Sicurezza industriale, intelligence

La gestione della sicurezza industriale fra previsioni normative e problemi di management, certificazioni, standardizzazione, problem solving, l'intelligence privata

Giuristi ed informatica

Per chi crede che la sicurezza delle informazioni sia solo materia di informatici e che tutto si riduca a bit, hardware e software... dimostreremo che si tratta di un errore concettuale profondo

Il mondo digitale non è solo strumento

Il giurista è chiamato a prestare la sua opera in più momenti e con diverse prospettive.
Nei nostri incontri esamineremo questi aspetti fondamentali, in relazione ad un principio sempre più evidente nel nostro sistema: il «Duty of care», che può essere tradotto in diverse declinazioni:

- Come dovere di diligenza professionale;
- Come obbligo di protezione connesso ad una o più «posizioni di garanzia» riferite al paradigma dell'art. 40 comma 2;
- In riferimento all'azione conformativa del diritto, in relazione alle previsioni costituzionali sull'esercizio dell'attività di impresa

Un lavoro paziente

- Il «duty of care» come requisito fondante dell'attività d'impresa (ma anche dello studio professionale), richiede un'attenta attività di comprensione del fenomeno ed immanente attenzione alle «rules of law» , inclusa la considerazione dei potenziali avversari, interni od esterni;
- Nella fase dell'emergenza e della crisi, la piena conoscenza degli strumenti della gestione del contenzioso, la raccolta delle evidenze probatorie e la costruzione di strategie di difesa risultano essenziali e presuppongono la piena, integrale consapevolezza del fatto che il mondo «cyber» ha regole sue proprie, che vanno comprese e governate

INTRODUZIONE

La comprensione della Sicurezza delle Informazioni come processo


Rai 1

Introduzione

Che cos'è l'informazione e perché è necessario proteggerla

A chiunque si chieda cosa sia l'informazione, non si riuscirà ad avere una risposta univoca.
possiamo solo dire che l'informazione:

- attiene alla conoscenza di elementi semplici o complessi riguardo a persone, cose, fatti, circostanze
- che l'informazione non è un elemento "statico" ma "dinamico", nel senso che
  - serve a qualcosa
  - è necessaria alle attività degli individui e delle organizzazioni
  - ha un valore

Introduzione - 2

perché è necessario proteggere l'informazione?

Viviamo di informazioni, nel quotidiano, per ogni nostra attività, individuale o relazionale.
La nostra conoscenza si basa sull'informazione, che quotidianamente utilizziamo anche per esigenze elementari.
Per le organizzazioni, semplici o complesse, le informazioni sono l'essenza stessa dell'attività, dal *know how* industriale ai processi di vendita e fatturazione; dalla ricerca e sviluppo alla gestione delle risorse umane.
L'informazione è dunque un **elemento vitale** che va adeguatamente protetto da eventi, naturali o umani, deliberati o involontari, che le possano pregiudicare

La sicurezza delle informazioni

Cosa significa proteggere l'informazione?

le caratteristiche dell'informazione, in un mondo interconnesso, le rendono esposte a diversi rischi.
La sicurezza delle informazioni è una questione che riguarda gli individui e le organizzazioni, perché per gli uni e gli altri, la perdita, il danneggiamento, il non poterle utilizzare quando serve, ed esattamente nel momento in cui servono, può determinare eventi critici, anche per la stessa vita ed incolumità personale.

Information Security Vs. Privacy

c’è spesso confusione sui due termini e sulle rispettive relazioni.
E’ fuor di dubbio che i due domini siano strettamente correlati, ma occorre fare chiarezza
la privacy riguarda il diritto di persone fisiche di essere tutelati da trattamenti non conformi dei propri dati personali e quindi una aspettativa di diritto ad un trattamento lecito, pertinente, conforme e nei limiti del consenso dato
La security delle informazioni, invece, riguarda il modo con cui le informazioni vengono protette, riguardo ai tre obiettivi della disponibilità, integrità e riservatezza.
Se un fornitore di servizi digitali (come evidenziato nei casi Facebook, Google, ecc.) vende i nostri dati a terzi o li utilizza per scopi non leciti, questa è questione di privacy.
Se qualcuno accede indebitamente ai dati presenti sul nostro pc, rubandoli o rendendoli permanentemente irraggiungibili, questa è questione di security

Art. 32 GDPR -Sicurezza del trattamento

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 pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) 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, a dati personali trasmessi, conservati o comunque trattati.

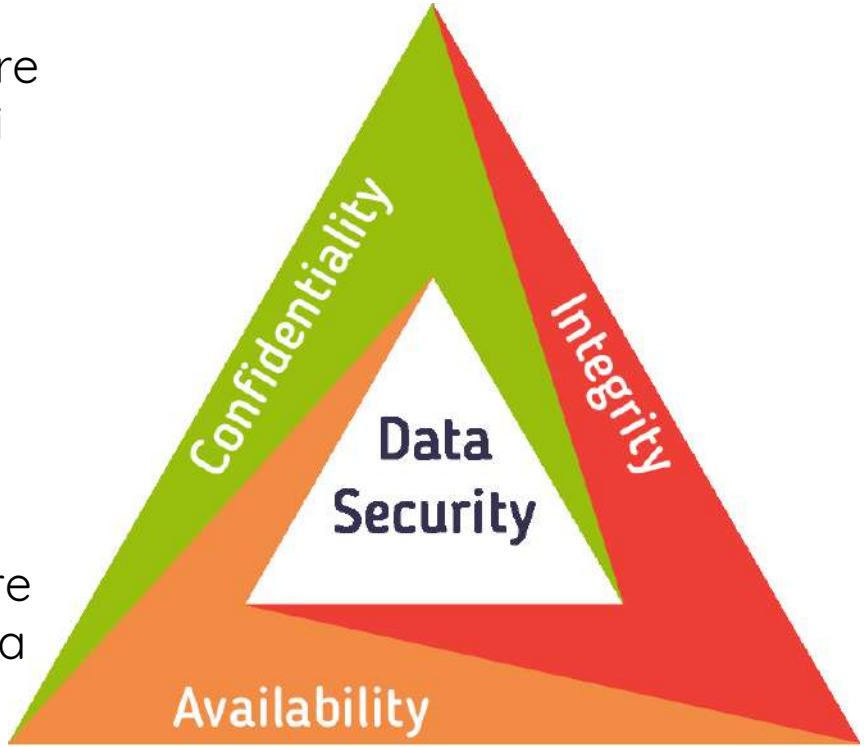
... (omissis)

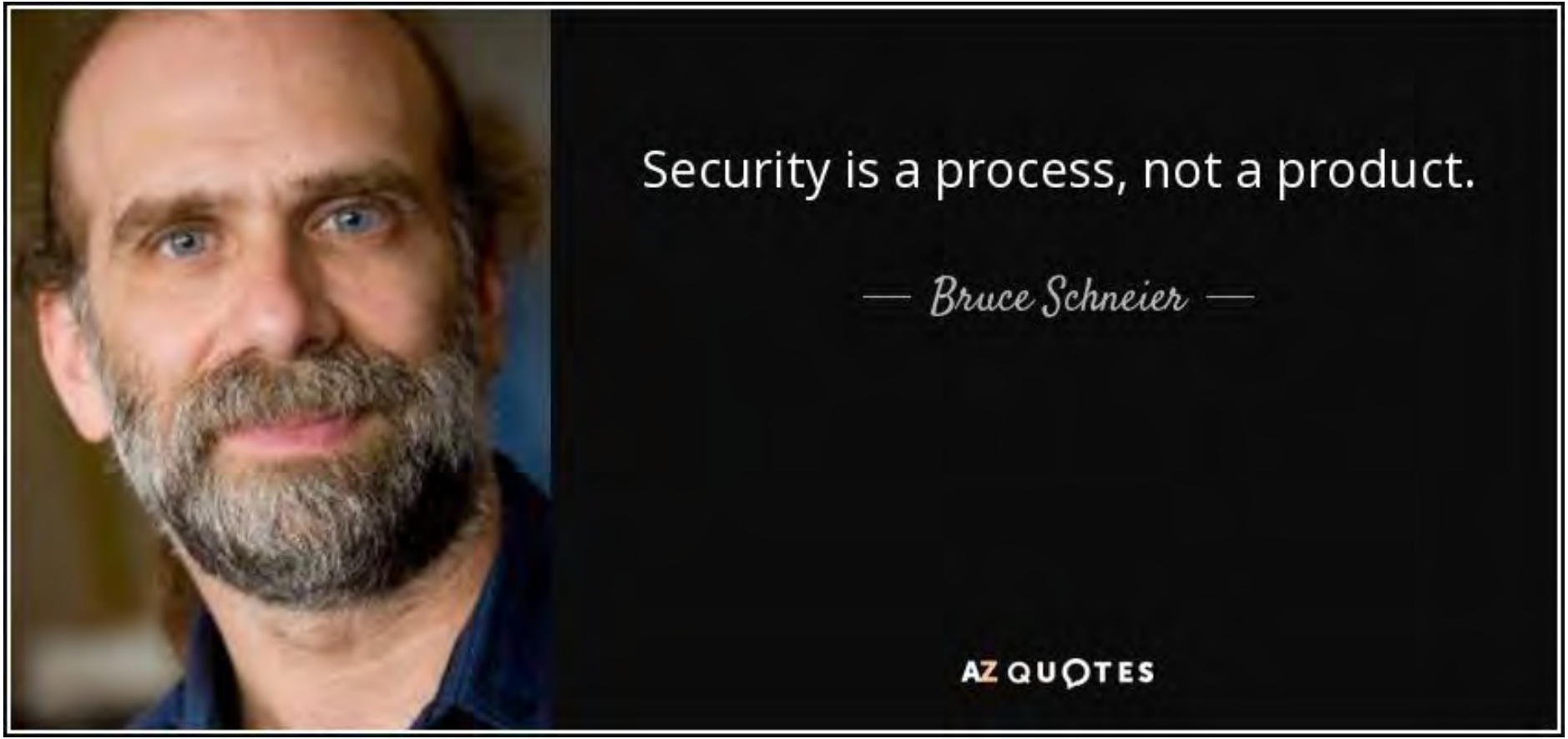
I pilastri della sicurezza delle informazioni

DISPONIBILITA' - L'informazione deve essere reperibile ed utilizzabile nel momento in cui serve

INTEGRITA' - l'informazione deve essere autentica, genuina, non alterata se non da chi ha titolo e conservare questo attributo per tutto il suo ciclo di vita

RISERVATEZZA - l'informazione deve essere accessibile ed utilizzabile esclusivamente da chi ha autorizzazione, titolo e ragione ad accedervi




Security is a process, not a product.
— Bruce Schneier —
AZ QUOTES

Information Security Governance

La sicurezza delle informazioni è **parte integrante del business** ed attiene alla sopravvivenza stessa delle imprese. Le organizzazioni che non pongono cura adeguata nella protezione delle loro informazioni, prima o poi, incontrano problemi gravissimi:

- di ordine legale, come nel caso della privacy, quando si verificano *data breach*;
- di sopravvivenza, perché il blocco delle attività derivanti da incidenti di sicurezza delle informazioni possono essere devastanti
- di reputazione, perché un'impresa che non protegge i suoi asset più preziosi è un'impresa inaffidabile.

No, non può capitare a me…

«Quando qualcuno mi chieda di descrivere la mia esperienza in quasi 40 anni in mare mi limito a dire 'senza incidenti'… Naturalmente ci sono stati venti invernali e le tempeste e nebbia, ma in tutta la mia esperienza non sono mai stato coinvolto in un incidente degno di nota… non ho mai visto un relitto e mai sono stato affondato né mi sono trovato in una qualche situazione di pericolo che potesse trasformarsi in un disastro… Non riesco a immaginare una condizione che possa portare una nave ad affondare… Non riesco a concepire alcun disastro fatale per questa nave… Le tecniche di costruzione delle navi moderne sono andate molto oltre … » Cap. Edward Smith


CYBER
SECURITY

Un mondo di minacce crescenti

La velocità con la quale, negli ultimi 15 anni, sono aumentati gli attacchi cibernetici è esponenziale rispetto all'evoluzione tecnologica. Gli attacchi sono sempre più sofisticati, gli aggressori sempre più preparati ed i danni infinitamente più rilevanti

Dove spesso la risposta è...

...Nuove leggi e regolamenti

IL PARADOSSO

Avere buone regole e procedure non basta

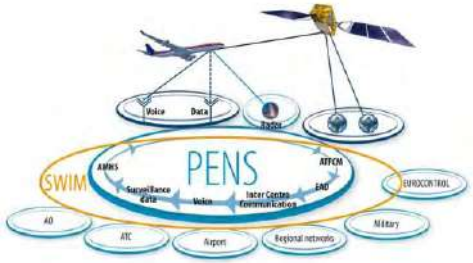
UN ESEMPIO, IL MONDO DELL'AVIAZIONE

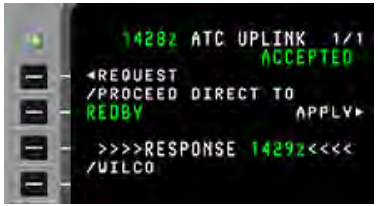
VELOCITA' DELLA TRASFORMAZIONE DIGITALE

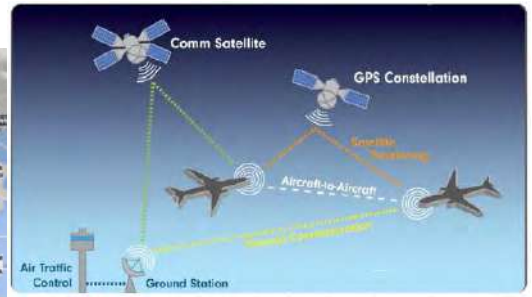
NUOVI CONCETTI OPERATIVI

INCREMENTO DELLE INTERDIPENDENZE

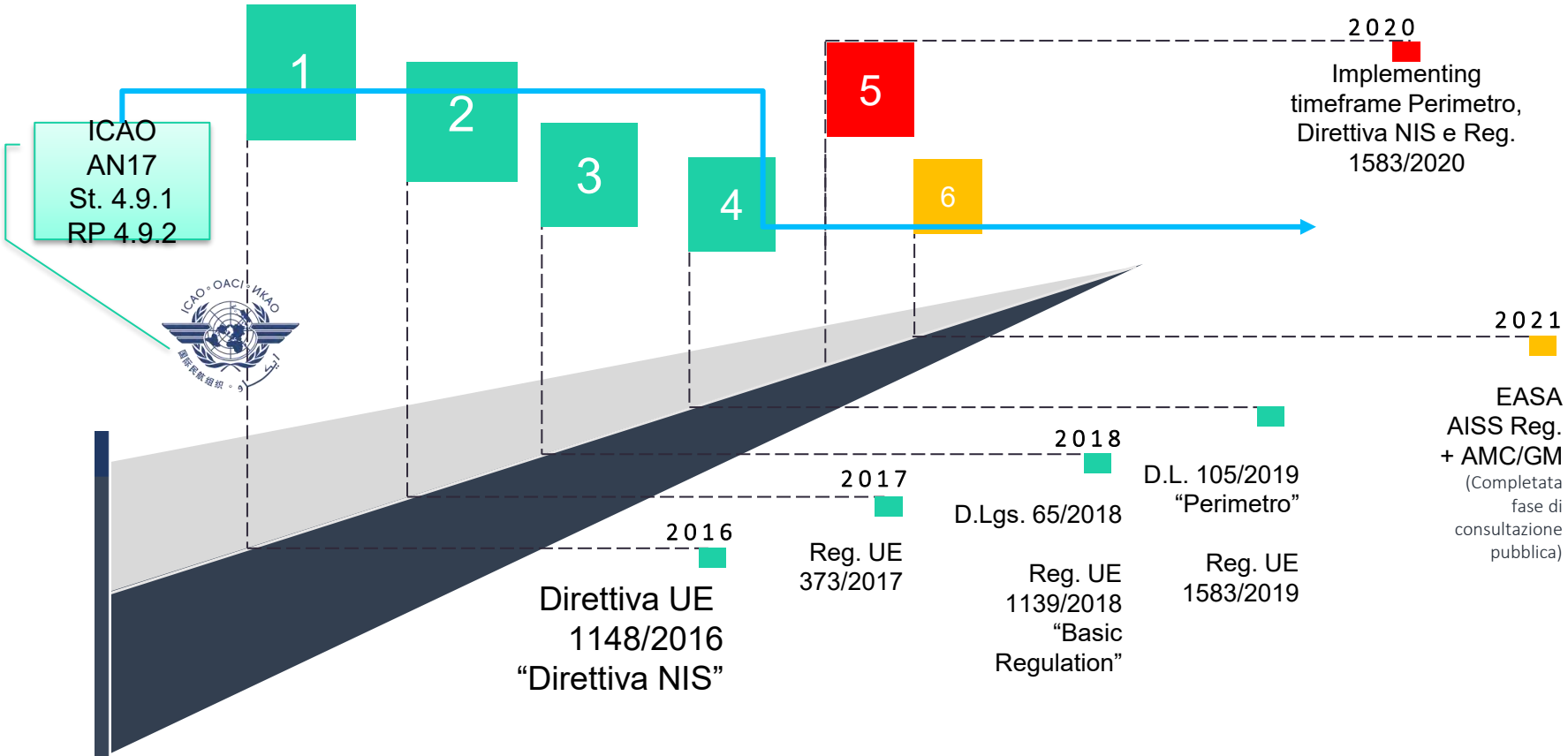
FLEXIBILITY NEEDED







ROADMAP
TIMELINE



INFRASTRUTTURE CRITICHE INFORMATIZZATE

società partecipate dallo Stato, dalle regioni e dai comuni interessanti aree metropolitane non inferiori a 500.000 abitanti, operanti nei settori delle comunicazioni, dei trasporti, dell'energia, della salute e delle acque

Decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155

INFRASTRUTTURE CRITICHE

infrastruttura, ubicata in uno Stato membro dell'Unione europea, che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale della popolazione ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in quello Stato, a causa dell'impossibilità di mantenere tali funzioni

Decreto Legislativo 11 aprile 2011, n. 61

Cui si associano le specifiche obbligazioni connesse alla natura di Operatore aeronautico

OPERATORE DI SERVIZI ESSENZIALI

a) un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali;
b) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi;
c) c) un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio.

Decreto Legislativo 18 maggio 2018, n. 65

OPERATORE DI SERVIZI ESSENZIALI

amministrazioni pubbliche, enti e operatori pubblici e privati … aventi una sede nel territorio nazionale, inclusi nel perimetro di sicurezza nazionale cibernetica e tenuti al rispetto delle misure e degli obblighi previsti

Decreto-Legge 21 settembre 2019, n. 105 convertito con modificazioni dalla Legge 18 novembre 2019, n. 133

OBBLIGAZIONI ORIGINARIE DEL FORNITORE DI SERVIZI DI NAVIGAZIONE AEREA

REG. UE 373/2019 E NORMATIVA COLLATERALE – 1)

(4) Affinché gli Stati membri acquisiscano fiducia reciproca nei loro rispettivi sistemi sono essenziali norme comuni per la certificazione e la sorveglianza dei fornitori di servizi interessati. Per questo motivo, e al fine di garantire il massimo livello di sicurezza e *security*, è pertanto opportuno rafforzare i requisiti per la fornitura di servizi e la loro sorveglianza. Ciò dovrebbe garantire la fornitura in sicurezza di servizi di alta qualità per la navigazione aerea nonché il riconoscimento reciproco dei certificati in tutta l'Unione e migliorare la libertà di circolazione e la disponibilità di tali servizi.

(5) Per assicurare un approccio armonizzato alla certificazione e alla sorveglianza è opportuno coordinare le misure da attuare per la *security* di sistemi, componenti in uso e dati tra gli Stati membri, i blocchi funzionali di spazio aereo e la rete costituita da servizi, funzioni e prodotti offerti da fornitori di servizi, dal gestore della rete, dagli aeroporti e da altre persone che offrono l'infrastruttura necessaria per le operazioni di volo.

(6) La gestione della sicurezza garantisce l'identificazione, la valutazione e la minimizzazione dei rischi di sicurezza e delle vulnerabilità a livello di *security* che incidono sulla sicurezza. È pertanto necessario elaborare ulteriormente i requisiti relativi alla valutazione, da parte di un'organizzazione certificata, delle modifiche del sistema funzionale in termini di sicurezza. Tali requisiti dovrebbero essere adeguati tenendo conto dell'integrazione dei requisiti relativi alla gestione delle modifiche nella struttura regolamentare comune per la sicurezza dell'aviazione civile e dell'esperienza acquisita dalle parti interessate e dalle autorità competenti in materia di sorveglianza della sicurezza.

OBBLIGAZIONI ORIGINARIE DEL FORNITORE DI SERVIZI DI NAVIGAZIONE AEREA

REG. UE 373/2019 E NORMATIVA COLLATERALE – 2)

REGOLAMENTO (CE) N. 550/2004 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 10 marzo 2004

sulla fornitura di servizi di navigazione aerea nel cielo unico europeo

(«regolamento sulla fornitura di servizi»)

La fornitura di servizi di traffico aereo, quale prevista dal presente regolamento, si ricollega all'esercizio di prerogative dei pubblici poteri che non presentano carattere economico che giustifichi l'applicazione delle norme sulla concorrenza previste dal trattato.

EC Reg. 550/2014, 5° *considerando*

Salvaguardia della vita umana in volo e a terra e tutela di diritti costituzionalmente rilevanti connessi alla continuità, efficienza e regolarità del sistema trasporto

OBBLIGAZIONI ORIGINARIE DEL FORNITORE DI SERVIZI DI NAVIGAZIONE AEREA

REG. UE 373/2019 E NORMATIVA COLLATERALE – 3)

ATM/ANS.OR.D.010 Gestione della sicurezza (*security*)

(a) Come parte integrante del loro sistema di gestione, secondo quanto previsto al punto ATM/ANS.OR.B.005, i fornitori di servizi di navigazione aerea e di gestione dei flussi di traffico aereo e il gestore della rete istituiscono un sistema di security al fine di assicurare:

(1) la sicurezza dei loro impianti e del loro personale in modo da prevenire qualsiasi indebita interferenza nella fornitura dei servizi;

(2) la sicurezza dei dati operativi che ricevono, producono o utilizzano, di modo che il loro accesso sia riservato alle sole persone autorizzate.

(b) Il sistema di gestione della security definisce:

(1) le procedure relative alla valutazione e all'attenuazione dei rischi per la sicurezza, al monitoraggio e al miglioramento della sicurezza, al riesame della sicurezza e alla diffusione degli insegnamenti tratti;

(2) gli strumenti intesi a individuare le violazioni della sicurezza e ad allertare il personale con idonei avvisi di sicurezza;

(3) i mezzi per contenere gli effetti delle violazioni della sicurezza e individuare le misure di ripristino della sicurezza e le procedure di mitigazione per evitare che tali eventi si ripetano.

(c) I fornitori di servizi di navigazione aerea e di gestione dei flussi di traffico aereo e il gestore della rete garantiscono che il loro personale sia dotato di nulla osta di sicurezza, se del caso, e si coordinano con le competenti autorità civili e militari per garantire la sicurezza degli impianti, del personale e dei dati.

(d) I fornitori di servizi di navigazione aerea e di gestione dei flussi di traffico aereo e il gestore della rete adottano le misure necessarie per proteggere i propri sistemi, componenti in uso e dati. In caso di minacce alla sicurezza delle informazioni e alla cibersicurezza che potrebbero comportare un'interferenza illegale con la fornitura dei loro servizi, essi si adoperano per prevenire la compromissione della rete.

OBBLIGAZIONI ORIGINARIE DEL FORNITORE DI SERVIZI DI NAVIGAZIONE AEREA

REG. UE 373/2019 E NORMATIVA COLLATERALE – 4) IL «REGOLAMENTO BASICO» 1139/2018

3. SISTEMI E COMPONENTI

3.1. Considerazioni generali

I sistemi ATM/ANS e i componenti ATM/ANS che permettono la trasmissione delle pertinenti informazioni da e verso gli aeromobili e a terra sono adeguatamente progettati, prodotti, installati, sottoposti a manutenzione, protetti dalle interferenze non autorizzate e impiegati in maniera tale da assicurarne l'idoneità allo scopo.

3.3. Progettazione di sistemi e componenti

3.3.1. Sistemi e componenti sono progettati per soddisfare i requisiti applicabili di sicurezza e di *security*.

3.3.4. Sistemi e componenti sono progettati in modo tale da assicurare la protezione degli stessi e dei dati trasportati da interazioni dannose con elementi interni ed esterni.

3.4. Mantenimento del livello di servizio

I livelli di sicurezza di sistemi e componenti sono mantenuti durante il servizio e durante eventuali interventi modifica di quest'ultimo.

OBBLIGAZIONI ORIGINARIE DEL FORNITORE DI SERVIZI DI NAVIGAZIONE AEREA

REG. UE 2015/1998

«1.7 INDIVIDUAZIONE DEI DATI E DEI SISTEMI DI TECNOLOGIA DELL'INFORMAZIONE E DELLA COMUNICAZIONE FONDAMENTALI PER L'AVIAZIONE CIVILE E LORO PROTEZIONE DALLE MINACCE INFORMATICHE

1.7.1. L'autorità competente deve fare in modo che gli operatori aeroportuali, i vettori aerei e gli altri soggetti definiti nel programma nazionale per la sicurezza dell'aviazione civile individuino e proteggano i dati e i sistemi fondamentali di tecnologia dell'informazione e della comunicazione da attacchi informatici che potrebbero pregiudicare la sicurezza dell'aviazione civile.

1.7.2. Operatori aeroportuali, vettori aerei ed altri soggetti devono individuare nel proprio programma di sicurezza, o in qualsiasi documento pertinente cui sia fatto riferimento nel programma di sicurezza, i dati e i sistemi fondamentali di tecnologia dell'informazione e della comunicazione di cui al punto 1.7.1.

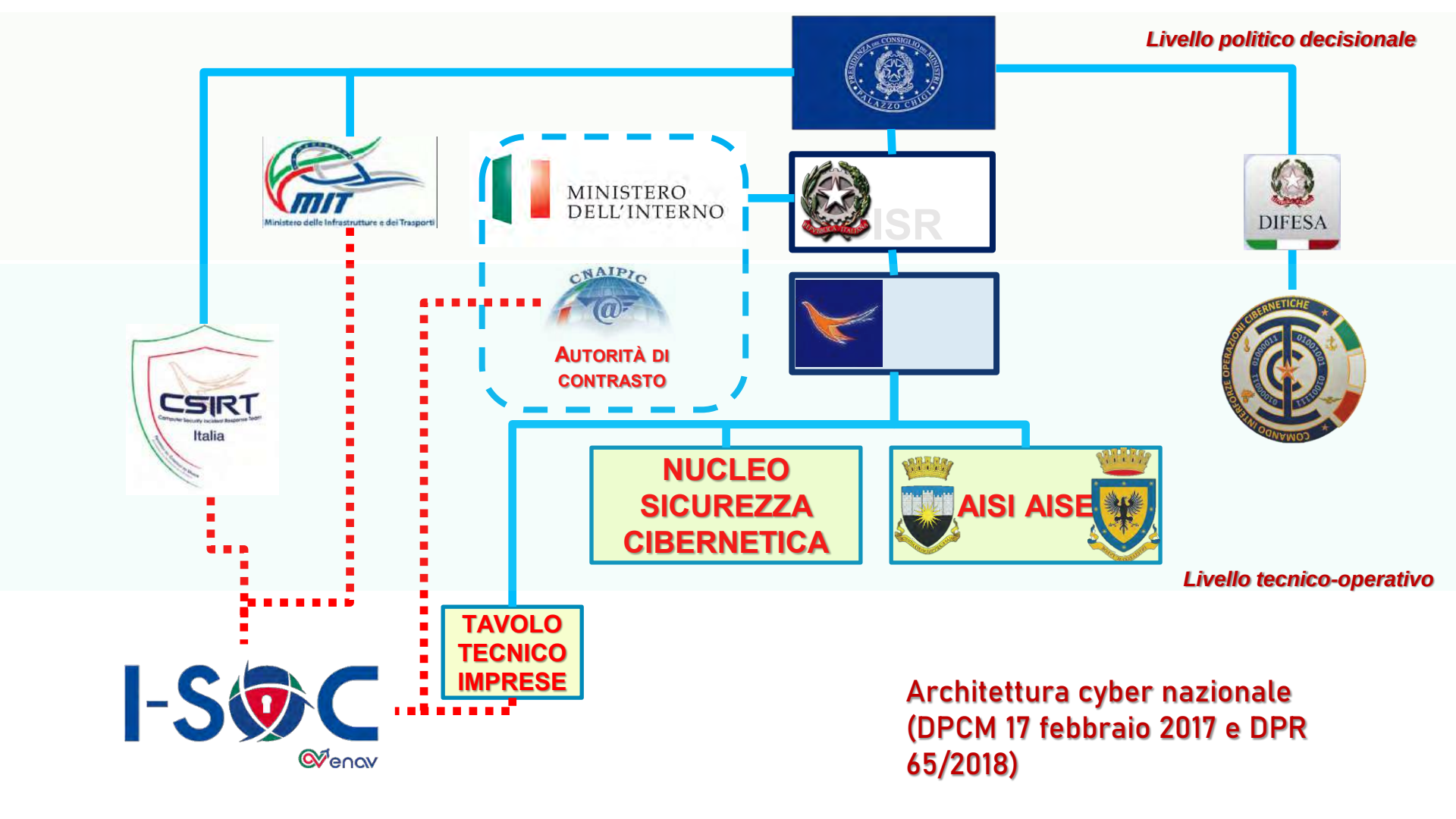
Nel programma di sicurezza, ovvero nel documento pertinente eventualmente indicato nel programma di sicurezza, devono essere descritte in dettaglio le misure protettive predisposte nei confronti degli attacchi informatici, oltre alle misure per il riconoscimento di tali attacchi, come descritto al punto 1.7.1.

1.7.3. Le misure di protezione dettagliate di tali dati e sistemi dalle interferenze illecite devono essere individuate, elaborate e attuate in conformità a una valutazione del rischio effettuata dall'operatore aeroportuale, dal vettore aereo o dal soggetto in questione, a seconda dei casi.

…

1.7.5. Nel caso in cui determinati operatori aeroportuali, vettori aerei e altri soggetti definiti nel programma nazionale di sicurezza dell'aviazione civile soggiacciano ad obblighi di cibersicurezza a parte, derivanti da altre normative dell'UE o nazionali, l'autorità competente può stabilire che al posto delle prescrizioni del presente regolamento debbano essere rispettate le prescrizioni di tali altre normative dell'UE o nazionali. L'autorità competente è tenuta a coordinarsi con le altre autorità competenti al fine di stabilire regimi di controllo coordinati o compatibili.»;

Riferimento al regime della Direttiva NIS e ad iniziative di *security & defence* nazionali


Livello politico decisionale
MIT
Ministero delle Infrastrutture e dei Trasporti
MINISTERO DELL'INTERNO
ISR
DIFESA
CNAIPIC
AUTORITÀ DI CONTRASTO
CSIRT
Italia
NUCLEO SICUREZZA CIBERNETICA
AISI AISE
Livello tecnico-operativo
TAVOLO TECNICO IMPRESE
I-SOC
enav
Architettura cyber nazionale (DPCM 17 febbraio 2017 e DPR 65/2018)

IL 5° DOMINIO DEL WARFARE

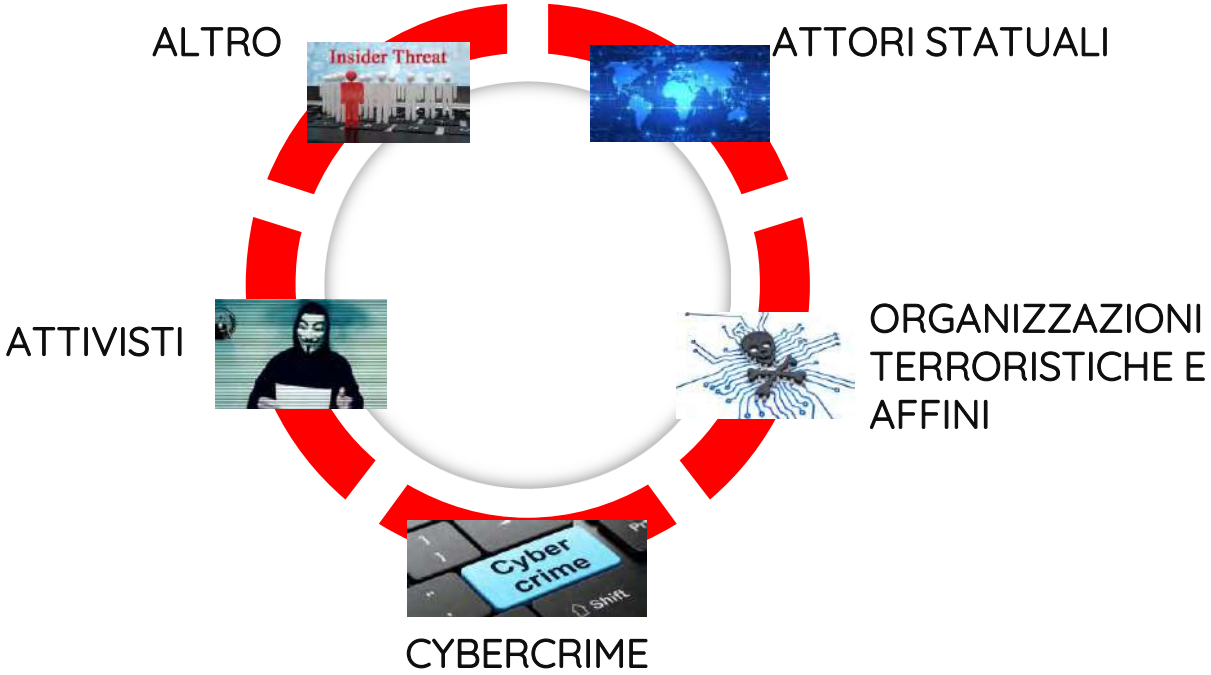
L’evoluzione dei processi di digitalizzazione delle strutture militari e civili rappresenta un’area di vulnerabilità ad alto livello di esposizione, che determina la necessità di un approccio efficace, effettivo, alla sicurezza ed alla difesa degli asset critici di un Paese

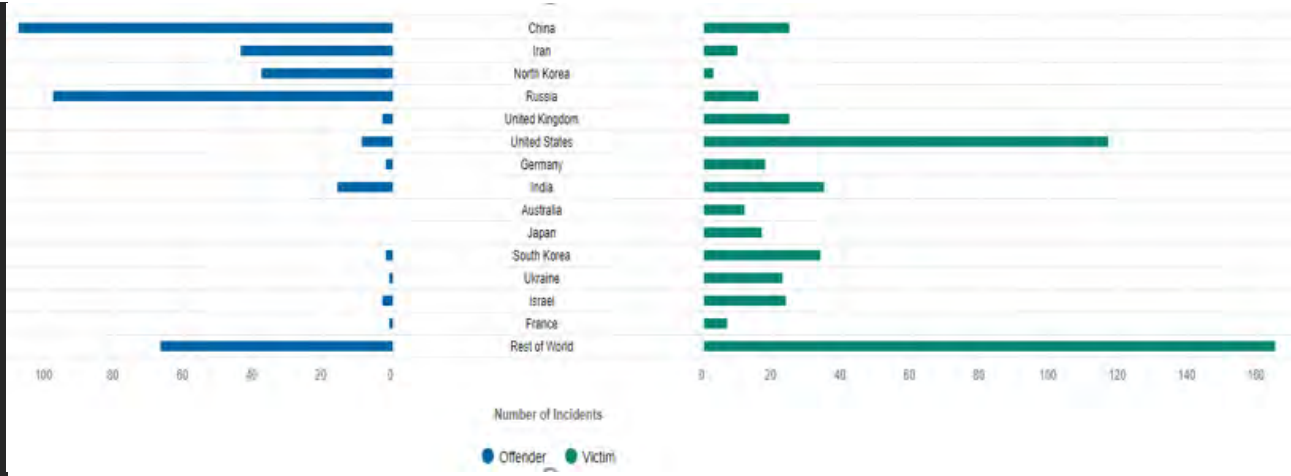
DISPONIBILITA’

INTEGRITA’

RISERVATEZZA

MINACCE COMPLESSE





EVERYWHERE

La dimensione del tema cyber è GLOBALE e coinvolge qualsiasi entità. Nessuno può considerarsi immune

SCENARI RILEVANTI

2007 - ESTONIA

2008 – PRIMO HACKING DEL PENTAGONO
ATTACCO ALLE INFRASTRUTTURE GEORGIA

2009 – WORM CONFICKER

2010 – STUXNET
- OP. AURORA

2011 – DUQU
- SONY/PLAYSTATION
- HACKER SL1NK SU ENTI DIFESA USA/UK
- TIGER-M@TE 700.000 SITI WEB DOWN

2012 – 0XOMAN > 1 MILIONE DI CREDIT CARD SOTTRATTE
- ATTACCO MASSIVO SCADA SU 9 PAESI
- TIGER-M@TE 700.000 SITI WEB DOWN
- MARRIOTT
- FOXCONN
- SAUDI ARAMCO
- LINKEDIN
- RED OCTOBER

2013 – NATO ATTACK
- SOUTH KOREA FINANCIAL ATTACK
- TUMBLR

2014 – INFILTRAZIONE CASA BIANCA
- EBAY
- SOUTH KOREAN NIGHTMARE
- PRIMO GRANDE FURTO BITCOIN
- YAHOO (1)

2015 – ATTACCO ALL'OFFICE OF PERSONAL MGMT USA
(21,5 MILIONI DI DATI PERSONALI INCLUSO DNA)
- TUMBLR
- ASHLEY MADISON
- VODAFONE
- FBI
- HACKING TEAM

2016 – US DEPARTMENT OF JUSTICE
- YAHOO (2) > 1 MILIARDO DI ACCOUNT COMPR.
- LINKEDIN
- ELEZIONI PRESIDENZIALI USA
- DYN DNS
- EYE PYRAMID

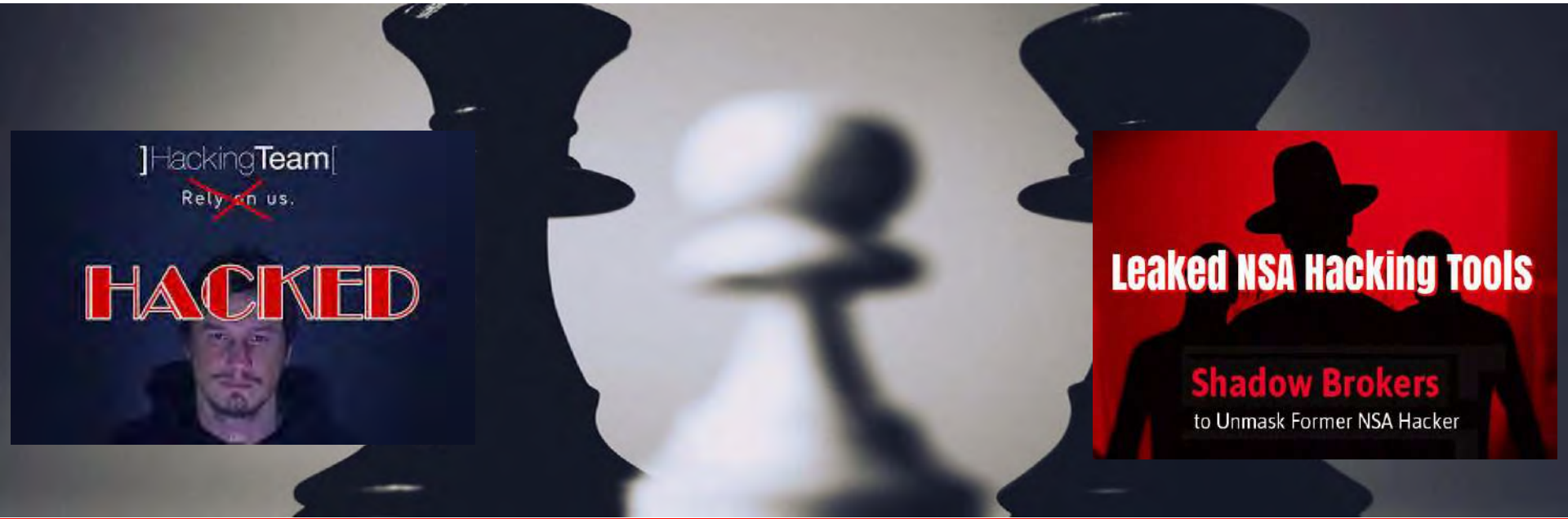
2017 – SHADOW BROKERS
- YAHOO (3) > 3 MILIARDI DI ACCOUNT COMPR
- EQUIFAX
- WANNACRY
- PETYA/NOTPETYA
- CLOUDBLEED

2018 – BRITISH AIRWAYS
- FACEBOOK
- GOOGLE
- CATHAY PACIFIC
- CAMBRIDGE ANALYTICA
- MY HERITAGE
- MARRIOTT
- EU DIPLOMACY COMPRIMISED BY CHINESES
- AVE MARIA (OIL & GAS)

2019 – AIRBUS/CHINA
- NORTH KOREAN BOTNET
- AUSTRALIAN FEDERAL PARLIAMENT (ATTEMPT)
- VISMA NORWAY (CHINA)
- ATTACCHI INFRASTRUTTURE ELETTRICHE USA
- HACKING DATI POLITICI TEDESCHI

2020: ANNUS HORRIBILIS

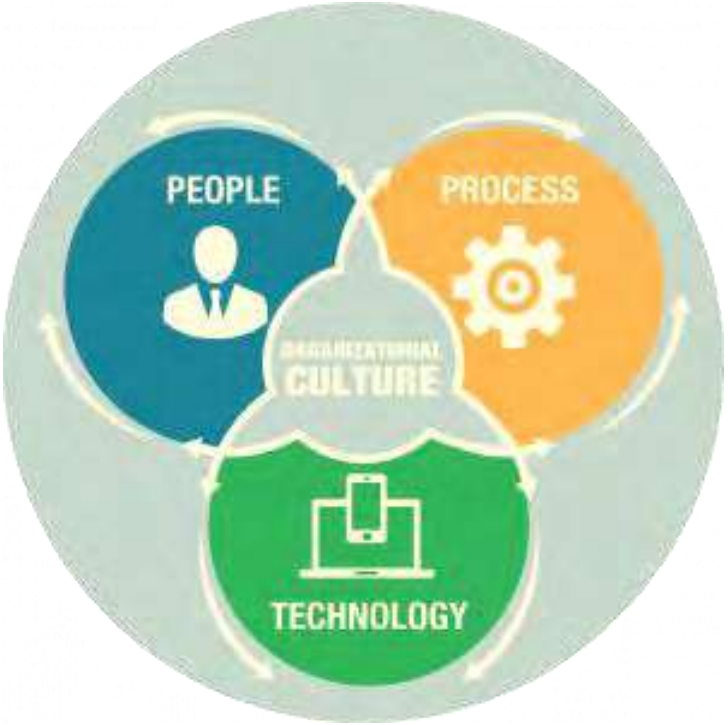
DUE SPECIFICI CASI A CONFRONTO



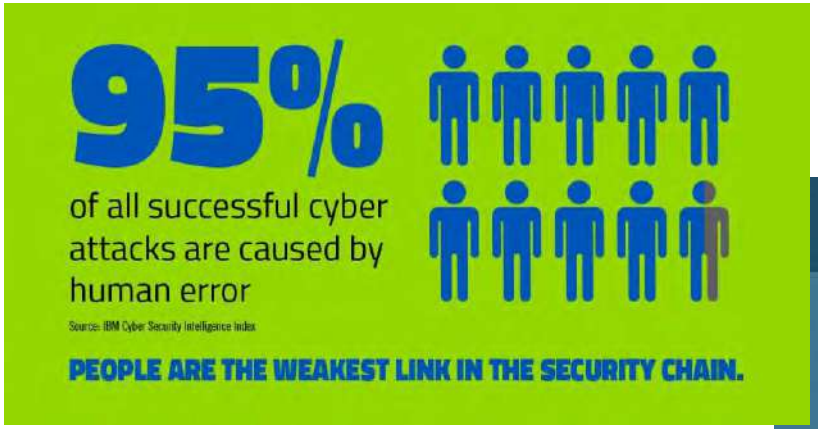
Non è solo una questione di tecnologie

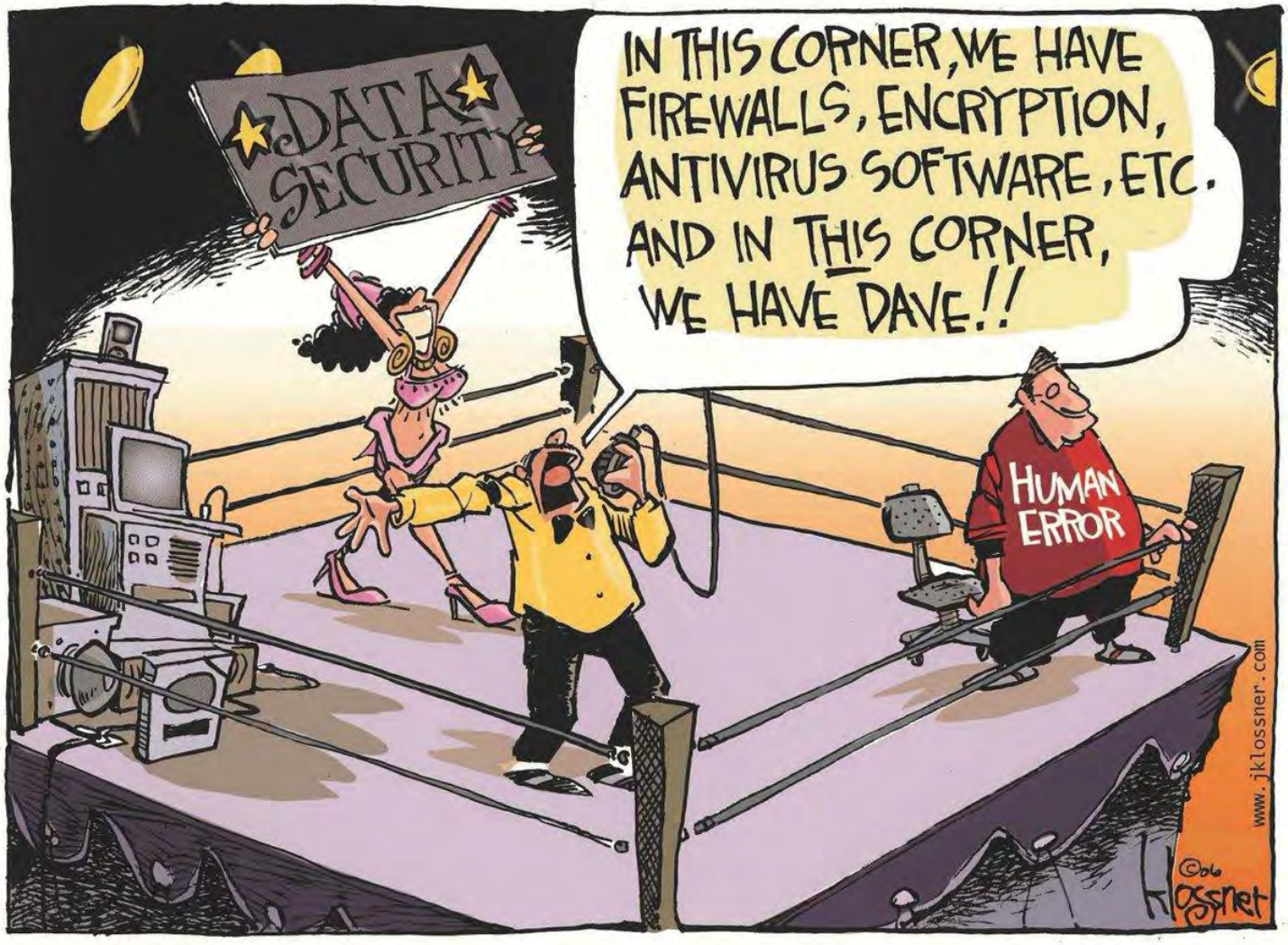
la sicurezza delle informazioni è una disciplina che, in primo luogo, attiene al fattore umano:

- per quanto riguarda gli attori malevoli, perché le azioni di attacco sono il frutto di un'attività intellettiva che costruisce i vettori offensivi studiando tecniche e sfruttando vulnerabilità;
- riguardo ai difensori, perché il fattore umano è un elemento critico di successo in ogni sua sfaccettatura



La centralità del fattore umano




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

Ripensare anche vecchi paradigmi

Tipologie di insider

Malicious insiders

Dipendenti o partner che abusano delle proprie credenziali per motivazioni personali

Inside agents

Attori malevoli interni, reclutati per commettere atti di interferenza illecita contro l'organizzazione

Disgruntled employees

Attori malevoli interni, animati da sentimenti di odio o rivalsa contro l'organizzazione

Careless workers

Dipendenti o partner negligenti, imprudenti, imperiti, o insofferenti verso le regole della security

Third parties

Terze parti che abusano degli accessi consentiti, per arrecare un danno o assumere vantaggi competitivi

Fonte: Verizon

La complessità dell'approccio al rischio «insider»

LIMITI AI PROCESSI DI BACKGROUND CHECK

L'attività svolta nelle infrastrutture landside è sottratta al regime del tesseramento aeroportuale

COSTI DELLE MISURE DI SICUREZZA

La security implica costi che si ribaltano sul Servizio e non sempre vi è la percezione del ritorno degli investimenti

PRIVACY

Oggettivi limiti di analisi di elementi della vita privata, connessi al rispetto della riservatezza dei dati personali

COORDINAMENTO CON LE FORZE DI POLIZIA

Limiti all'attuazione delle previsioni del Reg. UE 1035/2011

TUTELE DELLA DISCIPLINA GIUSLAVORISTICA

Limiti derivanti dal rispetto della normative in materia di controlli a distanza

COINVOLGIMENTO DEL PERSONALE

Necessità di coinvolgimento del personale nei processi di security, per il radicamento di un concetto culturale di "protezione"

Un tema aperto: la radicalizzazione

Con il regolamento 103/2019 viene introdotto un tema controverso, la «radicalizzazione», definita come *il fenomeno della "socializzazione all'estremismo" che vede persone abbracciare opinioni, punti di vista e idee che potrebbero condurre ad atti terroristici* (modifica al punto 11.0.8 del Reg. UE 1198/2015)
Si introduce un obbligo specifico di valutazione del rischio, per considerare il potenziale vettore di minaccia, le vulnerabilità e gli impatti in relazione al contesto complessivo dell'aviazione civile

Radicalizzazione e minaccia cyber

Le organizzazioni terroristiche hanno dimostrato un interesse notevole per il mondo cyber, ma maggiormente rispetto ai temi della «sicurezza passiva» attraverso l'uso di piattaforme di comunicazione sicura e utilizzo di tecniche di hacking su siti web, per veicolare messaggi di propaganda e proselitismo.

Ciò non di meno, l'attenzione verso le possibili capacità dell'antagonista va tenuta alta

Definiamo la sicurezza delle informazioni

La sicurezza delle informazioni è un processo strutturato che consiste in un insieme di attività - o sottoinsieme di processi - che includono la gestione del personale, la gestione del rischio, la dimensione dei controlli, in un'ottica di continuo miglioramento.

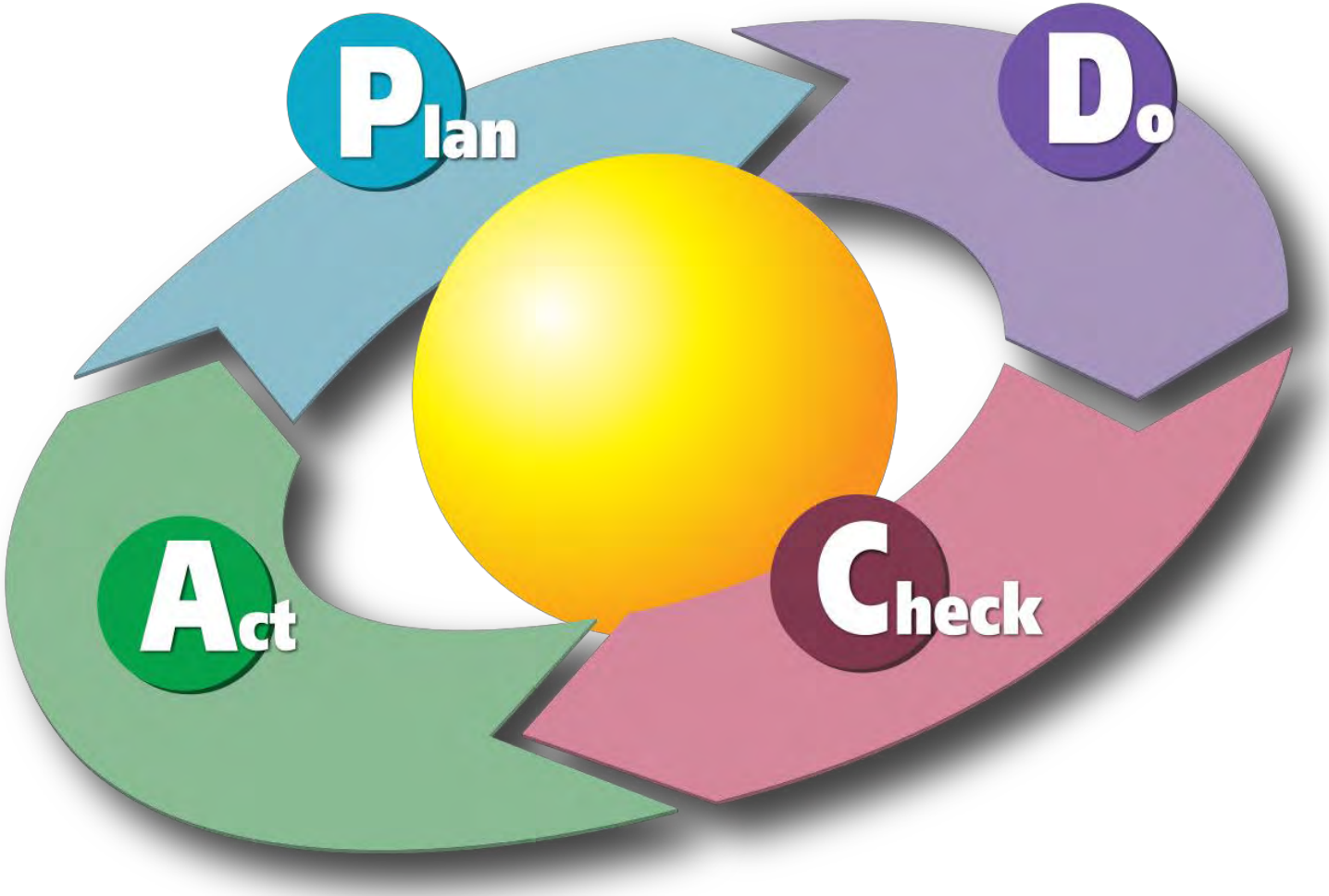
La sicurezza delle informazioni è un processo ciclico, iterativo, inarrestabile, che tende al continuo miglioramento e che richiede, in primo luogo, la comprensione dei rischi e, poi, la loro continua gestione, in una logica razionale, scientificamente orientata e basata, in maniera chiara, sull'adesione del vertice organizzativo

Da non dimenticare!!!

Sicurezza fisica e sicurezza logica non sono due mondi separati. Non può esistere sicurezza logica senza sicurezza fisica e la sicurezza fisica dipende dalla sicurezza logica.

Indispensabile valutare le convergenze e considerare, inoltre, la sicurezza fisica come ampliata anche ad eventi naturali o accidentali


DATA CENTER
SECURITY


Plan
Do
Check
Act

IL CONTESTO

Conoscere i requisiti di protezione e gli obiettivi della protezione

La governance e il contesto

Non si può determinare una strategia di protezione delle informazioni se non si identificano esattamente i “requisiti di protezione”, ossia rispondere alle domande:

- cosa bisogna proteggere
- perché bisogna farlo
- se esistano regole esterne e quali requisiti bisogna soddisfare
- se vi siano terze parti coinvolte: persone, clienti, fornitori

La Governance e il contesto (segue)

Attraverso l'analisi di contesto si definiranno:

a. le norme cogenti, che devono essere rispettate, per garantire che l'organizzazione sia rispettosa delle regole imposte dallo Stato, dagli Enti intermedi, dalle Autorità di Regolazione
b. gli input anche per l'analisi del rischio, dovendosi valutare espressamente i rischi di *compliance* che possono gravare sull'organizzazione;
c. gli elementi organizzativi e materiali che saranno necessari per il rispetto dei requisiti di contesto, interni ed esterni;
d. le aspettative degli altri soggetti, inclusi i lavoratori e la collettività.

Un esempio

Articolo 32

Sicurezza del trattamento

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

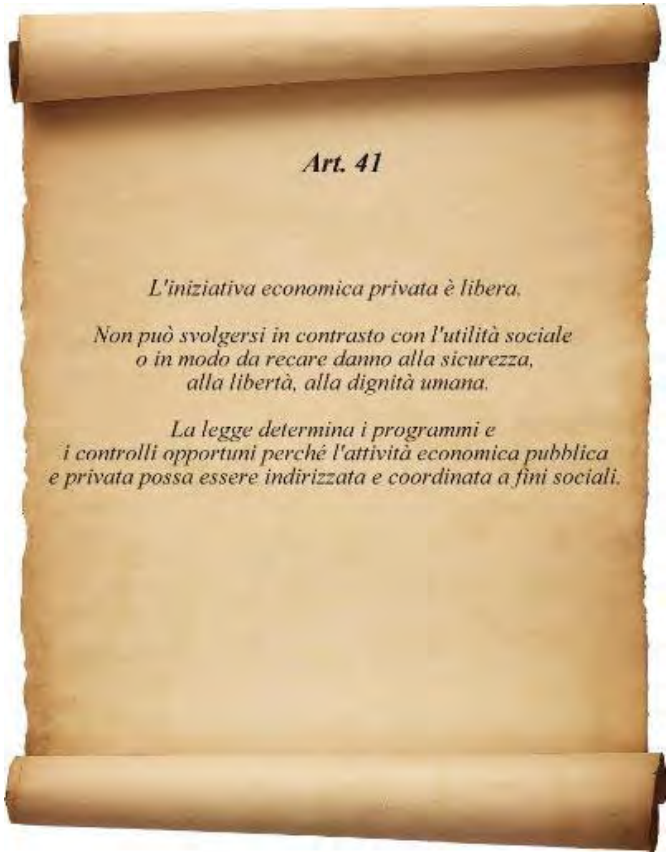
2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei **rischi presentati** dal trattamento che derivano in particolare dalla **distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso**, in modo accidentale o illegale, a dati personali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

3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

L'art. 32 del GDPR fornisce un chiaro esempio di requisito cogente.
La norma indica soltanto gli obiettivi della sicurezza del trattamento e l'elemento centrale precettivo: "*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…*".
Come raggiungere gli obiettivi spetta al titolare e al responsabile

Il “Duty of care”



la Security Governance non è soltanto una necessità di business.

Nell’esercizio delle attività quotidiane, l’impresa assume diversi tipi di obblighi, contrattuali e legali,che costituiscono una “posizione di garanzia” nei confronti di diversi soggetti: clienti, dipendenti, pubblico indistinto
la protezione dei dati personali crea una di queste posizioni di garanzia, che obbliga le organizzazioni e le imprese all’adozione di misure di protezione
“Non impedire un evento, che si ha l’obbligo giuridico di impedire, equivale a cagionarlo” (art. 40 comma 2 del Codice Penale

Scopo della Governance

lo scopo della governance della sicurezza delle informazioni è quello di stabilire, mantenere ed aggiornare un programma della sicurezza alle necessità dell'organizzazione e si riferisce ad una serie di attività definite ed organizzate per sviluppare idonei controlli di sicurezza al fine di proteggere l'organizzazione

La governance deve avere a riferimento alcuni elementi fondamentali tra i quali:

a. le risorse non sono infinite ed è quindi necessario agire per priorità
b. la security è fatta anche di regole, che devono promanare dal vertice e seguire appropriati ruoli e responsabilità
c. è necessario misurare i risultati

Elementi ed attività per la security governance

OBIETTIVI - i livelli desiderati o gli stati finali, espressi in maniera chiara, sostenibile e misurabili

STRATEGIA - “come” raggiungere gli obiettivi

LE REGOLE - allineate alla missione, riflettono gli obiettivi e fissano le modalità di processo

PRIORITA’ - obiettivi, strategie e missione organizzativa devono definire, in un ambiente a risorse limitate, le priorità da perseguire

PROCESSI - le attività che costituiscono l’espressione delle operazioni di security vanno formalizzate e devono contenere le istruzioni per i destinatari attraverso procedure

CONTROLLI -la descrizione delle attività critiche per assicurare gli obiettivi di security

MISURAZIONE - la descrizione di come processi, controlli e risultati vengono misurati e riportati al vertice dell’organizzazione

Programmazione e gestione

Quanto sopra non può che tradursi in un programma, che consiste in una pianificazione, che dovrà essere gestita esattamente con le logiche del program management, quindi con una maniacale attenzione ad obiettivi, tempistiche, risorse (umane e materiali), gestione dei "percorsi critici", contabilizzazione e reporting, per consentirne effettività, coerenza alla missione dell'organizzazione e connotare l'attività per la giusta rilevanza e responsabilità

Image credit: Constantin Agafonov

Elementi chiave

Per proteggere un'organizzazione, non possono mancare alcuni elementi chiave, che devono caratterizzare il "Security Management System":

GESTIONE DEL RISCHIO - assicurare che i rischi che possano pregiudicare l'organizzazione siano identificati; le vulnerabilità individuate e le azioni per ridurle a livelli accettabili siano definite e formalizzate

MIGLIORAMENTO DEI PROCESSI - assicurare che vengano imposti i necessari cambiamenti organizzativi e di processo per il raggiungimento degli obiettivi

IDENTIFICAZIONE DEGLI EVENTI - la capacità dei sistemi tecnologici e degli associati processi di rilevare, comprendere i rilevanti eventi di sicurezza, nel più breve tempo possibile

CAPACITA' DI RISPOSTA - l'attuazione di tutte le misure necessarie per prevenire gli incidenti, ridurne l'impatto e la probabilità, migliorare la capacità di risposta per ridurre al minimo gli effetti negativi sull'organizzazione

Elementi chiave - segue

CONTINUITA' OPERATIVA - nella consapevolezza dell'impossibilità di avere 100% di sicurezza, adottare le misure per garantire i processi di continuità e il ripristino in caso di eventi avversi

METRICHE - identificare ed applicare modalità di misurazione per verificare l'effettività del sistema di gestione

GESTIONE DELLE RISORSE - come eseguire il programma è anche questione di risorse umane e materiali, che devono essere definite ed allocate

MIGLIORAMENTO CONTINUO - il processo è trasversale all'intera organizzazione e deve tendere al conseguimento di obiettivi sempre più sfidanti, conformi alle attese degli "stakeholders"

la compliance

Art. 6 D. Lgs. 231/01. Soggetti in posizione apicale e modelli di organizzazione dell'ente

1. Se il reato è stato commesso dalle persone indicate nell'articolo 5, comma 1, lettera a), l'ente non risponde se prova che:

a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;

b) il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;

c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;

d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b).

un sistema di gestione efficace deve essere in grado di rispondere in maniera effettiva agli obblighi di leggi regolamenti, ordini e discipline.
un efficace sistema di gestione è il modo concreto con cui le organizzazioni possono evitare le conseguenze di azioni illecite, dei propri dipendenti o anche di terzi, che possano riverberare a danno degli interessati

Dolo e colpa

Articolo 43 del Codice penale:

Il delitto:

è doloso [c.p. 133], o secondo l'intenzione, quando l'evento dannoso o pericoloso, che è il risultato dell'azione od omissione e da cui la legge fa dipendere l'esistenza del delitto, è dall'agente preveduto e voluto come conseguenza della propria azione od omissione

....

è colposo, o contro l'intenzione, quando l'evento, anche se preveduto [c.p. 61, n. 3], non è voluto dall'agente e si verifica a causa di negligenza o imprudenza o imperizia, ovvero per inosservanza di leggi, regolamenti, ordini o discipline

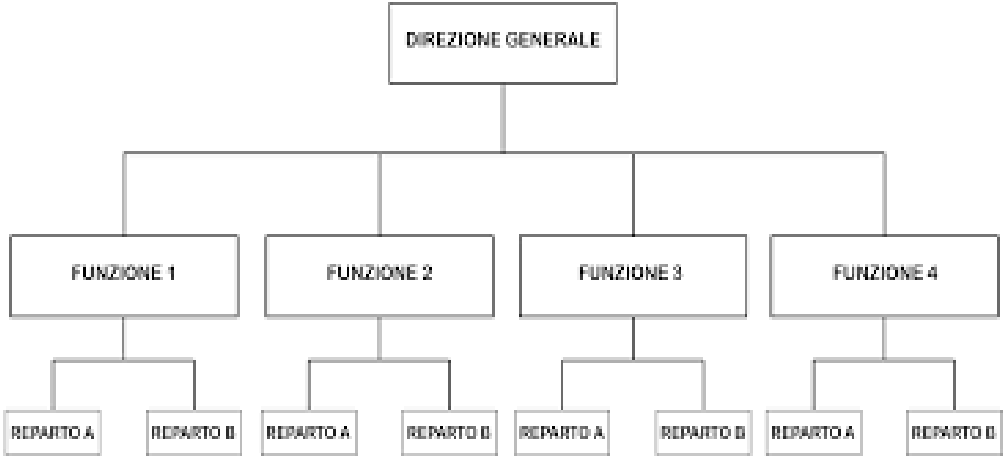
...

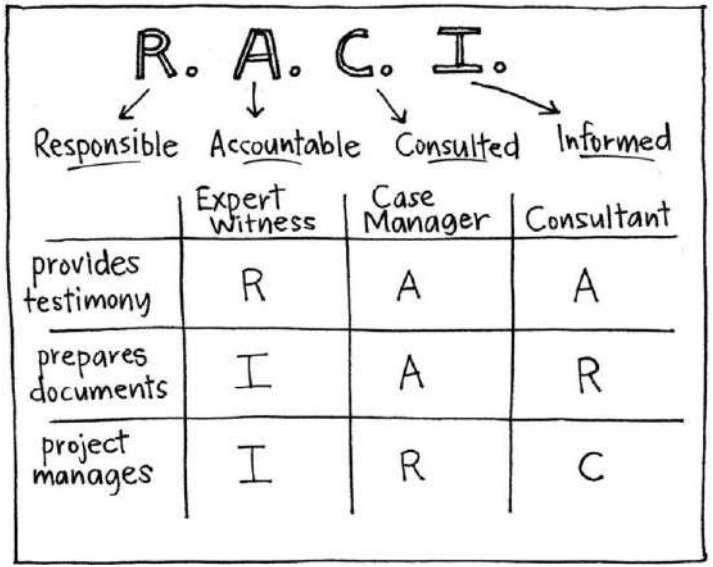
Ruoli e responsabilità

In un'organizzazione è sempre indispensabile, per l'effettivo conseguimento degli obiettivi, identificare i ruoli di ciascun attore del sistema, chiarendo allo stesso le effettive mansioni, cosa ci si aspetti in termini di obbligazioni professionali e risultati

Il "ruolo" è l'esatta individuazione della posizione operativa che la persona fisica ha all'interno dell'organizzazione, assegnata o dal posizionamento in organigramma o nel suo inquadramento organizzativo
la "responsabilità" descrive invece le attività dovute dal soggetto organizzativo, a qualunque livello, quale misura della prestazione e termine di riferimento della diligenza attesa

A livello descrittivo





In concreto:

“**Responsabile**”: la persona (o la struttura organizzativa) che è chiamato a svolgere l’effettivo incarico

“**Accountable**”: la persona, con poteri decisionali, che è effettivamente chiamata a rispondere per la corretta, accurata e tempestiva esecuzione del processo

“**Consultato**”: la persona o la struttura organizzativa che può o deve contribuire, per conoscenze o competenze o per una particolare posizione all’interno dell’organizzazione, alla definizione del lavoro

“**Informato**”: Uno o più soggetti o strutture organizzative cui va fornita informazione delle attività

La “Segregation of duties” e i conflitti di interesse

Non è possibile che una stessa persona o una stessa organizzazione svolga tutti i compiti di un’attività complessa. La struttura IT non può essere al tempo stesso il soggetto che decide i requisiti, che sceglie il contraente, che pone in essere il servizio, lo esercisce, lo verifica lo corregge e ne cura la sicurezza. E’ evidente che se ciò fosse, mancherebbe la necessaria terzietà in ruoli ben distinti ed in evidente conflitto di interesse.

La separazione dei compiti nella sicurezza IT è uno dei modi più basilari per proteggere il tuo ambiente. ISO / IEC 27001 richiede la separazione dei compiti e delle responsabilità potenzialmente in conflitto. In questo modo, l’organizzazione riduce il rischio di modifiche o usi impropri sia dannosi che accidentali. Inoltre, lo standard incorpora questi compiti e aree in conflitto come parte della valutazione del rischio in corso.

Alcuni esempi di ruoli e responsabilità

COSTRUIRE L'INFORMATION SECURITY MANAGEMENT SYSTEM

In questa parte parleremo di

standardizzazione
Leadership
policy
Obiettivi di sicurezza delle informazioni
Pianificazione per il conseguimento degli obiettivi
Creazione della struttura di supporto e in particolare

- gestione delle risorse
- competenze
- consapevolezza
- comunicazione

la gestione della documentazione

Perché la standardizzazione (e perché certificarsi)

Uno standard è l'identificazione di regole ed esperienze generalmente (e internazionalmente) riconosciute idonee a conseguire obiettivi, nel nostro caso di sicurezza. Esse corrispondono a "*best practices*" identificate e, nell'ordinamento giuridico, dono "lo stato dell'arte" o le "discipline" idonee a misurare la diligenza.
Seguire uno standard e magari certificarsi presenta diversi vantaggi:

- è la dimostrazione esterna di processi di qualità seguiti ed è un mezzo per rafforzare la fiducia verso l'organizzazione. Se certificati, un organismo indipendente verifica l'effettivo rispetto delle clausole di cui consta lo standard
- è un valido strumento per dimostrare, in caso di incidenti o di controversie anche contrattuali, il parametro della diligenza, della prudenza e della perizia;
- è uno strumento di aggregazione organizzativa, perché coinvolge tutta l'organizzazione nell'adesione ai processi indirizzati verso il continuo miglioramento;
- riduce la necessità di audit nei rapporti tra le parti, quando la certificazione indipendente garantisce idonei livelli di confidenza

è lo standard più diffuso in Europa ed in molti Paesi del mondo e fa parte di una famiglia di standard che hanno un tratto in comune: essere tutte "*Risk Based*"ossia fornire criteri, misure e controlli per fronteggiare i rischi. A questo ci si riferirà

esistono altri standard, o insiemi di standard, in particolare nel mondo anglosassone e specificamente quello statunitense, dove esiste un istituto pubblici di standardizzazione, il NIST, *National Institute of Standards and Technology* (e anche un'organizzazione federale indipendente di auditing, il GAO - *Government Accountability Office*)

Alcune assunzioni

La materia della gestione del rischio non rientra in questa lezione.
Assumiamo quindi per consolidati:

a. la definizione dell'ambito dell'analisi del rischio
b. la metodologia adottata
c. l'identificazione delle minacce
d. l'identificazione delle vulnerabilità
e. le opzioni di trattamento
f. il processo iterativo della gestione del rischio

Un “*caveat*” sull’analisi del rischio

L’analisi del rischio richiesta dalla normativa Privacy è elemento ben diverso da quella prevista da un sistema di gestione della sicurezza delle informazioni
Nell’analisi del rischio privacy devono essere valutati i rischi privacy, ossia quelli che hanno o possono avere effetti pregiudizievoli sui “dati personali” e quindi mettere a repentaglio diritti individuali personali.
Nell’analisi del rischio della sicurezza delle informazioni i rischi da valutare sono quelli che possono pregiudicare la disponibilità, l’integrità e la riservatezza delle informazioni, a prescindere dalla natura di esse.
Inoltre il rischio privacy attiene anche alle modalità di trattamento del dato, che si assume debba essere gestito nei limiti della legittimità e del consenso prestato mentre questo elemento è assente dalla valutazione di security

leadership

Un sistema di gestione è destinato al fallimento se non riceve dal management, in particolare dal vertice delle organizzazioni, l'appropriato supporto. La norma di standardizzazione richiede che questo supporto (l*eadership and commitment*) venga definito e comunicato, all'interno ed all'esterno:

a. definendo l'information security policy e i relativi obiettivi con chiarezza e resi compatibili con le strategie organizzative:
b. assicurando l'integrazione del sistema di gestione della sicurezza delle informazioni nei processi organizzativi
c. assicurando le risorse (umane e materiali) necessarie;
d. comunicando l'importanza del sistema di gestione della sicurezza delle informazioni e la rilevanza di una sua effettiva attuazione da parte di tutti i membri dell'organizzazione
e. assicurando che il sistema di gestione della sicurezza delle informazioni possa raggiungere i suoi obiettivi
f. dirigendo e sostenendo l'organizzazione ed i responsabili nell'attuazione effettiva
g. promuovendo il miglioramento continuo
h. stimolando tutto il management a dimostrare il loro supporto al conseguimento degli obiettivi

leadership - segue

la dimostrazione della leadership è permanente, tuttavia vi sono alcuni momenti fondamentali della vita organizzativa nei quali la dimostrazione è ancora più evidente:

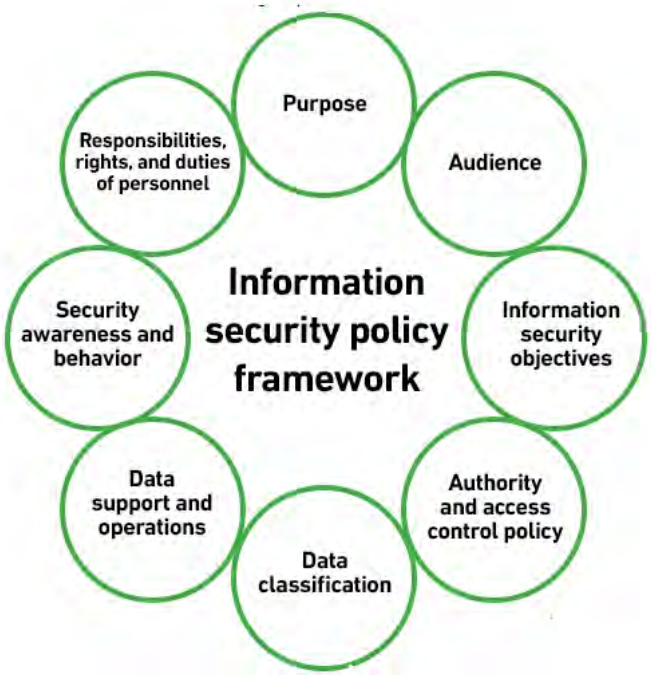
- nei rilasci e negli aggiornamenti della Information Security Policy, quando l'affermazione dell'importanza e cogenza dei principi deve essere evidente ed indiscutibile
- nei rilasci ed aggiornamenti delle procedure e delle regole discendenti;
- nella comunicazione interna ed esterna
- nell'atto fondamentale della vita di ogni sistema, che è il "Riesame della Direzione", nel quale il top management è chiamato a *riesaminare il SGSI dell'organizzazione [...] per accertarsi che lo stesso continui a rivelarsi idoneo, adeguato ed efficace*.

Ambito di applicazione

Nell'attività di pianificazione "plan" rientra, come primo passo la definizione dell'ambito di applicazione , definito nella clausola 4.3 e che richiede che l'organizzazione 'determini i confini e l'applicabilità del sistema di gestione della sicurezza delle informazioni per stabilirne l'ambito d'applicazione [prendendo in considerazione] le problematiche interne ed esterne, le esigenze [delle parti interessate, e] le interfacce e le dipendenze tra le attività svolte dall'organizzazione e quelle svolte da altre organizzazioni'.

Più nel dettaglio, l'ambito di applicazione deve definire a cosa si applichi il sistema di gestione e cosa ne sia fuori, analizzando anche i rischi derivanti da un'inclusione troppo ampia o troppo limitativa

Policy



La politica è un documento chiaro,, esplicito e formale, comunicato a tutti, che rappresenta il "programma della sicurezza delle informazioni. Il suo scopo è quello di fornire gli indirizzi ed esplicitare il supporto della direzione per la sicurezza delle informazioni ed è una espressa adesione ai valori ed alle norme

Secondo la clausola 5.1.1. la policy dovrebbe fornire "*l'approccio dell'organizzazione per la gestione dei propri obiettivi per la sicurezza delle informazioni*" avendo chiaro anche l'obiettivo di rendere il processo di security agevole, coerente con la missione dell'organizzazione e di obbligatoria applicazione

Policy e obiettivi

Il sistema di gestione della sicurezza delle informazioni identifica gli obiettivi di protezione e questi obiettivi devono essere indicati, ad alto livello, nella policy

A partire dagli obiettivi di gestione dei rischi,di compliance, di gestione delle risorse e della cultura della sicurezza, gli obiettivi sono l'esplicitazione degli intendimenti organizzativi, che trovano nell'allegato A della norma e, se del caso, in quelli della ISO 27002, la loro puntuale applicazione

pianificazione degli obiettivi

nel pianificare i propri obiettivi, ogni organizzazione deve chiarire:

- cosa sarà fatto
- quali risorse sarà necessario utilizzare
- chi ne sarà responsabile
- quando sarà completato
- come saranno valutati i risultati

A cosa serve un processo strutturato di «Program/Project Management»?
E che significato ha in in sistema di gestione della sicurezza delle informazioni?

Il progetto come identificazione di uno scopo

Avere chiaramente in mente qual è la finalità di un progetto, cosa si vuole conseguire con esso, è essenziale ed è la chiave per rendere efficiente la gestione di un programma, sia esso di investimento che di esercizio

Un progetto è un'attività complessa che richiede considerazione per:

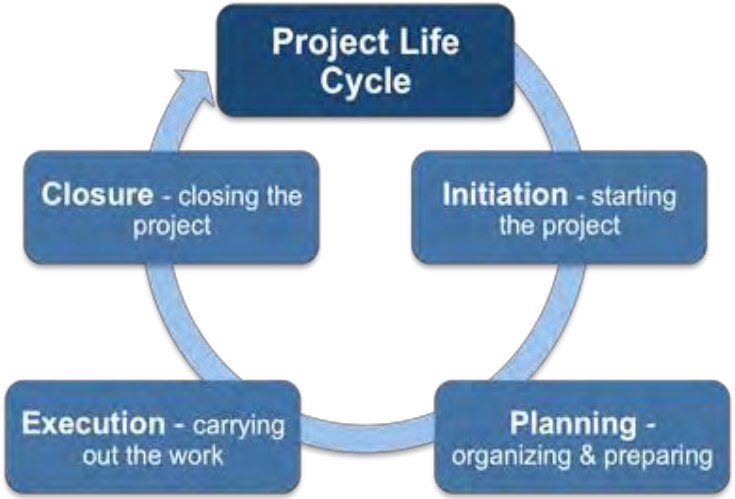
a. I costi associati (budget) ed il relativo controllo;
b. Uno scopo, chiaramente definito in termini di obiettivi e risultati
c. La misura delle performances

Il Project Management implica la necessità di facilitare le attività che sono necessarie per il raggiungimento degli obiettivi.

Program management ≠ lavoro individuale

il program management implica necessariamente l’orchestrazione di un team e di un insieme di processi e risorse

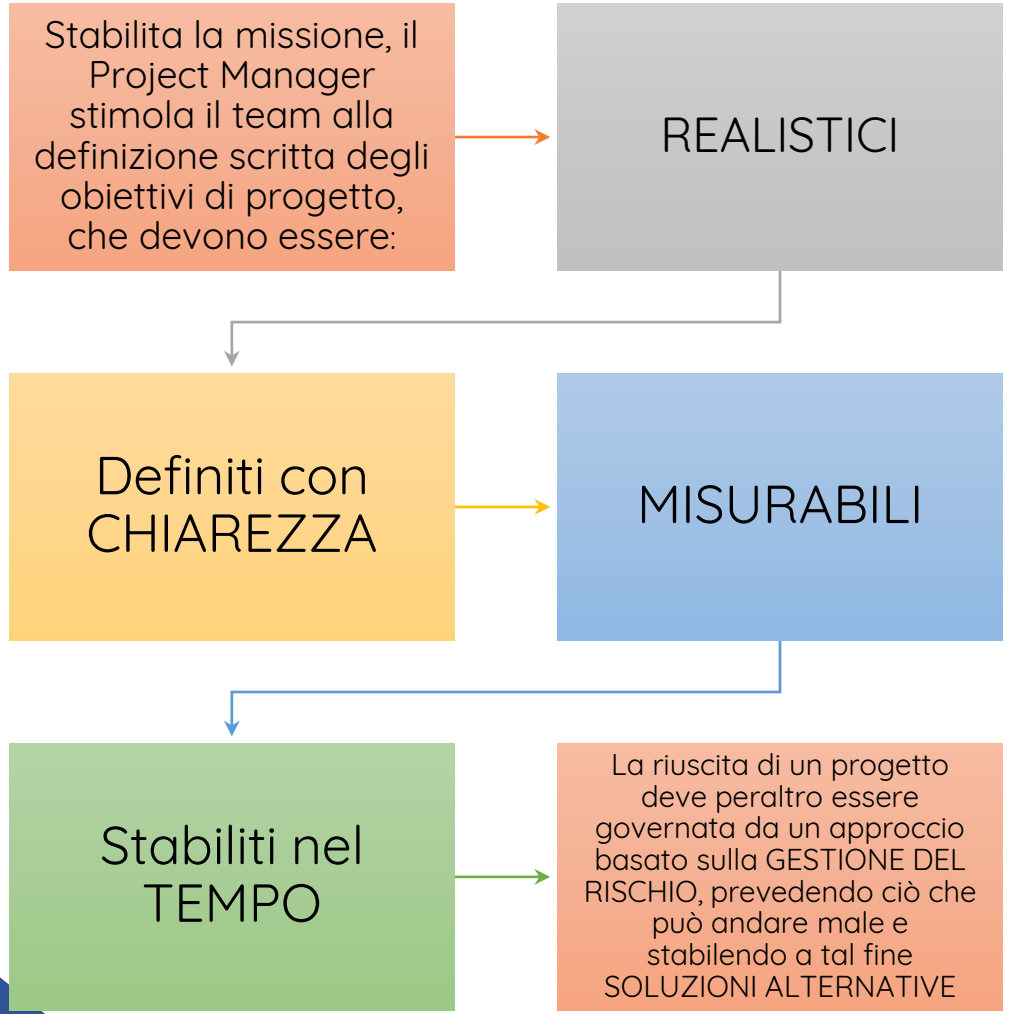
Il ciclo di vita di un progetto



Vi sono quattro fasi di un progetto:

1. Definizione
2. Pianificazione
3. Esecuzione
4. chiusura

Visione olistica, realistica e basata sulla gestione del rischio



Mantenere il controllo dei progetti

«La quantità di progetti che sforano costi e tempi è il dramma della nostra azienda» (un CEO a caso)

In realtà non sono i progetti ad andare male, ma la capacità del program management che può migliorare, quando siano stabiliti dei solidi e tempestivi **presidi di controllo** che anticipino i possibili problemi di sforamento dei costi e tempi.

Questo può tuttavia implicare la necessità di un investimento iniziale per la formazione e per il supporto tecnico.

Supporto

la security non è un fungo che nasce spontaneo. Occorrono capacità, risorse, effort. L'organizzazione dimostra la sua effettiva adesione al modello del continuo miglioramento fornendo le risorse effettivamente necessarie alla costruzione, all'implementazione, al mantenimento ed al continuo miglioramento (clausola 7.1)

ma non basta.

competenze e conoscenze

la sicurezza delle informazioni non si inventa e non si improvvisa. L'organizzazione dovrà:

a) individuare e determinare le competenze necessarie delle persone coinvolte in processi che possano avere impatto sulla sicurezza delle informazioni
b) assicurare che tali persone abbiano effettivamente le competenze necessarie per background, esperienza o training;
c) in caso di mancanza, provvedere all'appropriato addestramento, valutandone l'efficacia

questo, come altri processi, dovrà essere opportunamente documentato e tracciato

Consapevolezza

La sicurezza delle informazioni è prima di tutto un processo culturale e la consapevolezza dei rischi, delle misure di sicurezza e degli obiettivi di security deve permeare tutta l'organizzazione.
Il personale deve in particolare acquisire consapevolezza:

- della security policy
- del contributo di ciascuno e di tutti all'effettività del sistema nell'interesse dell'organizzazione, dei singoli e di tutti gli interessati;
- delle implicazioni che possono derivare dalla negligenza, imprudenza o imperizia riguardo alle misure del sistema di gestione della sicurezza delle informazioni

Comunicazione

nel mondo contemporaneo la sicurezza passa anche attraverso i processi comunicativi - interni ed esterni - ed ogni organizzazione deve riflettere sulla maniera più appropriata per comunicare, nell'ordinario, per trasmettere sicurezza, come nelle fasi della gestione delle emergenze e delle crisi.
Questa vera e propria arte deve concentrarsi su diversi punti:

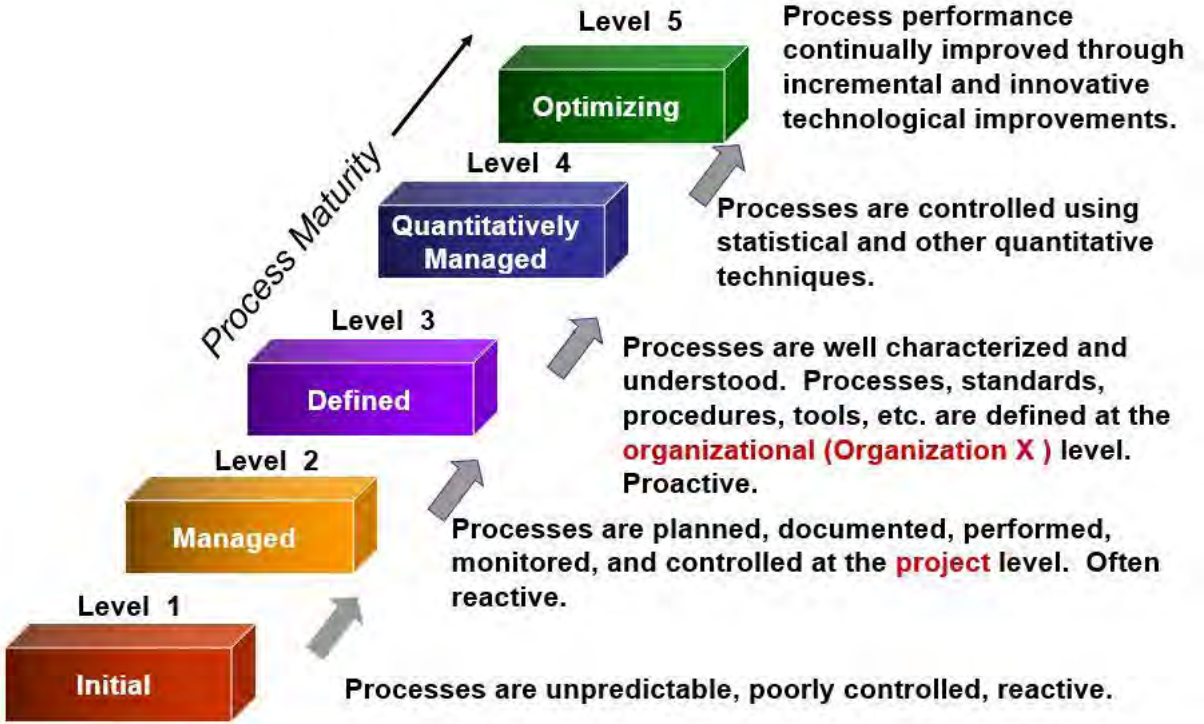
- cosa comunicare
- quando comunicare
- quali sono i destinatari del messaggio
- chi deve comunicare
- gli effetti potenziali della comunicazione

Focus sulla documentazione

La maturità di un'organizzazione si dimostra attraverso fatti concludenti e la possibilità di verificare i processi, la loro ripetibilità, il modo con il quale sono tracciate le informazioni e rese disponibili, secondo il principio del "need to know" e costantemente aggiornate.

Questo principio, comune a tutte le norme basate sulla matrice ISO 9001, deve essere osservato sin dalla fase della pianificazione del sistema di gestione e deve ispirare l'intero suo ciclo di vita

sviluppo del SGSI e maturità

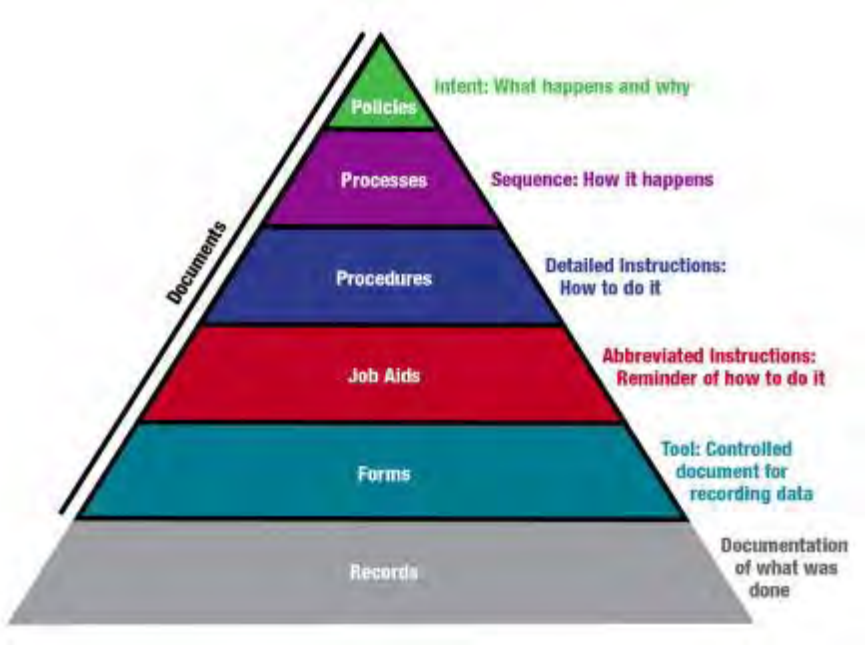


La maturità dei processi e dell'organizzazione complessivamente considerata trova un suo diretto riflesso nella documentazione. La documentazione non è un orpello, ma riflette la capacità dell'organizzazione di definire, applicare e migliorare i propri processi

Documenti e registrazioni

La norma ISO 27001 distingue tra:

- “documenti”, intesi genericamente come elementi scritti che riguardano principi, regole, processi, procedure e quanto altro necessario a descrivere il sistema di gestione; e
- “registrazioni”, quali rappresentazioni scritte di eventi rilevanti, di cui è necessario trattenere memoria in forma documentata



adattato da WHO - Quality Training Module 16

Requisiti per la documentazione

Vi sono documenti che la norma ISO 27001 richiede come obbligatori ed altri che dovranno essere redatti, in ragione della natura e della dimensione e complessità dell'organizzazione, per garantire l'efficacia del sistema di gestione.

Creazione e aggiornamento

nel creare o aggiornare i documenti sarà necessario provvedere:

a) all'identificazione e descrizione del contenuto e degli altri elementi rilevanti
b) il formato e il supporto di conservazione (digitale o cartaceo)
c) il processo di revisione e di approvazione

Ciclo di vita

La documentazione deve essere tenuta sotto controllo per garantirne la disponibilità, l'adeguatezza, la protezione quando la conoscenza dei contenuti sia ristretta a determinati persone e il controllo sui cambiamenti, per assicurare che i contenuti siano aggiornati, coerenti e sia in uso l'ultima versione

la documentazione obbligatoria

Per la ISO 27001:2017 vi sono alcuni documenti obbligatori. essi sono:

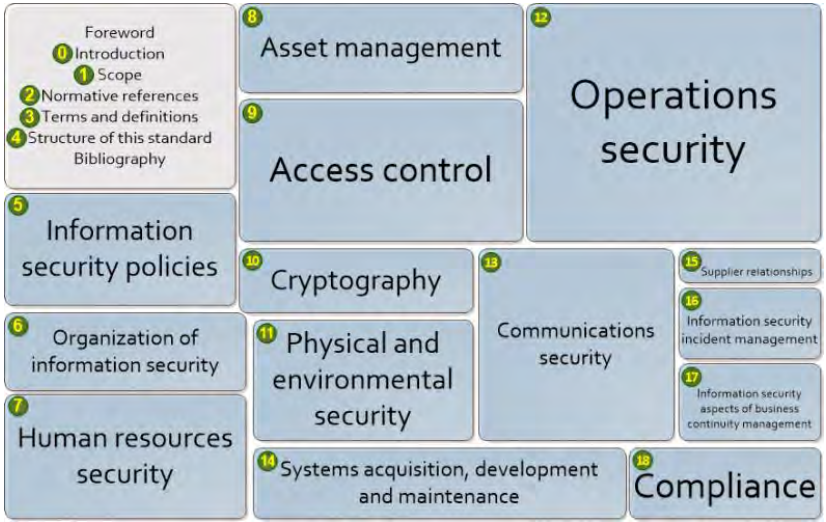
- Scopo del Sistema di Gestione (clausola 4.3)
- Information security policy and objectives (clausole 5.2 e 6.2)
- Metodologia di analisi e gestione dei rischi (clausola 6.1.2)
- Statement of Applicability (clausola 6.1.3 d)
- Piano di trattamento del rischio (clausole 6.1.3 e, 6.2, e 8.3)
- Report di analisi del rischio (clausole 8.2 e 8.3)
- Definizione dei ruoli e delle responsabilità (clausole A.7.1.2 e A.13.2.4)
- Asset inventory (clausola A.8.1.1)
- Uso consentito degli asset (clausola A.8.1.3)
- policy per il controllo degli accessi (clausola A.9.1.1)
- Procedure operative per la gestione dell'IT (clausola A.12.1.1)
- Principi di progettazione di security dei sistemi (clausola A.14.2.5)
- security policy per le forniture (clausola A.15.1.1)
- Procedura per la gestione degli incidenti (clausola A.16.1.5)
- procedure di continuità operativa o Business continuity (clausola A.17.1.2)
- Requisiti legali, regolatori e contrattuali (clausola A.18.1.1)

documentazione facoltativa

- Procedura per il controllo dei documenti (clausola 7.5)
- Controlli per la gestione delle registrazioni (clausola 7.5)
- Procedura per internal audit (clausola 9.2)
- Procedura per le azioni correttive (clausola 10.1)
- Bring your own device (BYOD) policy (clausola A.6.2.1)
- policy per la gestione dei device mobili e per il lavoro a distanza (clausola A.6.2.1)
- policy per la classificazione delle informazioni (clausole A.8.2.1, A.8.2.2 e A.8.2.3)
- Password policy (clausole A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1 e A.9.4.3)
- Disposal and destruction policy (clauses A.8.3.2 and A.11.2.7)
- Procedures for working in secure areas (clause A.11.1.5)
- Clear desk and clear screen policy (clause A.11.2.9)
- Change management policy (clauses A.12.1.2 and A.14.2.4)
- Backup policy (clause A.12.3.1)
- Information transfer policy (clauses A.13.2.1, A.13.2.2, and A.13.2.3)
- Business impact analysis (clause A.17.1.1)
- Exercising and testing plan (clause A.17.1.3)
- Maintenance and review plan (clause A.17.1.3)
- Business continuity strategy (clause A.17.2.1)

I controlli

Un sistema di gestione della sicurezza delle informazioni non è solo un cumulo di carta.
La documentazione deve corrispondere ad un ragionato set di controlli che derivano essenzialmente dalla necessità di proteggere in maniera ragionata, coerente e sostanziale il patrimonio informativo dell'Organizzazione
Di conseguenza l'organizzazione dovrà porre in essere tutte quelle misure idonee a soddisfare i requisiti di security, raggiungere gli obiettivi definiti nella strategia e verificarne l'applicazione



I controlli: Allegato A ISO 27001 e ISO 27002

La definizione di controlli è contenuta nel nomenclatore generale ISO 27000 e sono così definiti:
Controllo: Misura che modifica il rischio
I controlli sono di diversa natura

- riguardati in ordine agli effetti (preventivi, di recupero)
- valutati in ordine alle loro relazioni (alternativi es.: bussole a controllo accessi anziché guardia con registrazione manuale; compensativi: es.: telecamera anziché bussola a controllo individuale quando ne sia impossibile l'installazione; complementari es.: misure che si affiancano tra loro per aumentare il livello di sicurezza atteso; e correlati es.: misure complementari legate da una relazione)

I controlli hanno una unica matrice di origine: la gestione del rischio

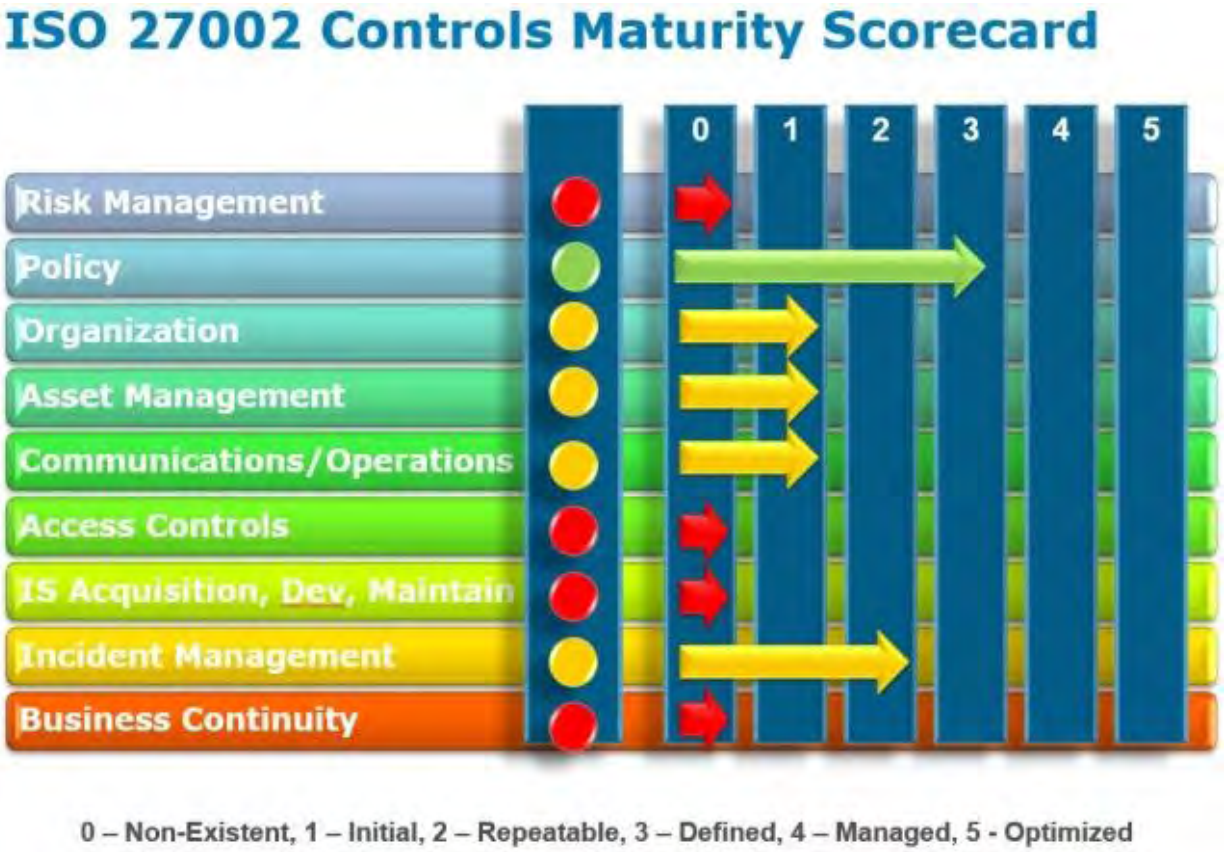
Valutazione delle performances

L'organizzazione è chiamata quindi a valutare l'efficacia ed efficienza del proprio sistema di gestione attraverso un idoneo sistema che ponga alla base una considerazione razionale dell'insieme delle attività poste in essere ed in particolare determinerà:

- chi deve misurare (e chi deve analizzare i risultati)
- cosa bisogna misurare
- come bisogna misurare
- perché bisogna misurare
- quando bisogna misurare

dalla misurazione devono essere quindi tratti degli opportuni indicatori, che rappresentano (in maniera oggettiva e ripetibile) lo "stato di salute" del sistema di gestione, inteso come la sua idoneità a conseguire gli obiettivi e le finalità poste a base delle strategie e della politica

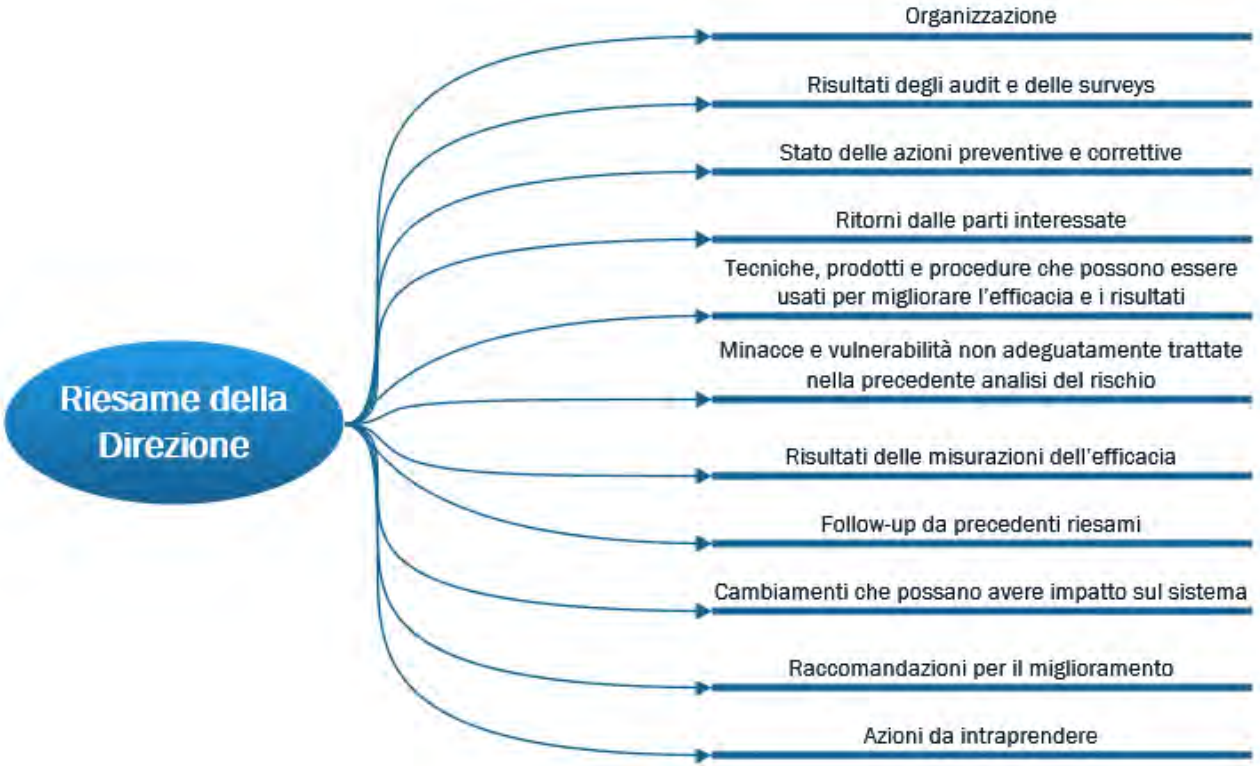
attraverso un processi di continuo miglioramento



i controlli interni

L’applicazione delle regole poste dal sistema di gestione della sicurezza va verificata, con periodicità, rilevando se l’organizzazione vi si adegui,
Sarà quindi necessario pianificare, stabilire, attuare e mantenere un programma di controlli interni, le cui risultanze confluiscano nel processo di riesame della direzione e forniscano ai decisori l’effettiva dimensione dell’attuazione dei principi posti a base del sistema di gestione

il riesame della Direzione



97% - Companies Tested – Breached in Prior 6 mos.

Non è per portare seccia…

Ma un incidente può avvenire

Perché è necessario affrontare il tema

- per garantire il rispetto della *due diligence* e tutelarei diritti di tutti gli “interessati”
- per soddisfare requisiti normativi
- per assicurare una efficace ripresa delle normali operazioni
- per limitare i danni derivanti da un evento interruttivo con carattere impattivo

Ma a che cosa ci riferiamo esattamente?

Le organizzazioni vivono nel mondo reale.

Il mondo reale può presentare eventi, di varia natura, che possono avere un impatto significativo sulla vita operativa delle organizzazioni, determinando interruzioni che possono avere conseguenze anche drammatiche sulle entità, con effetti devastanti sulle persone, e sugli “stakeholders”

la business continuity è dunque una disciplina che studia le modalità con le quali le organizzazioni si predispongono per affrontare eventi avversi, al fine di mitigare i danni, interni ed esterni ed assicurare un ordinato, strutturato ripristino delle capacità operative

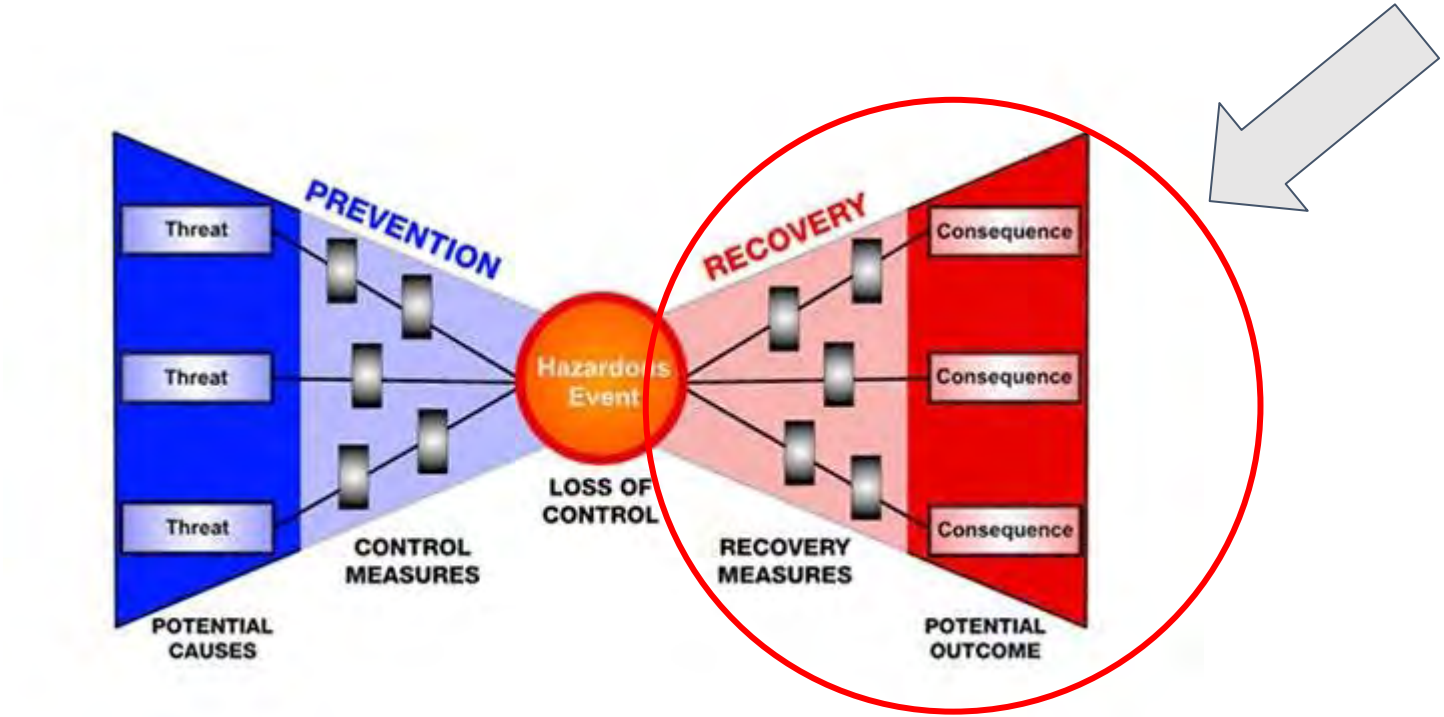
Inquadramento

Abbiamo visto che un sistema di gestione della sicurezza delle informazioni pone l'accento principalmente sul tema della "prevenzione" e della "detection, attraverso il processo di analisi del rischio, la categorizzazione delle minacce, l'individuazione delle vulnerabilità ed una serie di controlli, di tipo tecnologico, organizzativo e di processo, finalizzati alla gestione del rischio.

100% security, tuttavia, è una illusione

Gli eventi avversi, di varia natura, possono avvenire e normalmente avvengono, nonostante l'organizzazione ponga ogni cura per prevenirli, essi si verificano e la cattiva gestione delle emergenze e delle crisi, se non addirittura la mancanza di pianificazione, comporta esiti nefasti

La Business Continuity è un requisito dell'Information Security Management



Definiamo il Business Continuity Management

3.4
business continuity management
holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities

Fonte: Clausola 3.4 dello standard ISO 22301

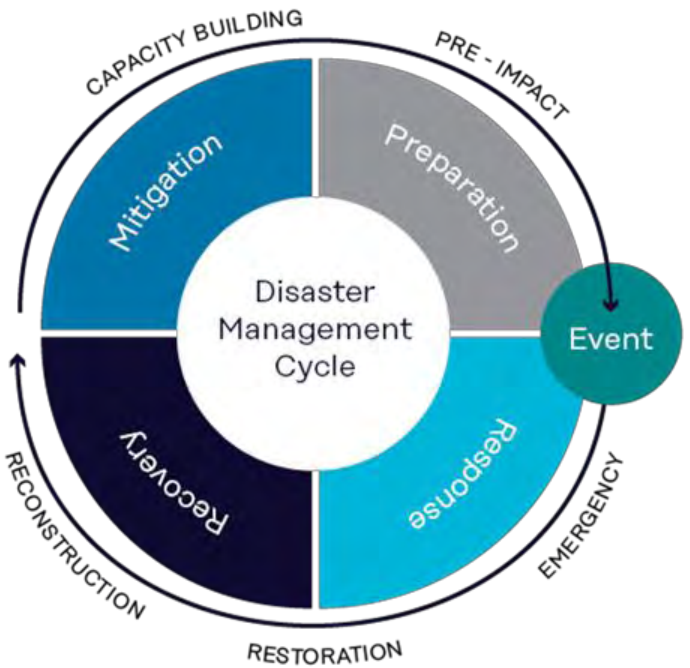
“All Hazard approach”

La disciplina della business continuity si disinteressa dell’aspetto preventivo e guarda soltanto alle conseguenze di un evento potenziale che, se verificato, può determinare l’effetto pregiudizievole.

La disciplina, dunque, è “neutra” rispetto alle cause e non si interessa delle misure atte a prevenire l’evento.

Essa, perciò, si interessa esclusivamente a come gestire un evento pregiudizievole e a come intervenire sulle sue conseguenze e sull’organizzazione.

Il focus, dunque, è sugli **impatti** che un accadimento, naturale o umano; volontario o deliberato, possa provocare.



Incidenti ed effetti negativi

Un’organizzazione può essere esposta ad una molteplicità di minacce e vulnerabilità che possano incidere sulle proprie operazioni.

L’evento pregiudizievole può essere sistematicamente distinto in tre componenti:

- l’incidente in sé
- l’interruzione (disruption)
- l’impatto

Qual è l’aspetto che ha maggiore influenza nella costruzione e gestione di un Business Continuity Management?

L’impatto

Il processo di gestione della continuità non può e non deve traguardare esclusivamente la componente tecnologica.

Gli eventi possono essere molteplici e l’interruzione del servizio può riguardare diverse componenti dell’organizzazione ed in particolare:

- le infrastrutture
- il personale
- la supply chain
- il mondo IT
- gli aspetti finanziari di supporto

In questo senso, il BCM deve essere un approccio olistico e guardare tutti i tipi di impatti che possano pregiudicare la continuità operativa di un’organizzazione

Con riferimento ai principi sul trattamento dei dati personali (Reg. UE 679/2016)

Ricordiamo:

Articolo 5 Principi applicabili al trattamento di dati personali: i dati personali sono … trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Articolo 32 Sicurezza del trattamento - 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, se del caso…
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

BCM e Disaster Recovery come parte integrante del processo di *data protection*

Il processo di continuità aziendale e ripristino di emergenza consente alle organizzazioni di recuperare la capacità operativa a seguito di un evento avverso, riducendone al minimo gli effetti e limitando l'interruzione dell'attività, salvaguardando i dati da possibili distruzioni o perdite, garantendone l'integrità e il ripristino della disponibilità

La continuità aziendale è dunque un processo che implica la necessità di un'azione sistematica, razionale, elaborata e continuativa, sottoposta a verifiche ed analisi e basata su una forte componente di fattore umano e con il coinvolgimento di tutte le persone che fanno parte, ai vari livelli, dell'organizzazione.

nel dettaglio delle definizioni

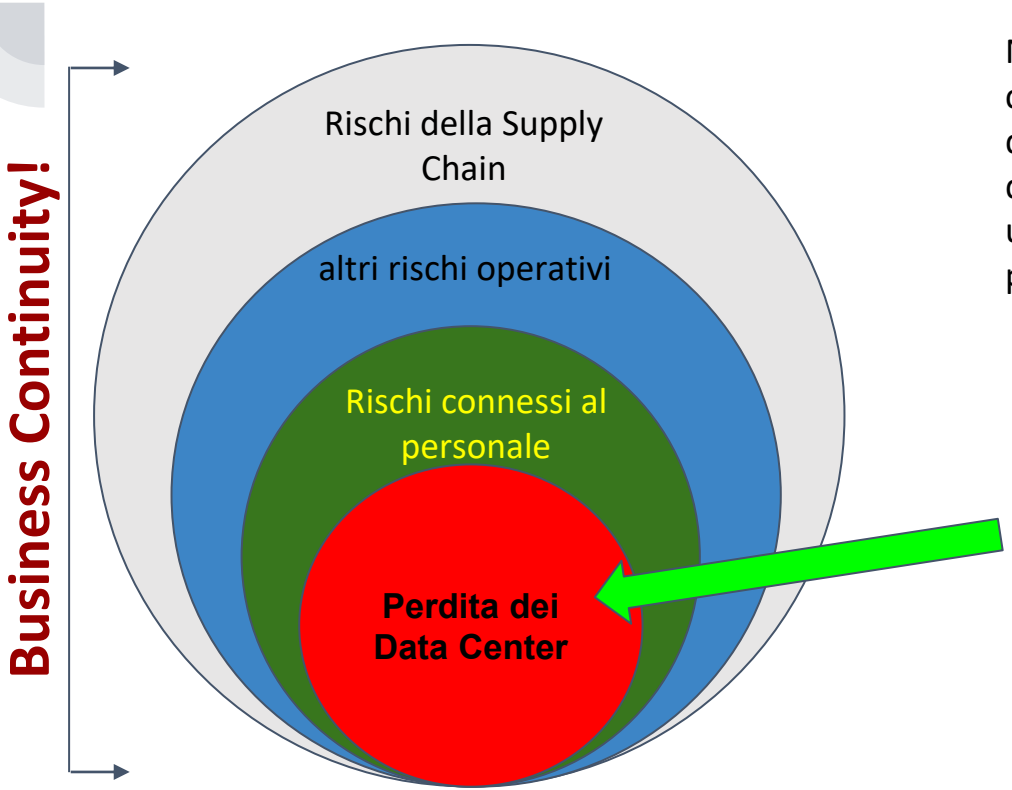
nel linguaggio corrente, Business Continuity e Disaster Recovery sono usati in modo intercambiabile, come se fossero la stessa cosa.

In realtà sono concetti profondamente differenti

Il Business Continuity Management è un processo continuativo che attiene all'identificazione di TUTTE le minacce che possano insorgere sulla continuità delle operazioni e non solo a quelle IT.

Il Disaster Recovery attiene invece alle procedure emergenziali che affliggono l'infrastruttura IT, per ripristinare dati, applicazioni e sistemi informatici necessari per l'operatività del business, a seguito di eventi in grado di interrompere il regolare svolgimento dell'attività (erogazione di beni o servizi) o addirittura minacciare la stessa sopravvivenza aziendale

graficamente parlando...



Nella **Business continuity** l'attenzione si concentra sulla pianificazione di strategie di ripristino che mirano alla continuità delle operazioni nel più ampio senso, in una varietà di scenari di rischio, inclusa la perdita del data center

Il **Disaster Recovery** attiene invece al ripristino tecnologico dei servizi dei data center

… e sulla timeline degli eventi

La continuità è un processo complesso

Gli elementi fondamentali del processo di continuità operativa sono:

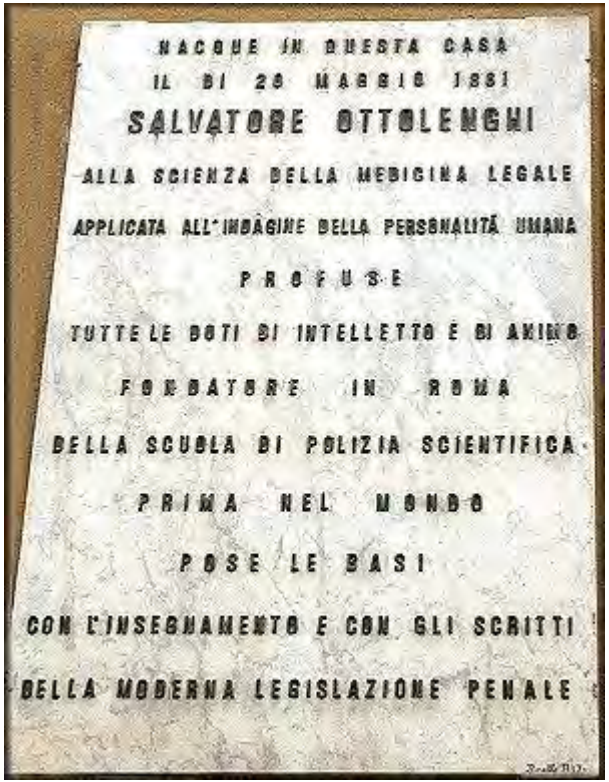
- l’identificazione degli asset e dei processi operativi critici
- l’analisi del rischio
- la Business Impact Analysis
- la determinazione delle “misure chiave” della continuità (RTO, RPO, MBCO)
- la definizione delle strategie di ripristino
- la creazione del piano
- la definizione di ruoli, responsabilità e l’articolazione della gestione dell’emergenza e delle comunicazioni
- la pianificazione delle strategie di Disaster Recovery
- la formazione
- le attività di verifica, di esercitazione e di manutenzione

Miglioramento continuo

Il processo deve essere ciclico e deve saper reagire alle non conformità, eliminando le cause e imparando dalle lezioni, facendo in modo che il sistema risulti adattivo, prevenendone il ripetersi

Criminalistica forense digitale

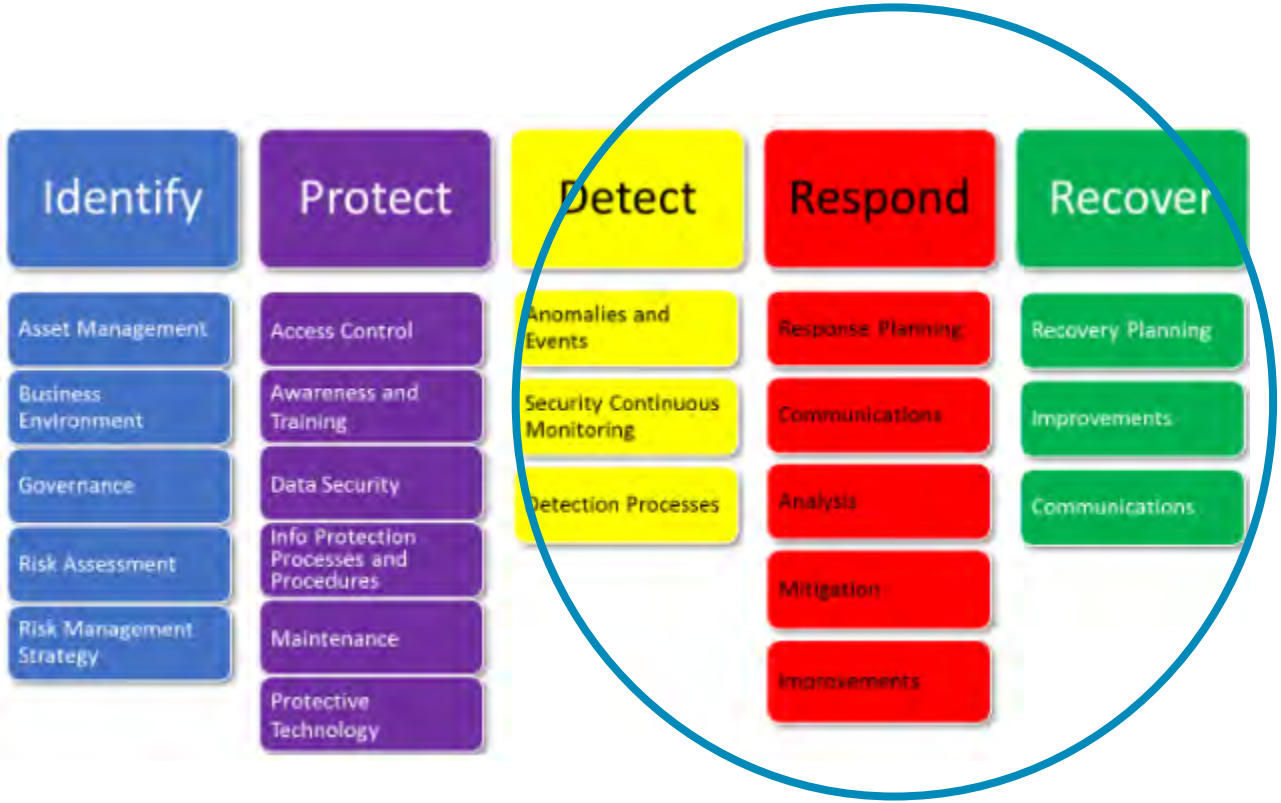
Che cos'è la criminalistica forense digitale?



La scuola criminalistica italiana nell'800 pose per prima le basi di un'attività d'indagine, fondata sul metodo scientifico, per raccogliere le prove, analizzarle e presentarle al giudice, corredate da rigore scientifico e garanzia di non alterazione.
La criminalistica digitale forense è l'evoluzione, nel mondo forense, di quegli stessi principi, attraverso:

- La pratica della raccolta, conservazione e analisi di evidenze per finalità di investigazione, con l'obiettivo della preservazione dell'integrità dei dati;
- La risposta a quesiti pratici, in caso di incidenti, che spieghino cosa sia avvenuto, come, quando, e le eventuali responsabilità individuali

Relazioni tra sicurezza delle informazioni e criminologia forense digitale



Le fasi del processo investigativo forense

Preparazione

Il successo dipende dalla preparazione precedente, e senza una tale preparazione c'è sicuramente il fallimento.

- Confucio

Fissazione della scena dell'incidente

Si tratta di una delle attività più complesse, soprattutto quando vi è la necessità di ripristinare la funzionalità di una infrastruttura critica o di un servizio essenziale.
Soprattutto nelle fasi iniziali di un incidente, diversi fattori possono interferire nella corretta preservazione della scena del crimine, inclusa la condotta non collaborativa della vittima.
Mantenere un PC o un server connesso alla rete ne determina, immancabilmente, una sua modificazione rispetto al momento dell'evento e addirittura potrebbe consentire all'attore malevolo, ancora all'interno dei sistemi, di cancellare tutte le evidenze

Analisi della scena e sua documentazione

In totale analogia con quanto avviene con i crimini ordinari, l'investigazione deve procedere raccogliendo non solo tutti gli elementi tecnici, ma anche quelli che definiscono il contesto interno o esterno, per comprendere già dalle prime fasi se si tratti di un incidente tecnico o di una vera e propria azione criminale.
Il team investigativo sarà, quindi, per sua natura, una combinazione di professionalità

Raccolta delle evidenze

È l'attività tra le più delicate nell'indagine forense, perché può determinare la sorte dell'utilizzabilità delle stesse.
Tenere sempre in evidenza le regole del codice di procedura penale e coordinarsi, all'occorrenza, con la polizia giudiziaria
La raccolta delle evidenze può comportare la rimozione delle apparecchiature dalla loro sede naturale e può anche comportare la necessità di una documentazione (mediante rilievi fotografici ed altri elementi tipici del sopralluogo).

È di imprescindibile importanza la necessità di tenere sempre in evidenza il principio della «catena di custodia»

Preservazione

La catena di custodia è un documento nel quale sono registrate tutte le attività che riguardano un determinato reperto, dalla sua acquisizione sino alla consegna finale.

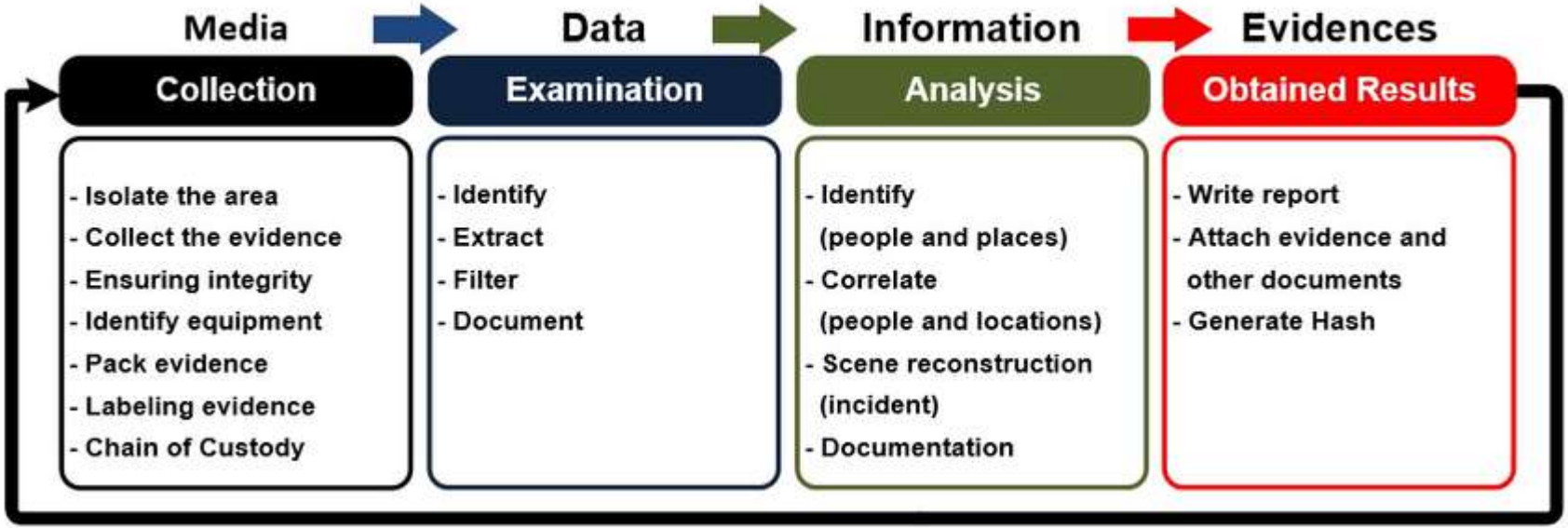
Molto spesso l'attività è svolta dalla polizia giudiziaria, ma potrebbe essere possibile che una determinata situazione d'urgenza, nella quale renda assolutamente necessario procedere al ripristino dei sistemi, p. es. con la sostituzione di un server compromesso, richieda un'attività di conservazione del mezzo di prova.

Conoscere i principi della catena di custodia serve anche nelle attività di difesa, per garantire i diritti dell'interessato e assicurarsi che l'autorità pubblica proceda secondo criteri di legge e di buone pratiche

Esame ed analisi

Lo scopo di questa attività è quello di un accertamento – possibilmente ripetibile – sulle copie forensi dei supporti e dei dati al fine di raccogliere evidenze relative alla causa, alle conseguenze ed alle responsabilità di un incidente di sicurezza.

Da tale analisi possono discendere dati oggettivi e scientificamente sostenibili che possano costituire elementi di giudizio per l'autorità decidente, in risposta alle domande di base dell'investigazione



Presentazione

È la rappresentazione scritta, poi destinata anche alla illustrazione orale dinanzi al giudice, dei risultati delle attività forensi, nelle forme previste dai codici di rito.

L'attività deve illustrare anche i criteri, le tecniche usate, le metodologie applicate e le leggi scientifiche su cui si basano le conclusioni, attraverso un processo logico che permetta la verifica dei razionali e, quando possibile, la riproducibilità scientifica dei fatti dedotti in relazione.

Nella presentazione non vi è spazio per la soggettività delle opinioni, ma solo per fatti, oggettivi, reali, documentati e suscettibili di misura

Grazie