Presidenza del Consiglio dei Ministri
Scuola Nazionale dell'Amministrazione

LEZIONE WEBINAR DEL 31/03/2020

SICUREZZA INFORMATICA:
la gestione del rischio informatico
e la risoluzione degli incidenti

31 marzo 2020

Vincenzo G. Calabrò
Ministero dell'Interno
vincenzo.calabro@interno.it

who am i

Formazione

- laureato in ingegneria informatica (università la sapienza di roma) e sicurezza informatica (università di milano)
- specializzato in advanced cybersecurity (stanford university)
- certificato in cybersecurity engineering and software assurance e digital forensics (carnegie mellon university)

Esperienza professionale

- funzionario alla sicurezza cis (ministero dell'interno)
- consulente in sicurezza informatica e informatica forense
- professore a contratto di tecnologie per la sicurezza informatica
- relatore e autore sui temi della cybersecurity

Contatti

vincenzo.calabro@interno.it

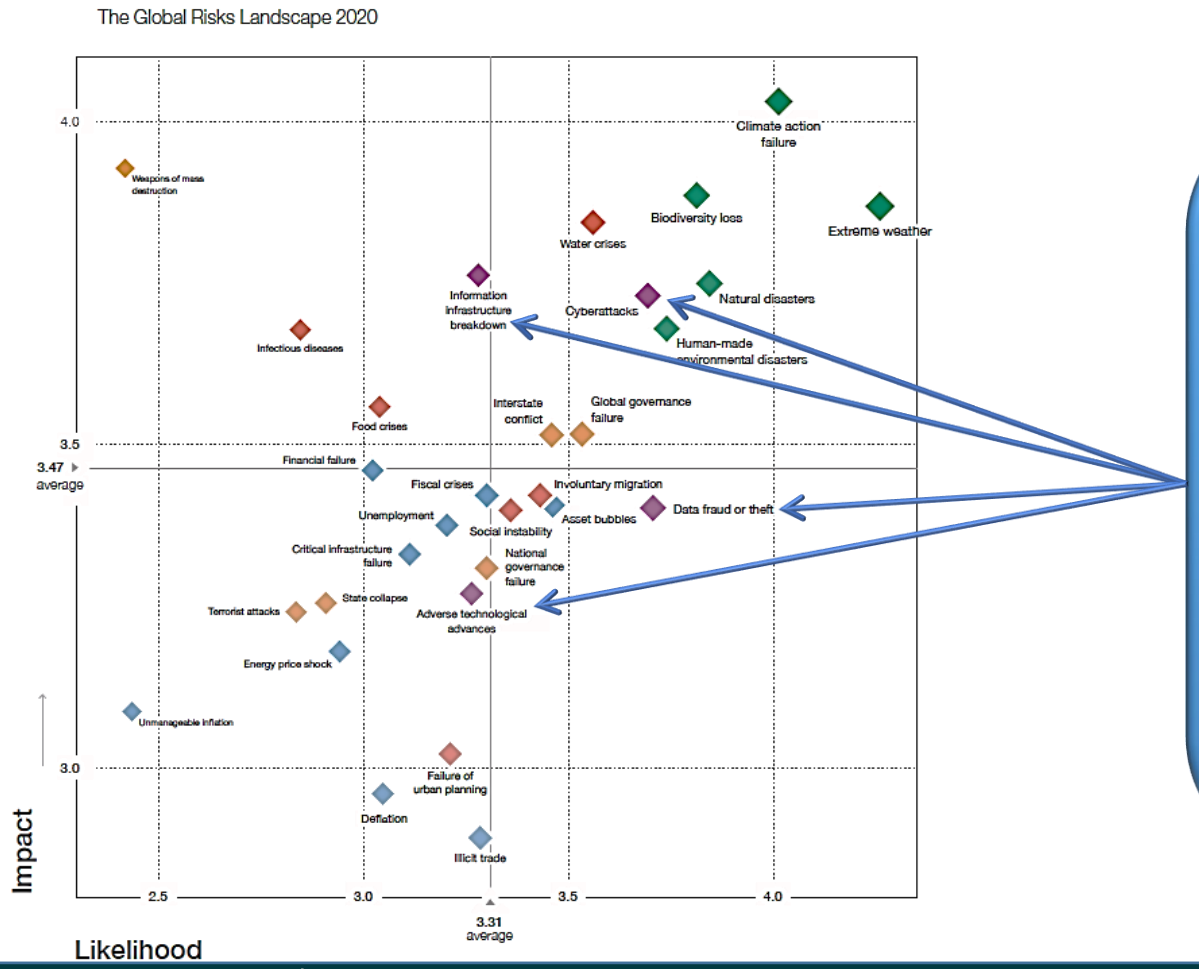
www.vincenzocalabro.it

LinkedIn vincenzocalabro.it

SICUREZZA INFORMATICA:
la gestione del rischio informatico e la risoluzione degli incidenti

- **Principi Generali**
  - Siamo sotto attacco?
  - Dalla Cyber Security alla Cyber Resilience
  - La Normativa di riferimento
  - Cyber Resilience Framework → Maturity Level
  - Gli Standard e le Linee Guida Internazionali
- **Costruire la Cyber Resilience Organizzativa**
  - La Resilienza Informatica
  - Le fasi del Resilience Framework dell'IT Governance
    - Gestire e Proteggere
    - Identificare e Rilevare
    - Rispondere e Ripristinare
    - Governare e Garantire
- **Conclusioni**

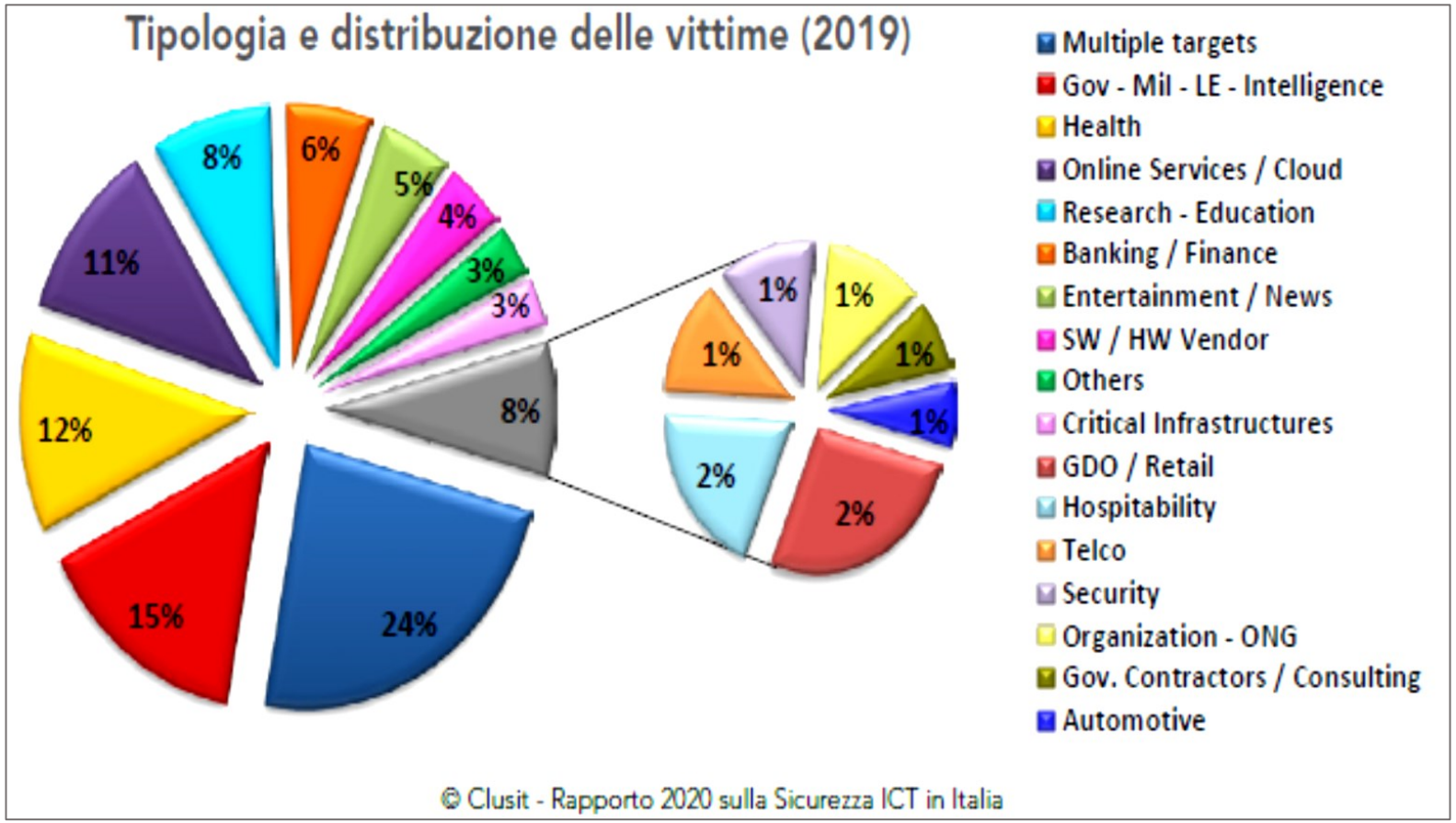
Perché abbiamo bisogno della sicurezza informatica?



Dalle violazioni dei dati e dal furto di identità all'interruzione delle operazioni e delle infrastrutture critiche, il Rapporto sui rischi globali del World Economic Forum 2019 classifica gli attacchi informatici tra i primi cinque rischi globali.

«La connettività digitale svolge un ruolo cruciale nel consentire l'innovazione e la prosperità in tutto il mondo, ma sempre più le minacce informatiche rappresentano un grave ostacolo al continuo percorso della società verso il progresso»

La Pubblica Amministrazione Italiana è sotto attacco?



«Il tema della sicurezza informatica è diventato cruciale per la pubblica amministrazione», anche perché va di pari passo con l'estensione e lo sviluppo della digitalizzazione dei servizi pubblici. Pertanto, per realizzare la completa trasformazione digitale della pubblica amministrazione, è necessario che il processo sia resiliente alle minacce digitali.

< Data breach >

la Repubblica

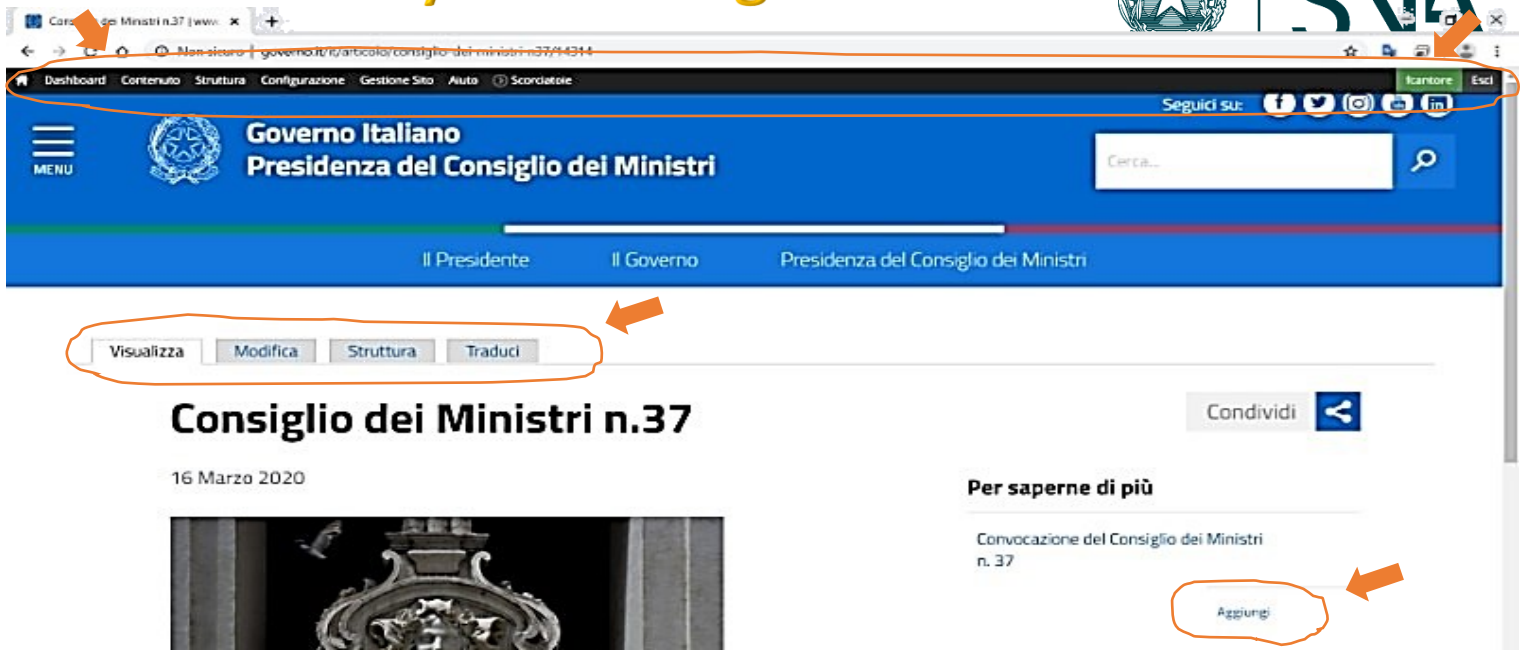
Cronaca

HOME POLITICA ECONOMIA SPORT SPETTACOLI TECNOLOGIA MOTORI TUTTE LE SEZIONI D REP TV

Furto di dati alla Pubblica amministrazione, hacker in manette

Operazione della polizia postale. L'uomo - originario del torinese e residente a Imperia - si sarebbe appropriato di centinaia di credenziali di accesso a dati sensibili e migliaia di informazioni private di cittadini. E avrebbe a sua volta organizzato - assieme a dei complici, denunciati - una banca dati online illegale consultabile a pagamento

< Security Misconfiguration >



< Phishing >

Italia Attualità

Temi Caldi Coronavirus - lo speciale Mappa dei contagi Guida al «Cura Italia» Aiutiamo I numeri utili

Pubblicità

23 dicembre 2019

Natale
Iban
Ing Bank
NoiPA
CONSOB

Salva Commenta

CYBER SICUREZZA

Truffa di Natale: hacker contro NoiPA, rubati stipendi e tredicesime a dipendenti pubblici

Operazione basata su tecniche di phishing, che riguarderebbe un numero non definito di dipendenti pubblici. Un furto che lascia spazio a molti interrogativi e al pesante dubbio di non poter recuperare il maltolto

< Remote access >

IL GAZZETTINO.it

Il telelavoro scatena gli hacker, quattromila attacchi via mail al giorno

NORDEST > TREVISO

Martedì 24 Marzo 2020 di Mattia Zanardo

Computer Emergency Response Team
Pubblica Amministrazione
CERT-PA

4.070

Segnalazioni pervenute dal 1.1.2015

SHODAN

191.050

Host con RDP open in Italia il 31.3.2020

Le possibili conseguenze di un incidente informatico?

INCIDENTE INFORMATICO

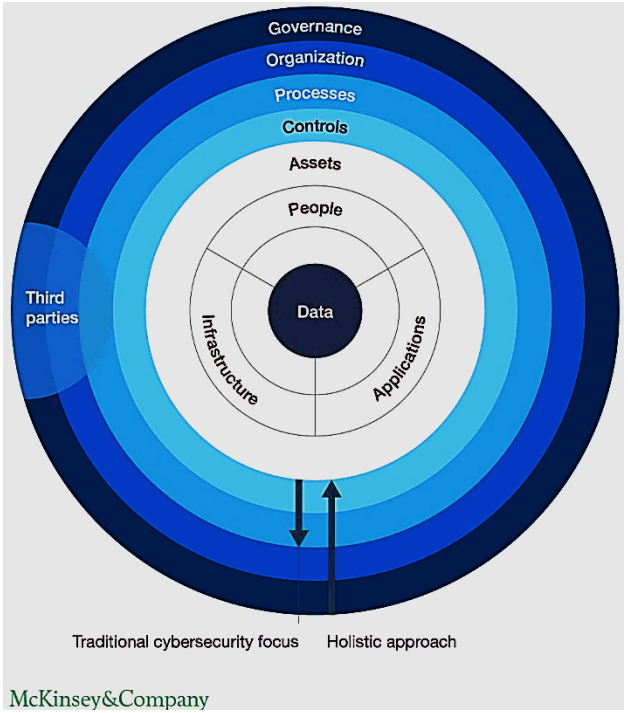
- un evento interno o avverso che può influire sulle risorse delle organizzazioni e comprometterne gli obiettivi di sicurezza (Riservatezza, Integrità, Disponibilità, Controllo degli Accessi, ecc.)
- un evento, incidentale o accidentale, che indica che il sistema o i dati di un'organizzazione potrebbero essere stati compromessi oppure che le misure di sicurezza per proteggerli sono fallite

- Danni all'infrastruttura, ai beni e alle attività dell'organizzazione
- Deterioramento della reputazione o dell'immagine
- Disservizi verso gli stakeholders (utenti ed altre entità)
- Incremento delle perdite o dei costi aggiuntivi
- Violazione delle normative vigenti
- Aumento dei tempi di risposta

Dalla Cyber Security alla Cyber Resilience

La sicurezza informatica richiede un approccio «*Olistico*».

Storicamente le organizzazione, pubbliche e private, hanno adottato un approccio «*addizionale*» o «*a silos*» nei confronti della Sicurezza Informatica.
La Sicurezza Informatica è mutata ed è diventata una materia trans-disciplinare, che impatta con tutte le componenti rappresentative di un'organizzazione:
i dati, le persone, le procedure, le infrastrutture, gli asset, i processi, i sistemi di controllo, l'organizzazione e la governance, e, pertanto, richiede un approccio «*olistico*».



Il nuovo paradigma è la «*Cyber Resilience*».

La governance di un'organizzazione deve gestire
la sicurezza informatica al pari degli altri asset
perché da essa può dipende il raggiungimento o il fallimento dei risultati attesi.
Gli attacchi informatici cambiano velocemente e, di conseguenza, gli scopi della sicurezza informatica, «*Confidenzialità*, *Integrità* e *Disponibilità*», sono rafforzati con la «*Resilienza*», ovvero la capacità di adattarsi al contesto e di resistere alle minacce in modo da garantire l'erogazione dei servizi essenziali. (se ne parla all'interno del RGPD e della normativa NIS)

Le principali norme in tema di sicurezza informatica

- **Direttiva 2008/114/CE**, «Direttiva per l'individuazione e la designazione delle infrastrutture critiche europee e valutazione della necessità di migliorarne la protezione»
- **Regolamento n. 679/2016**, «Regolamento Generale sulla Protezione dei Dati (RGPD)», entrato in vigore il 24 maggio 2016, applicabile dal 24 maggio 2018
- **Regolamento n. 910/2014**, «Regolamento Electronic Identification Authentication and Signature (EIDAS)», entrato in vigore il 17 settembre 2014, applicabile dal primo luglio 2016, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno
- **Direttiva n. 680/2016**, «Direttiva sul trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati», entrata in vigore il 24 maggio 2016
- **Direttiva n. 1148/2016**, «Direttiva Network and Information Security (Direttiva NIS)», entrata in vigore l'8 agosto 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione
- **Regolamento n. 881/2019**, il «Cybersecurity Act», entrata in vigore il 27 giugno 2019, crea un nuovo sistema di certificazione della sicurezza di prodotti e servizi ICT e che rafforza il ruolo dell'ENISA (Agenzia Europea di sicurezza delle reti e dell'informazione istituita nel 2004)

- **Direttiva 16/1/2002** «Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni»
- **D.lgs 196/2003 e GDPR** «Normativa sulla privacy e tutela dei dati personali», prevede l'adozione delle misure di sicurezza e le procedure di notifica e di ripristino a seguito di un incidente
- **D.LGS. 7.3.2005, art. 71 CAD** «Regole tecniche da adottare per garantire una efficace protezione dei dati e dei livelli di sicurezza necessari» (agg. 2017), prevede le regole tecniche per la sicurezza dei dati
- **DPCM 24.1.2013** «Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali» (agg. nel 2017)
  DPCM 17.2.2017 «Piano nazionale per la protezione cibernetica e la sicurezza informatica», prevedono la riorganizzazione della struttura che si occupa di Cyber Security e la costituzione del CERT-PA e CERT-NAZIONALE
- **Circolare AgID n. 2/2017** «Misure minime di sicurezza ICT per le pubbliche amministrazioni»
- **D.LGS. 65/2018** «Misure per un livello comune elevato di sicurezza delle reti e dei sistemi informatici dell'Unione (NIS)», indica linee per l'identificazione degli operatori di servizi essenziali (OSE), la nascita del CSIRT , gli obblighi in materia di sicurezza e notifica degli incidenti, la sicurezza della rete e dei sistemi informativi dei fornitori di servizi digitali
- **L. 133/2019** «Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica», la normativa è finalizzata ad assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure volte a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi

Cyber Resilience Framework → Maturity Level

Cyber Governance Framework

=

ISO 27014

+

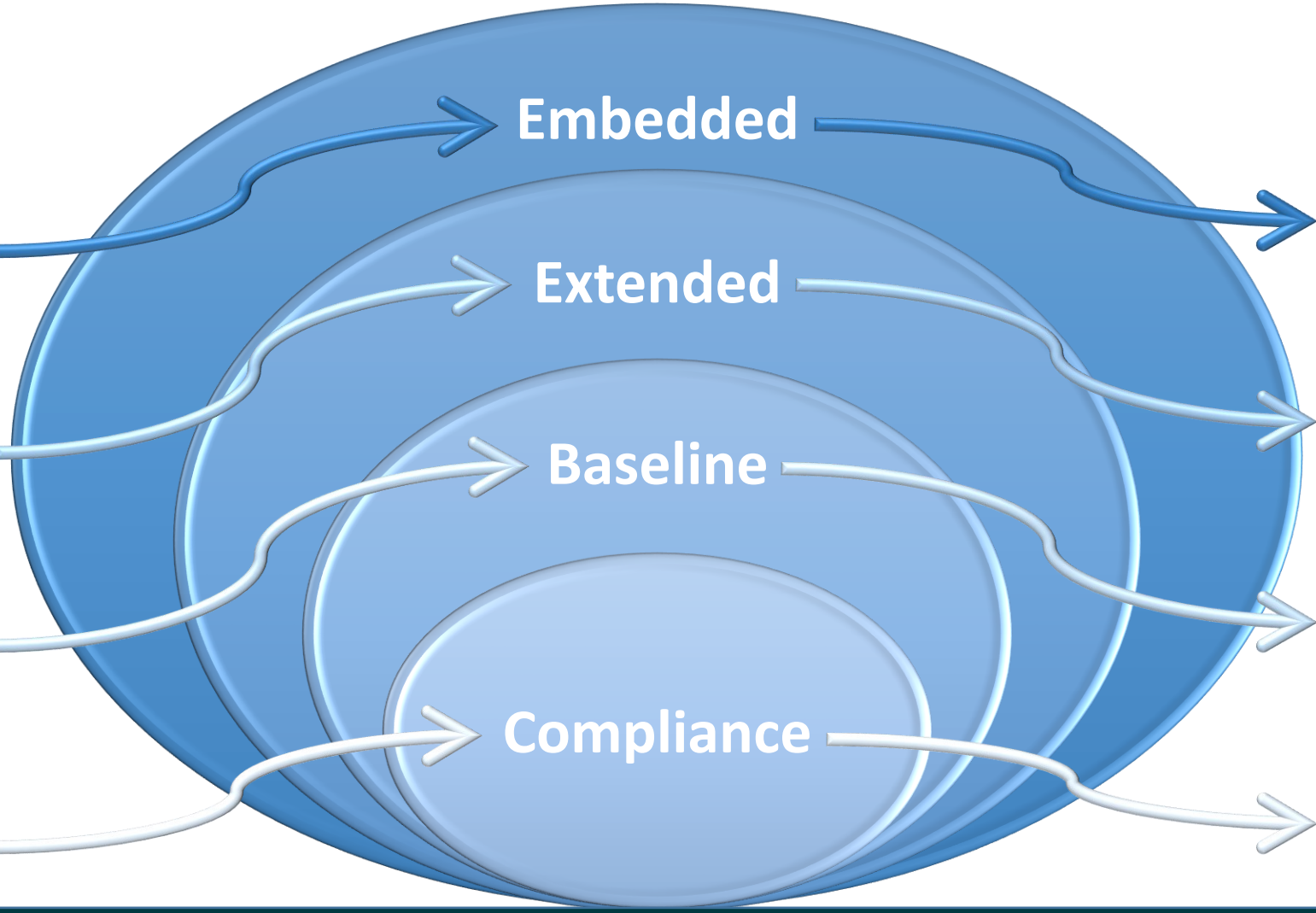
ISO 22301
ISO 27035
ISO 27036
ISO 27017/18

+

ISO 27001

+

Misure Minime di Sicurezza



Obiettivo

- Integrare il programma della sicurezza informatica tra gli obiettivi gestionali generali
- Garantire l'erogazione delle forniture e dei servizi e gestire la continuità operativa
- Integrare la sicurezza informatica nell'attività operativa creando un framework per la gestione dei rischi
- Proteggersi dai comuni attacchi informatici e implementare i controlli di sicurezza di base

Gli Standard e le Linee Guida Internazionali

- ISO / IEC 27001:2013 Specifica i requisiti per stabilire, implementare, mantenere e migliorare do continuo un sistema di gestione della sicurezza delle informazioni nel contesto dell'organizzazione.
- ISO 22301:2019 Questo documento specifica i requisiti per implementare, mantenere e migliorare un sistema di gestione per proteggere, ridurre la probabilità che si verifichino, prepararsi, rispondere e recuperare dalle interruzioni quando si presentano.
- ISO / IEC 27035-1:2016 Presenta i concetti e le fasi di base per la gestione degli incidenti di sicurezza delle informazioni e combina questi concetti con i principi di un approccio strutturato per rilevare, riferire, valutare e rispondere agli incidenti e applicare le lezioni apprese.
- ISO / IEC 27035-2:2016 Fornisce le linee guida per pianificare e preparare la risposta agli incidenti. Le linee guida si basano sulla fase "Pianifica e prepara" e sulla fase "Lezioni apprese" del modello "Fasi di gestione degli incidenti relativi alla sicurezza delle informazioni" presentato nella norma ISO / IEC 27035-1.
- ISO / IEC 27036-3: 2013 Fornisce indicazioni, con particolare riguardo ai potenziali rischi sulla sicurezza delle informazioni, per gli acquirenti e i fornitori di prodotti e servizi nella catena di fornitura delle tecnologie dell'informazione e della comunicazione.
- ISO / IEC 27017: 2015 Fornisce le linee guida per i controlli di sicurezza delle informazioni applicabili alla fornitura e all'uso dei servizi cloud.
- ISO / IEC 27018:2019 Questo documento stabilisce gli obiettivi di controllo, i controlli e le linee guida comunemente accettate per l'implementazione di misure per proteggere le Informazioni di identificazione personale in linea con i principi di privacy in ISO / IEC 29100 per l'ambiente di cloud computing pubblico.
- ISO / IEC 27014: 2013 Fornisce una guida sui concetti e i principi per la governance della sicurezza delle informazioni, mediante la quale le organizzazioni possono valutare, dirigere, monitorare e comunicare le attività relative alla sicurezza delle informazioni all'interno dell'organizzazione.

Costruire
la cyber resilience organizzativa

La Resilienza Informatica

- La resilienza informatica è la capacità di **rispondere ad un incidente informatico e riprendere l'operatività**. Sebbene sia un concetto relativamente recente, deriva dall'evoluzione di soluzioni consolidate. Ciò significa che qualsiasi organizzazione può sfruttare le linee guida esistenti per passare ad uno stato di **cyber resilience**.
- La **cyber resilience organizzativa**:
  - aiuta un'organizzazione a proteggersi dai rischi informatici
  - la difende dalle minacce informatiche
  - limita la gravità di un incidente
  - garantisce la continuità operativa

Il Resilience Framework dell'IT Governance

Il Framework proposto organizza le linee guida esistenti in un modello conforme ai requisiti legali, nonché agli standard internazionali. È composto da 4 elementi di controllo, a cui corrispondono 4 fasi di resilienza, e si basa sul profilo di rischio di un'organizzazione.

Gestire e Proteggere

Individuare gli asset di maggior valore e i rischi associati per indirizzare le aree strategiche al miglioramento attraverso azioni di audit e test.

Compliance

Identificare e Rilevare

Colmare il gap del rischio cibernetico sviluppando controlli efficaci basati su requisiti unici, profili di rischio e contesto organizzativo.

Baseline

Rispondere e Ripristinare

Eseguire le operazioni sotto stress e dimostrare agilità nella risposta agli incidenti per ripristinare rapidamente l'operatività dopo il verificarsi di un incidente informatico.

Extended

Governare e Garantire

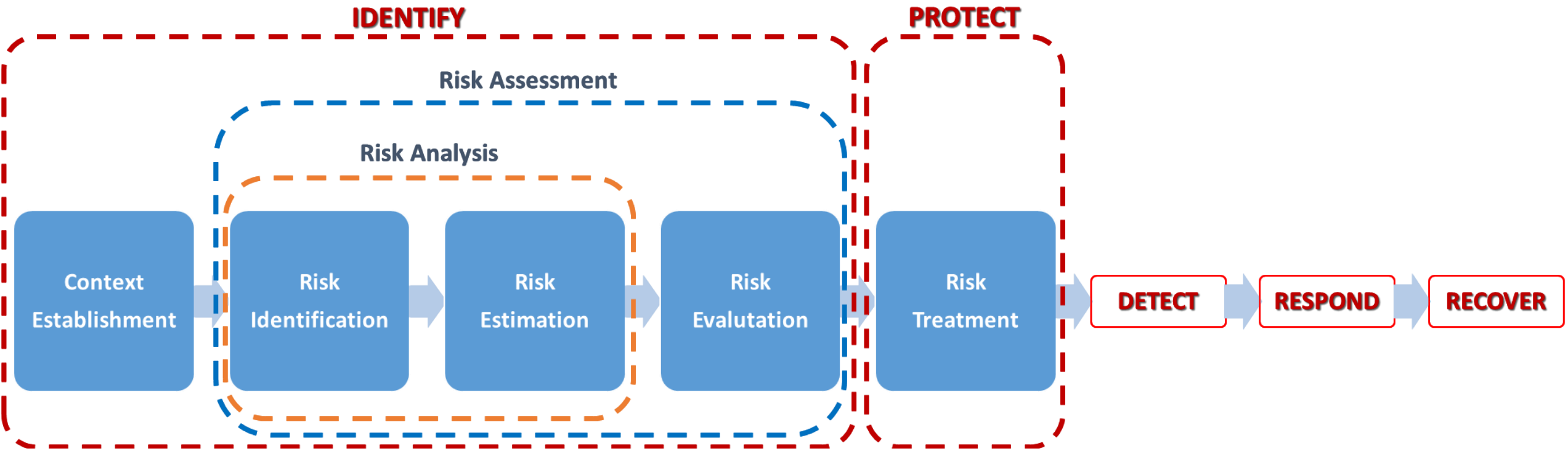
Informare, coinvolgere e condividere con i dirigenti, i consigli di amministrazione e i principali stakeholders, la strategia di resilienza informatica.

Embedded

1. Gestire e Proteggere { Compliance }

La prima e la più ampia categoria del Framework comprende le attività fondamentali per **la gestione della sicurezza informatica e la protezione dell'organizzazione dalle minacce.**

Lo Standard ISO 27k individua 5 funzioni: **Identify, Protect, Detect, Respond e Recover**.



Le attività di questa fase sono caratterizzate dalle funzioni «**Identify** e «**Protect**».

1. Gestire e Proteggere { Compliance }

Per implementare il processo occorre affrontare innanzitutto il Risk Assessment, tale attività è necessaria per ridurre al minimo la probabilità di interruzione di servizio. Di seguito è riportata la descrizione delle cinque attività:

- **Context Establishment**: comprende il rischio relativo all'operatività: i servizi erogati, le funzioni, gli asset e gli individui.
- **Risk Identication**: effettua l'identificazione dei rischi, basandosi su:
  - l'identificazione dei processi aziendali che contribuiscono alla fornitura del servizio
  - l'identificazione delle minacce che potrebbero provocare un impatto sulla normale fornitura del servizio
  - l'analisi delle condizioni necessarie affinché si verifichi un impatto sul servizio
  - l'analisi degli asset critici per l'erogazione del servizio e delle misure di sicurezza presenti a supporto di ogni asset
  - la definizione e la prioritizzazione dei rischi che devono essere mitigati.
- **Risk Estimation**: effettua l'analisi del rischio inerente, cioè l'analisi del rischio di accadimento di possibili scenari di rischio e delle loro conseguenze, senza considerare l'esistenza di misure di mitigazione. Il rischio inerente tiene conto:
  - probabilità di accadimento di una specifica minaccia cyber
  - impatto sull'asset.
- **Risk Evaluation**: effettua l'analisi del rischio residuo, cioè l'analisi del rischio che permane dopo le contromisure.
- **Risk Treatment**: tratta il rischio residuo attraverso:
  - la definizione dei criteri di accettazione del rischio
  - la prioritizzazione dei rischi sulla base del relativo livello di rischio residuo
  - l'identificazione dei rischi che devono essere mitigati e le relative contromisure da implementare.

È necessario che il processo venga regolarmente reiterato, monitorato e verificato.

1. Gestire e Proteggere { Compliance }

Le principali misure per mitigare e contenere i rischi connessi alla sicurezza informatica dovrebbero riguardare:

- **La protezione dai malware**: i sistemi software ed altre misure tecniche che dovrebbero proteggere i sistemi informatici e le informazioni da un'ampia gamma di malware (inclusi virus, worm, spyware, software botnet e ransomware).
- **Le informazioni e le politiche per la sicurezza:** l'organizzazione deve documentare come prevede di proteggere le proprie risorse fisiche e informative. Le politiche devono essere comunicate e comprese da tutto il personale e dai partners.
- **Un programma formale per la gestione della sicurezza delle informazioni:** dovrebbe esserci un approccio strutturato per proteggere le risorse informative all'interno dell'organizzazione, tenendo conto delle persone, dei processi e della tecnologia. Questo approccio dovrebbe unificare tutti gli altri processi.
- **L'identità e il controllo degli accessi**: è necessario attuare misure per garantire che le persone che tentano di accedere alle informazioni e ai sistemi informatici siano chi dichiarano di essere e che siano autorizzate ad accedere a tali informazioni. Ciò deve includere l'accesso fisico e l'accesso logico.
- **Le competenze e la formazione del team di sicurezza**: i team di sicurezza dovrebbero essere adeguatamente qualificati e regolarmente aggiornati su come rispondere agli incidenti di sicurezza informatica. Inoltre, dovrebbero esistere processi per lo sviluppo di team di sicurezza e l'identificazione delle competenze necessarie.
- **La formazione per la consapevolezza del personale**: i dipendenti devono ricevere regolarmente una formazione sulla consapevolezza della sicurezza informatica, sulle minacce e sulle procedure di sicurezza. Ciò potrebbe includere i poster, i briefing.
- **La crittografia:** l'organizzazione dovrebbe avere un processo documentato che definisce quando e come viene applicata la crittografia per proteggere le informazioni, che tenga conto delle informazioni sia in transito che a riposo

..../...

1. Gestire e Proteggere { Compliance }

- **La sicurezza fisica e ambientale:** i controlli di sicurezza fisica e ambientale dovrebbero essere implementati per ridurre il rischio rappresentato dalle minacce provenienti dell'ambiente fisico, inclusi i rischi naturali o ambientali e le intrusioni fisiche da parte di individui non autorizzati.
- **La gestione delle patch:** l'organizzazione dovrebbe avere un processo che definisca come viene aggiornato il software sui computer e sui dispositivi di rete. I processi di gestione delle patch potrebbero influire sulle politiche di acquisto per garantire che il software sia supportato e continuerà a ricevere le patch necessarie e ritirare il software non supportato.
- **La sicurezza della rete e delle comunicazioni**: l'infrastruttura di rete dell'organizzazione dovrebbe essere protetta con tecnologie e processi adeguati, come switch, firewall, segregazione e DMZ. Ciò potrebbe includere la protezione fisica delle risorse di comunicazione.
- **La sicurezza dei sistemi**: i sistemi dovrebbero essere progettati per essere sicuri, compresi i sistemi interni ed esterni come le applicazioni web e i database.
- **La gestione delle risorse**: le risorse (sia informative che fisiche) devono essere registrate, tracciate e gestite durante tutto il loro ciclo di vita. Ogni risorsa dovrebbe avere un "proprietario" definito, che ne è responsabile.
- **La gestione del rischio nella catena di approvvigionamento**: l'organizzazione dovrebbe disporre di misure per proteggere le informazioni lungo tutta la catena di approvvigionamento, come i requisiti di sicurezza nei contratti, gli accordi di non divulgazione e le regole per la condivisione delle informazioni. Questi dovrebbero coprire l'intera catena di approvvigionamento, compresi i fornitori di prodotti fisici, i fornitori di software e i fornitori di servizi cloud.

L'estensione con cui verranno implementate queste misure dipenderà dall'ambiente e dai requisiti di conformità.

2. Identificare e Rilevare { Baseline }

Il secondo elemento del Framework si concentra sul monitoraggio delle informazioni e dei sistemi informativi dell'organizzazione al fine di individuare eventuali anomalie. (**DETECT**)

Queste attività dovrebbe riguardare:

- **Il monitoraggio della sicurezza:** i sistemi, le reti e le misure di sicurezza dell'organizzazione devono essere costantemente monitorati e registrati (logs), sia attraverso mezzi automatizzati, che attraverso attività meno frequenti come la scansione delle vulnerabilità e i test di penetrazione. Le eventuali anomalie e i punti deboli identificati devono essere subito presi in considerazione.
- **Il rilevamento attivo:** l'organizzazione dovrebbe anche cercare attivamente di rilevare incidenti (ad esempio, rivedendo manualmente i registri di controllo e raccogliendo informazioni dall'esterno dell'organizzazione). Dovrebbero essere messe in atto misure per aiutare a rilevare le attività dannose che potrebbero altrimenti essere difficili da identificare.

L'estensione con cui verranno implementate queste misure dipenderà dall'ambiente e dai requisiti di conformità.

3. Rispondere e Ripristinare { Extended }

Il terzo elemento del Framework affronta la necessità di gestire gli incidenti in modo rapido ed efficace per limitare i danni e ripristinare la piena funzionalità. (**RESPONSE & RECOVER**)

Dovrebbe riguardare:

- **La gestione della risposta agli incidenti**: i servizi ICT sono resistenti in caso di calamità e possono essere recuperati entro i tempi concordati con il senior management.
- **La gestione della continuità delle TIC**: i piani, i ruoli definiti, l'addestramento, l supervisione della comunicazione e della direzione per scoprire rapidamente un incidente e contenere efficacemente il danno, sradicare la minaccia e ripristinare l'integrità della rete e dei sistemi interessati. Esistono soglie e tempistiche concordate per il recupero delle funzioni ICT a seguito di un incidente.
- **La gestione della continuità operativa**: le misure per identificare il rischio di esposizione alle minacce interne ed esterne e per far fronte a gravi perturbazioni come attacchi informatici, inondazioni e guasti degli approvvigionamenti.
- **La condivisione delle informazioni e la collaborazione**: le informazioni sulle minacce e le vulnerabilità sono condivise tra i fornitori, i partner, gli enti del settore e le autorità per migliorare la capacità collettiva di rilevare, prevenire, mitigare, rispondere e recuperare in modo proattivo dagli incidenti di sicurezza informatici.

L'estensione con cui verranno implementate queste misure dipenderà dall'ambiente e dai requisiti di conformità.

Incident Response Life Cycle

Prima: PREPARE

- PEOPLE: INCIDENT RESPONSE TEAM
- PROCESS: INCIDENT RESPONSE PLAN
- TECH: INCIDENT RESPONSE PLATFORM
- IMPROVEMENT PROGRAM

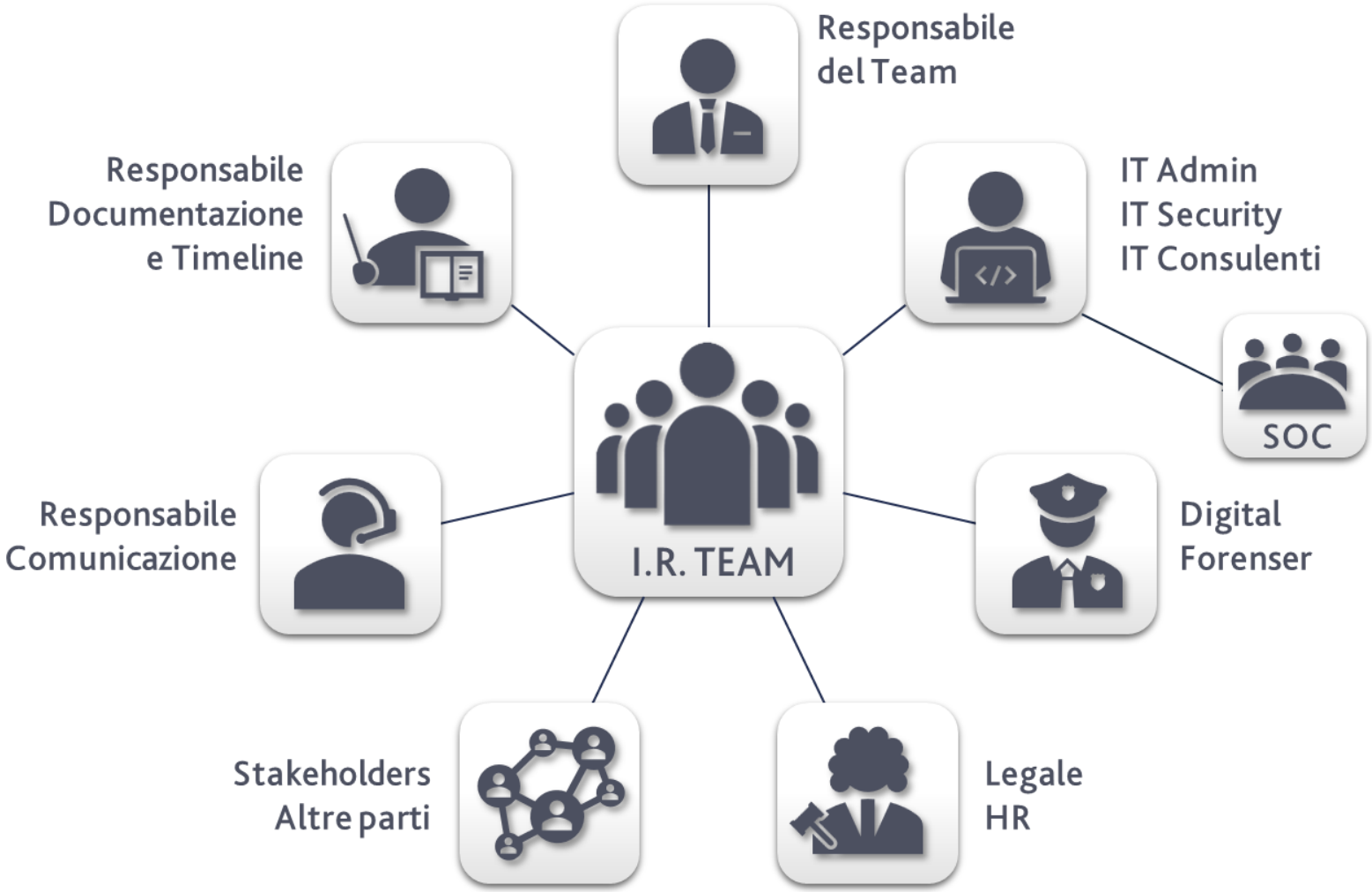
Durante: DETECT & RESPOND

- IDENTIFICAZIONE DELL'EVENTO
- CONTENIMENTO DEGLI EFFETTI
- RIMOZIONE DELLA MINACCIA
- RIPRISTINO DELL'OPERATIVITÀ

Dopo: FOLLOW UP

- DIGITAL FORENSICS
- ANALISI DELL'EVENTO
- LEZIONE DI APPRENDIMENTO
- CONDIVISIONE DEL CASO

Persone → Incident Response Team



QUAL È L'OBIETTIVO DELL'I.R.TEAM?

- L'obiettivo principale consiste nel coordinare e valutare le risorse principali e i membri del team durante un incidente di sicurezza informatica per ridurre al minimo l'impatto e ripristinare l'operatività il più rapidamente possibile

CHE COSA FA UN I.R.TEAM?

- Analizza le informazioni raccolte (regola 5 W)
- Risponde agli incidenti informatici
- Gestisce le comunicazioni interne ed esterne
- È responsabile della notifica dell'incidente alle agenzie governative
- Verifica periodicamente le procedure dell'IR

QUALI COMPETENZE SONO NECESSARIE?

- Cercare denominatori ed eccezioni comuni
- Fare affermazioni e non ipotesi
- Eliminare l'impossibile
- Cercare sempre la spiegazione più semplice
- Ragionare come un hacker

Processi → Incident Response Plan

QUAL È L'OBIETTIVO DELL'I.R.PLAN?

- Formalizzare i ruoli e le responsabilità
- Gestire una serie completa di risposte agli incidenti informatici pertinenti all'organizzazione per cui è stato elaborato

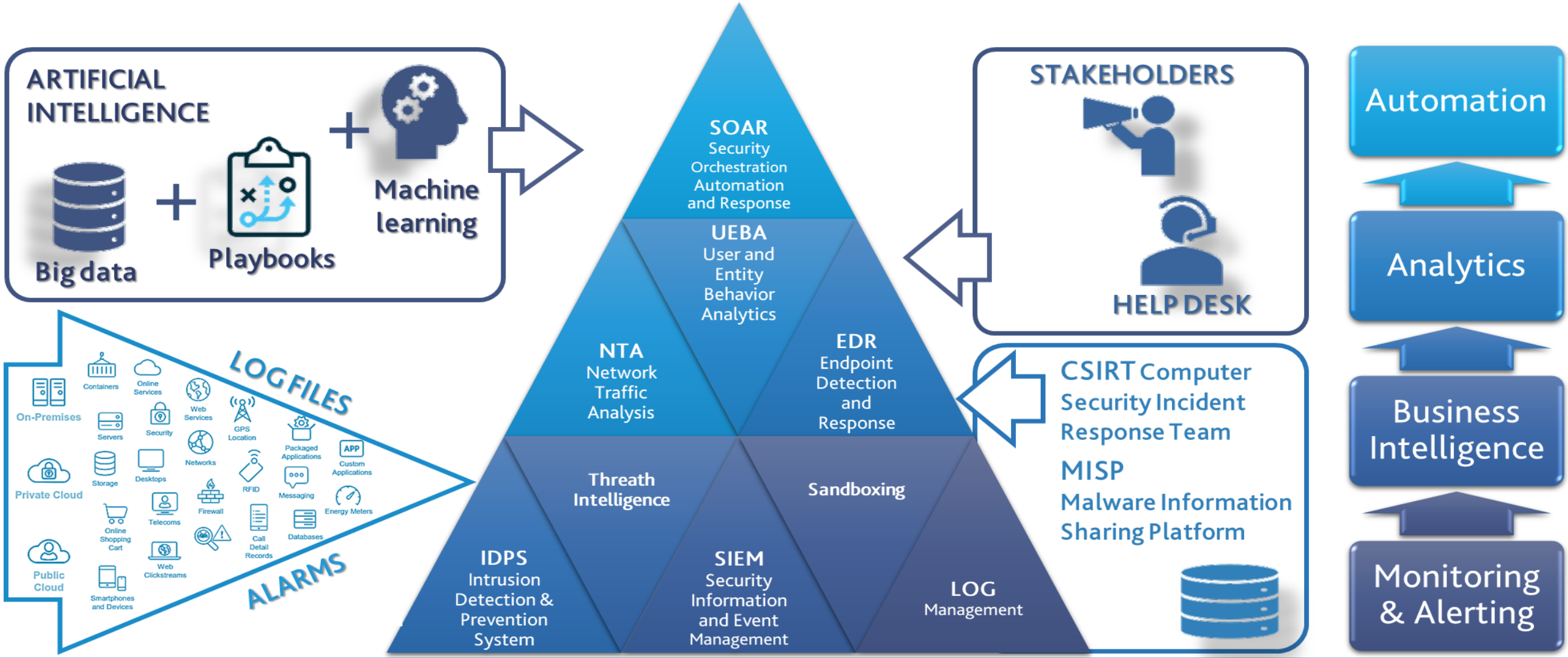
COME SI SVILUPPA UN I.R.PLAN?

- Effettuare una valutazione delle criticità
- Eseguire un'analisi realistica delle minacce
- Considerare le implicazioni sulle persone, sui processi, sulle tecnologie e sulle informazioni
- Creare modelli di risposta appropriati (Playbook)
- Rivedere periodicamente la capacità di risposta

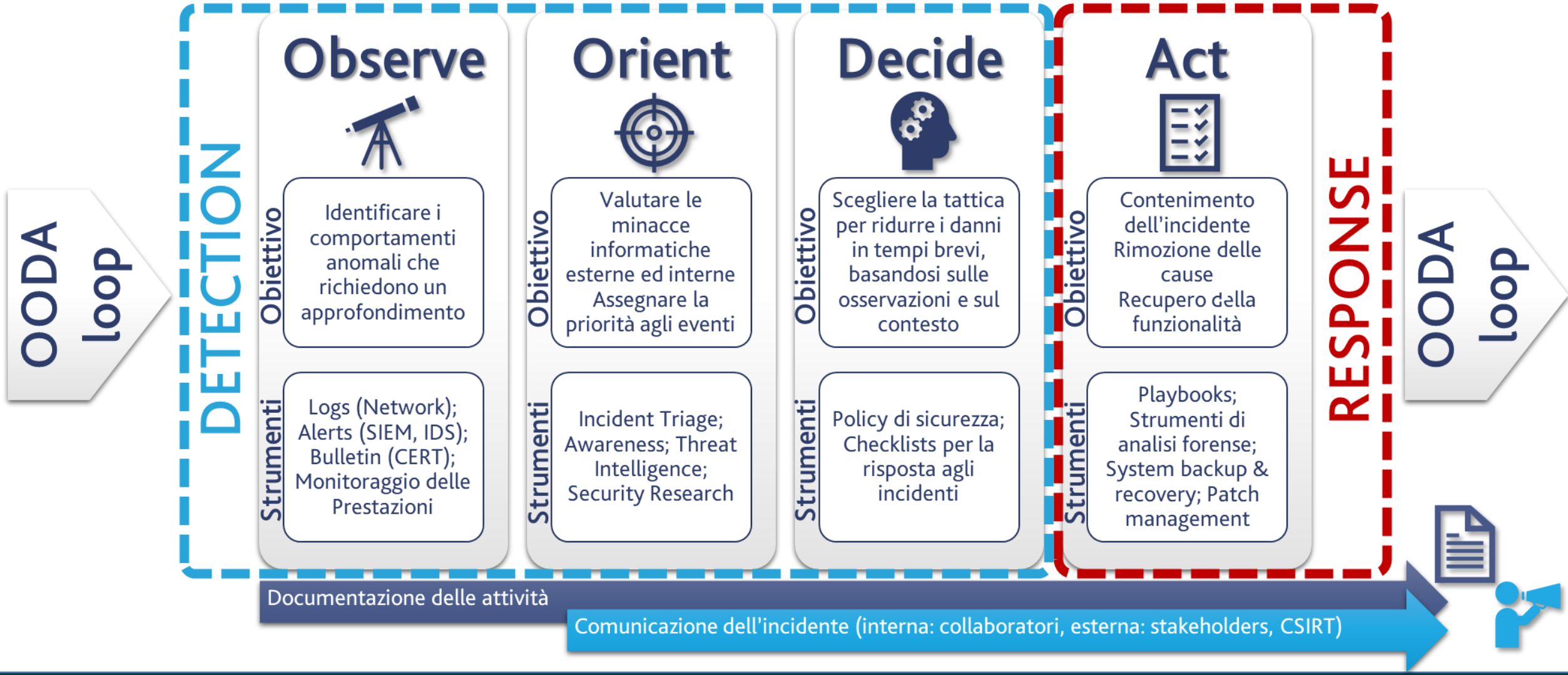
QUALI SONO LE CRITICITÀ DI UN I.R.PLAN?

- Obsolescenza per carenza di aggiornamenti
- Complessità delle procedure da adottare
- Scarsa condivisione con gli stakeholders

Tecnologia → Incident Response Platform



Detection & Response



Incident Triage → Cyber Kill Chain

La "cyber kill chain" è una sequenza di fasi che consente ad un utente malevolo di accedere ad una rete ed estrarre i dati

Follow up → Lessons Learned

4. Governare e Garantire { Embedded }

Il quarto elemento del Framework include l'attività per il consiglio di amministrazione e i senior manager al fine di garantire che la cyber resilience sia supervisionata e convalidata dal top management dell'organizzazione.

Dovrebbe riguardare:

- **Il programma completo di gestione dei rischi**: un processo sistematico e continuo di identificazione, valutazione e risposta ai rischi di sicurezza informatica. Questa è una competenza fondamentale per qualsiasi cyber security o framework di cyber resilience efficace e informa come e quando verranno applicati gli altri processi.
- **La convalida / la certificazione esterna**: la certificazione secondo gli standard internazionali o i frameworks di sicurezza informatica consolidati fornisce la convalida esterna della sicurezza informatica e della resilienza dell'organizzazione e può fornire sicurezza agli utenti e alle altre parti interessate. In alcuni casi, terze parti possono richiedere l'audit di conformità o di convalida attraverso uno schema specifico.
- **L'audit interno**: un regolare programma di audit valuta i controlli di sicurezza delle informazioni dell'organizzazione. I risultati sono valutati nell'ambito di una revisione della direzione.
- **L'impegno e il coinvolgimento a livello di board**: il board approva, supporta e partecipa alla strategia di sicurezza informatica e riceve regolari aggiornamenti sui problemi di sicurezza, i rischi e le conformità.
- **La struttura e i processi di governance**: l'organizzazione dispone di strutture di governance chiare e definite catene di responsabilità per sovrintendere ai suoi processi di sicurezza informatica e resilienza. Ciò potrebbe includere l'organizzazione di diversi elementi del framework in funzioni supervisionate da un direttore responsabile o da un comitato di governance.
- **Il processo di miglioramento continuo**: un processo per riesaminare e migliorare continuamente le misure di sicurezza dell'organizzazione e per adattarsi all'evoluzione del panorama delle minacce. Ciò potrebbe includere l'adozione di noti modelli di miglioramento come il PDCA (Plan-Do-Check-Act), il servizio di miglioramento continuo del ITIL o il ciclo di vita del miglioramento continuo di COBIT.

Conclusioni

- La sicurezza informatica da sola non è più sufficientemente.
  Non è più pensabile che ci si possa difendere da ogni potenziale incidente.
  Si deve accettare che, prima o poi, qualche attacco avrà successo.
- La resilienza informatica è un approccio più ampio,
  comprende la sicurezza informatica e la business continuity
  e mira non solo a difendere contro i potenziali incidenti, ma anche a
  garantire la sopravvivenza dell'operatività a seguito di un attacco riuscito.

«Sono convinto che ci siano solo due tipi di aziende: quelle che sono state attaccate e quelle che devono ancora esserlo. E, a loro volta, convergono in una sola categoria: aziende che sono state attaccate e che saranno nuovamente attaccate» (Muller, 2012)

Grazie

CI SONO DOMANDE?