analisi e la gestione dei rischi.

Il valore dell'asset informativo per il mondo esterno può essere :

- intrinseco all'informazione stessa
- determinato dalla sua facile disponibilità.

IL VALORE DELL'INFORMAZIONE NEL TEMPO

Il valore di una informazione non è statico nel tempo

- Ciò che oggi non vale nulla nel futuro potrebbe avere un valore importante sia interno che esterno
- Ciò che oggi ha un valore rilevante nel futuro potrebbe non "servire" più a nessuno

Attenzione soprattutto al primo dei due punti…perchè non sempre è possibile prevedere l'evoluzione del valore di alcune informazioni !

In entrambi i casi gli aspetti di **riservatezza** sono i più rilevanti

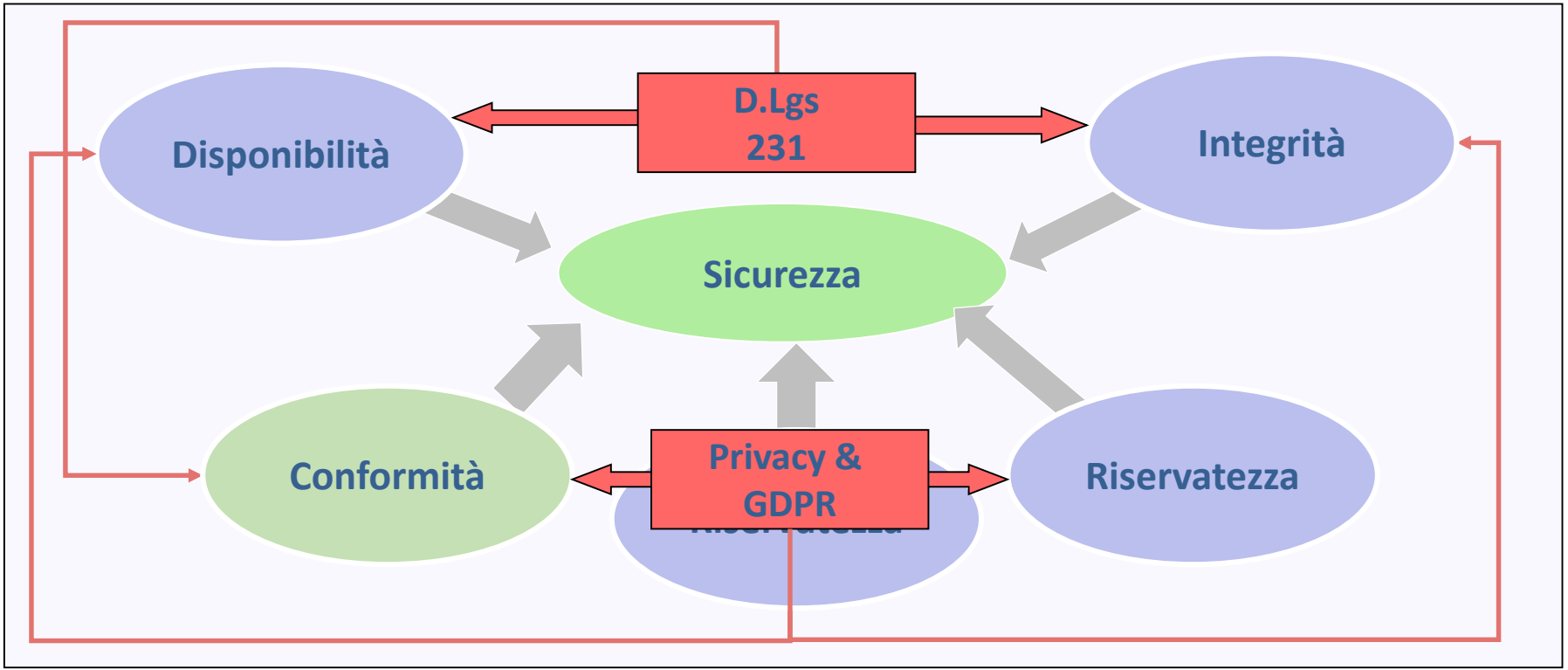
GLI ELEMENTI CARATTERISTICI

Gli elementi “caratteristici” di base della sicurezza dell’informazione potrebbero essere caratterizzati come:

- *la sua **riservatezza***
- *la **disponibilità** della stessa nel momento in cui serve*
- *la sua **integrità**, ovvero preservare il suo contenuto*
- *e forse anche altro….*

garantire tali “caratteristiche” significa non passare solo attraverso la tecnologia ed un Sistema di Governance interno ma anche e soprattutto attraverso la consapevolezza *e la competenza* di chiunque tratti l’informazione.

Modello R.I.D....e Conformità



AGENDA

1 Contesto di riferimento

2 Approccio alla sicurezza & Compliance

3 Analisi dei rischi

4 ISO27001 e ISO27002

5 Conclusioni

IL CUORE PROGETTUALE

L’analisi dei rischi rappresentano è il cuore di un qualsiasi progetto sulla sicurezza delle informazioni.

L’analisi dei rischi rappresentano, anche in termini di sforzi e risultati, l’80% di tutto il progetto.

Solo una corretta analisi dei rischi consente di sviluppare una conseguente gestione dei rischi ed un piano della sicurezza efficiente e **adeguato**.

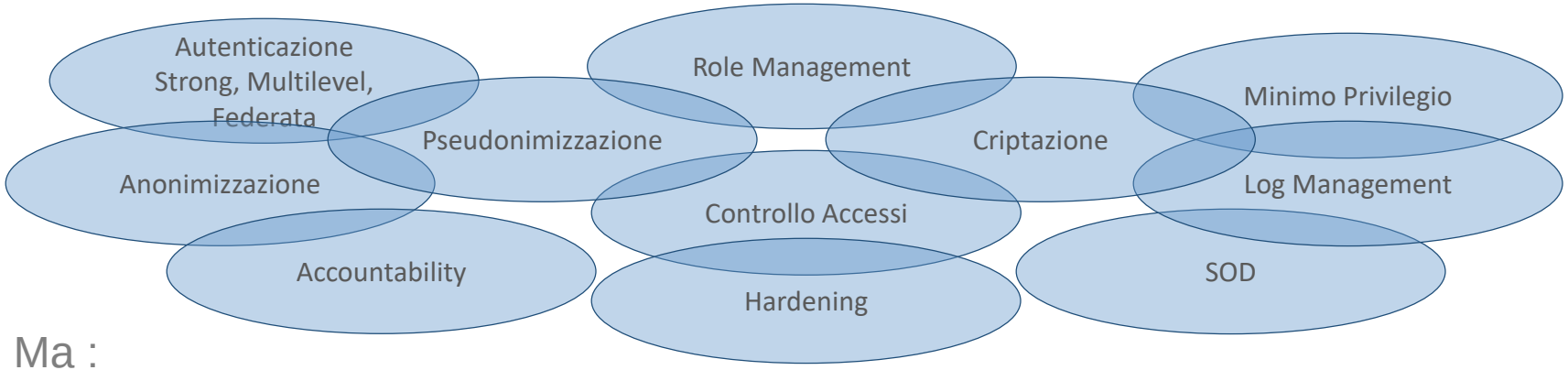
A COSA SERVE L'ANALISI DEI RISCHI

L'analisi dei rischi è un processo per identificare e valutare il danno causabile da minacce e vulnerabilità in combinazione. Serve inoltre a giustificare le contromisure, a valutare che siano efficaci, di costo ragionevole, effettivamente applicabili al contesto e in grado di rispondere in tempo alle minacce.

Permette anche di assegnare una **priorità di trattamento dei rischi** e consentire di determinare l'investimento necessario all'azienda per proteggersi da essi.

APPROCCIO A «REQUISITI MINIMI»

In un approccio molto semplificato potrei concentrarmi direttamente sulle potenziali vulnerabilità e relative contromisure



Ma :

- Le misure identificate potrebbero essere non idonee
- Non riesco a dimostrare una correlazione fra rischio e controlli
- Potrei implementare contromisure eccessive

Attenzione all'effetto "misure minime di sicurezza" del Dlgs 196/03

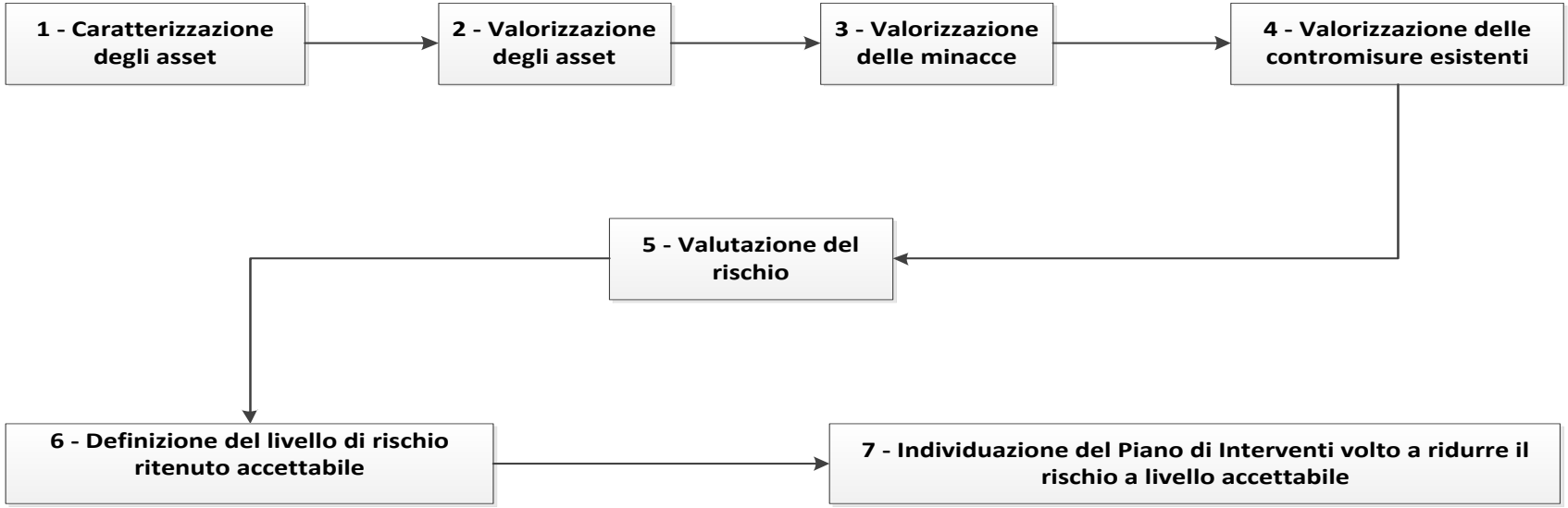
GLI OBIETTIVI DELL'ANALISI DEL RISCHIO

Gli obiettivi principali dell'analisi del rischio sono:

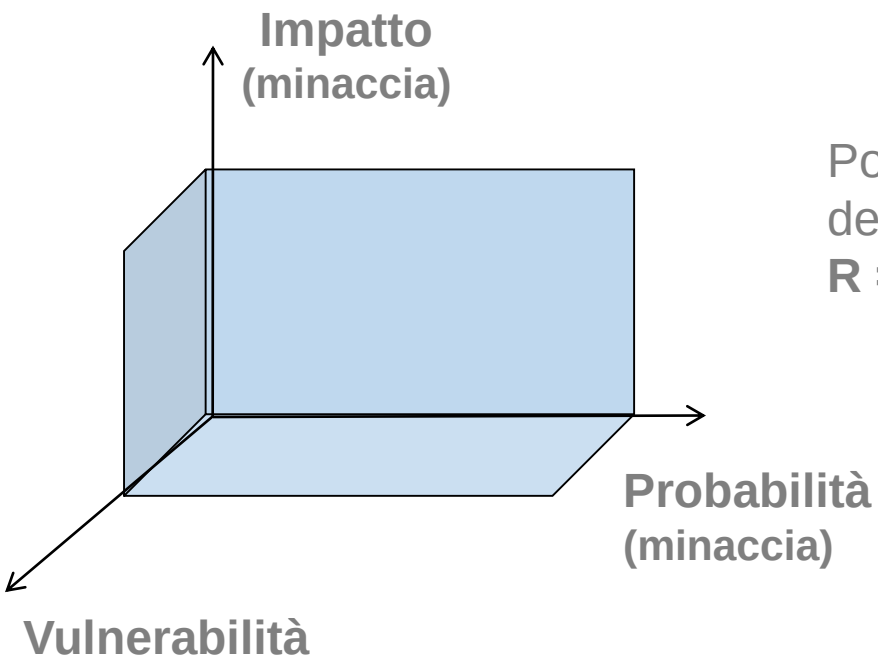
- Identificarlo
- Quantificare l'impatto
- Permettere di individuare il bilanciamento ottimale tra l'impatto e il costo delle misure di sicurezza necessarie a ridurlo

Nell'analisi del rischio il costo delle misure di sicurezza viene confrontato con il relativo costo delle perdite attese, fornendo di conseguenza anche un'analisi costi-benefici.

FASI DELL'ANALISI DEL RISCHIO



CONCETTO DI RISCHIO



Possibilità di subire perdite al seguito del verificarsi di un evento dannoso

R = f (I, P, V)

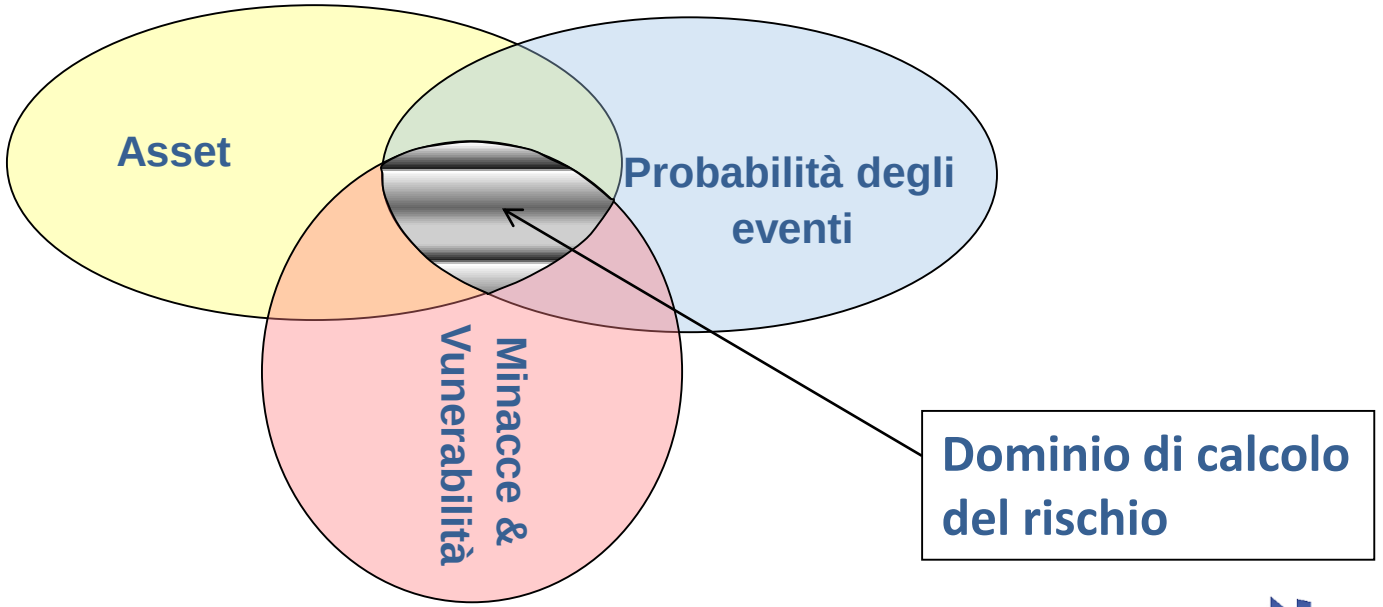
ANALISI DEI RISCHI : LE DOMANDE

L’analisi dei rischi, in estrema sintesi, si sostanzia nelle risposte alle seguenti domande:

- Cosa potrebbe accadere? (qual è la minaccia?)
- Quale danno potrebbe causare (qual è l’impatto?)
- Quanto spesso può accadere? (qual è la frequenza?)

ANALISI DEI RISCHI: DOMINIO DI APPLICAZIONE

Focalizzare l'analisi sulle risorse più critiche ai fini del conseguimento della missione aziendale; una precisa definizione del dominio di applicazione consente una riduzione dei tempi e dei costi.



ANALISI DEI RISCHI : LE MINACCIE

Natura: **Eventi Naturali, Eventi non Intenzionali, Eventi Industriali, Eventi Dolosi**

L'insieme delle minacce (uso improprio di risorse, simulazione d'identità, introduzione di software dannoso, gusti, ecc..) è lo stesso per tutti i sistemi; ciò che cambia è la probabilità di accadimento.

Esempio: la minaccia terremoto insiste sia un sistema ubicato a Los Angeles sia su un sistema ubicato a Roma, la probabilità di accadimento è però diversa.

La frequenza di accadimento della minaccia spesso (ma non sempre) resta inalterata. Le misure di sicurezza riducono la vulnerabilità, quindi l'impatto, relativa ad una certa minaccia, ma a volte hanno efficacia anche sulla frequenza con la quale si manifesta.

ANALISI DEI RISCHI : LE VULNERABILITÀ

Rappresentano una misura del grado di esposizione al rischio del sistema.
Per provocare un danno una minaccia deve trarre vantaggio da una vulnerabilità del sistema.

Il livello di vulnerabilità può essere ridotto attraverso l'implementazione di opportune misure di sicurezza.

La vulnerabilità non può mai essere ridotta a zero, perché
le misure di sicurezza presentano loro stesse delle vulnerabilità.

GESTIONE DEL RISCHIO

L’attività di Gestione del Rischio (Risk Management) ha l’obiettivo di definire le opportune strategie per ridurre i rischi ad un livello accettabile.
E’ essenzialmente funzione di:

- missione aziendale
- conformità a leggi e norme
- disponibilità economica

Rappresenta un giusto compromesso tra il “costo della sicurezza” e i “costi della non sicurezza”

ANALISI DEI RISCHI : CONCLUSIONI

E’ importante che l’analisi sia portata avanti da un gruppo di lavoro (meglio interdisciplinare composto dagli “owner” delle informazioni) dove sia possibile mettere a confronto le diverse esperienze e sensibilità.

In questo modo la mancanza di “oggettività” (base statistica) viene sopperita da una ponderata visione degli asset aziendali (informazioni), dei pericoli a cui sono sottoposti e delle loro reali vulnerabilità.

ANALISI DEI RISCHI : PERCHÉ VA FATTA …

I sistemi di analisi dei rischi difficilmente fanno emergere vulnerabilità e minacce non già note nell'organizzazione

E' difficile ottenere un vero bilanciamento rischi-contromisure dal punto di vista quantitativo (€)

Pone le fondamenta per il rispetto dei principi di Accountability

(Rischi vs Contromisure)

Consente il monitoraggio dell'efficacia del SIGSI nel tempo

Consente di impiegare in maniera "equilibrata" e consapevole i limitati budget aziendali

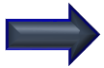
Il vero valore è quello di fare una analisi completa e condivisa di tutte le "variabili" in gioco

AGENDA

1 Contesto di riferimento

2 Approccio alla sicurezza & Compliance

3 Analisi dei rischi



4 ISO27001 e ISO27002

5 Conclusioni

“HOMEMADE” O ISO27001

E’ possibile adottare proprie metodologie e approcci progettuali anche creativi, fermo restando il rispetto e l’esecuzione delle principali fasi con una cura particolare alla parte di analisi dei rischi.

La ISO27001 per “non è una norma di certificazione” ma una **metodologia internazionale e consolidata** utile per sviluppare un progetto sulla sicurezza delle informazioni senza lasciare nulla al caso.

L’adozione di un “metodo” ISO27001 rende la certificazione una pura formalità.

ISO27001:2013

L'obiettivo della norma ISO27001:2013 è quello di "fornire un modello per la progettazione e realizzazione di tutti gli aspetti di funzionamento, monitoraggio, revisione, mantenimento e miglioramento di un **S**istema di **G**estione della **S**icurezza delle **I**nformazioni (SIGSI).

L’adozione di un sistema di Gestione della Sicurezza delle informazioni dovrebbe essere una decisione strategica dell’azienda.

La progettazione e la realizzazione di un SGSI di un azienda è influenzata dai suoi obiettivi strategici, dai requisiti di sicurezza, dall’organizzazione ed i processi adottati e dalla sua dimensione.

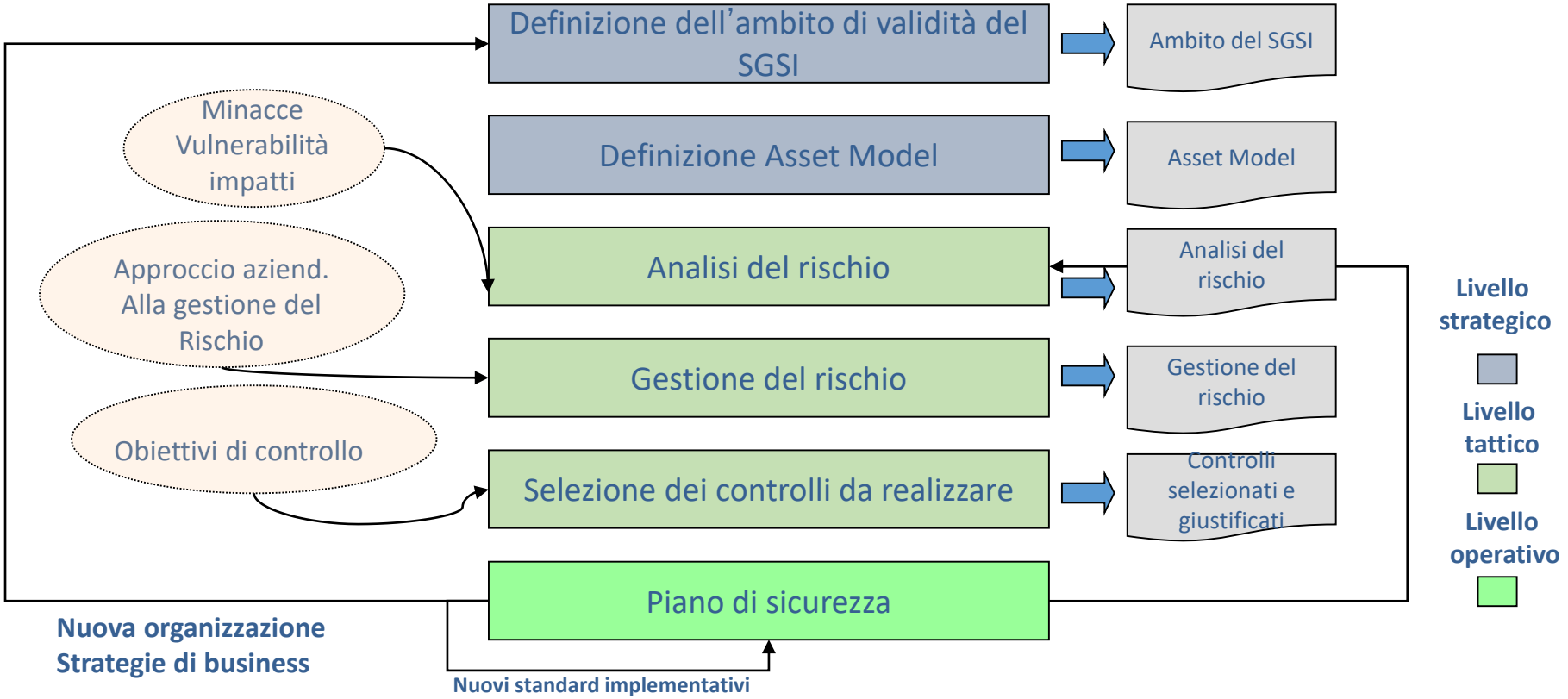
Lo standard ISO 27001 prevede due macro fasi distinte:

L'analisi del rischio, che ha come scopo quello di fornire una serie di raccomandazioni riguardanti la gestione della sicurezza dell'informazione (***ISMS***-*Information Security Management System*) per garantire la possibilità di organizzare tale gestione su una base comune e soprattutto la più possibile oggettiva e condivisa.

La gestione del rischio, che mette a disposizione le specifiche per progettare, attuare, gestire, monitorare, revisionare ed aggiornare un **ISMS** correttamente documentato e orientato ai rischi di Business dell'azienda.

Si identificano le decisioni che l'azienda deve intraprendere in funzione del rispetto dei tre requisiti della sicurezza (riservatezza, integrità, disponibilità)

ANALISI E GESTIONE DEL RISCHIO IN AMBITO ISO 27001



ISO27002:2013

La norma ISO 27002:2013 è una raccolta di "best practices" che possono essere adottate per soddisfare i requisiti della norma ISO 27001:2013 (la norma ISO 27002:2013 non è certificabile in quanto si tratta di una raccolta di raccomandazioni)

- Politiche di Sicurezza
- Organizzazione della sicurezza
- Controllo e classificazione dei beni
- Gestione dei comportamenti delle risorse umane
- Sicurezza fisica e ambientale
- Gestione di comunicazioni e operazioni
- Controllo degli accessi
- Sviluppo e manutenzione di sistemi
- Monitoraggio e Gestione degli incidenti di sicurezza
- Gestione continuità operativa
- Conformità normativa

AGENDA

1 Contesto di riferimento

2 Approccio alla sicurezza & Compliance

3 Analisi dei rischi

4 ISO27001 e ISO27002

5 Conclusioni

IL SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI - SGSI

Obiettivo del SGSI (27001)

Insieme di regole e procedure per la progettazione e realizzazione di tutti gli aspetti di funzionamento, monitoraggio, revisione, mantenimento e miglioramento della Sicurezza delle Informazioni in azienda

Fasi

Analisi del rischio – Sicurezza delle informazioni

Gestione del rischio – Specifiche per un Sistema di gestione documentato e orientato ai rischi di business dell'azienda

Si identificano le decisioni che l'azienda deve intraprendere in funzione del rispetto dei requisiti della sicurezza (riservatezza, integrità, disponibilità…e altro) emersi da un'attenta analisi dei rischi

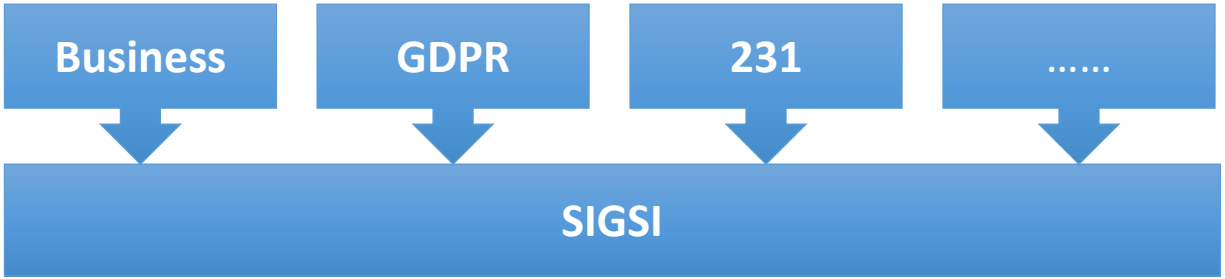
l'implementazione di un sistema di gestione integrato e completo sulla sicurezza (SGSI)
innalza il livello di protezione delle informazioni

APPROCCIO ALLA SICUREZZA

"Governare" la sicurezza significa prima di tutto avere la conoscenza di quello che può accadere e degli impatti che questo può provocare sulla nostra organizzazione sotto ogni punto di vista (business e compliance)

- metodologia
- organizzazione
- esperienza

giocano un ruolo **fondamentale**



E comunque meglio partire da metodologie e strumenti acquisiti e consolidati, adattandoli e contestualizzandoli alla nostra realtà (es. ISO27001) anche quando si tratta di coprire aspetti di conformità

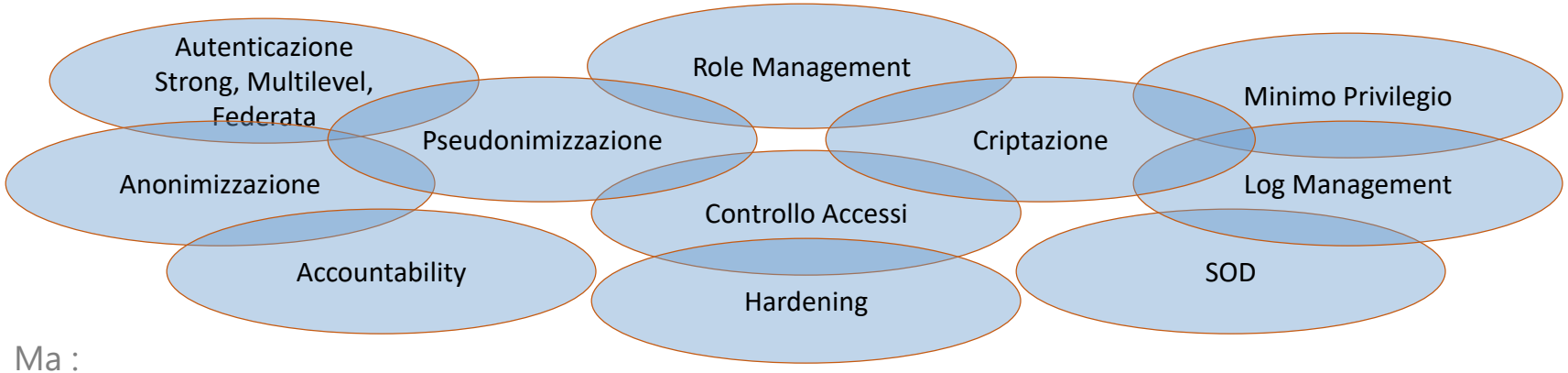
SOLUZIONI DI IDENTITY GOVERNANCE

In un approccio molto semplificato dove si ipotizza che:

mancanza di un controllo di sicurezza = vulnerabilità

È anche vero però che sicuramente …

potrei concentrarmi direttamente sulle contromisure….



Ma :

- Le misure identificate potrebbero essere non idonee
- Non riesco a dimostrare una correlazione fra rischio e controlli
- Potrei implementare contromisure eccessive

…sono tutte best practice alla base di un buon

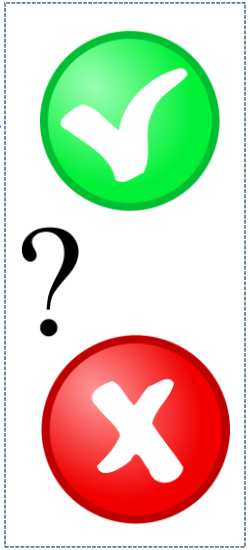
Attenzione all'effetto "misure minime di sicurezza" del Dlgs 196/03

In un mondo privo di identità….

Identità digitale

Controllo accessi
e autorizzazioni

Cosa posso fare?



Sono in regola ?

Identità e Anagrafe

Pubblica sicurezza

Non Governare le identità digitali e …tutto il mondo degli accessi logici …è come cercare di fare pubblica sicurezza in un mondo privo di Anagrafe & documenti di identità
(e tutta al gestione necessaria)

Q&A

NET studio