La Comunicazione - Note, Recensioni e Notizie n. 64
Anno 2021

Incidenti di sicurezza delle informazioni – preparazione e risposta efficace

Information security incidents - preparedness and effective response

Fabrizio Cirilli♦

♦ PDCA Srl

Sommario

Con l'incremento del numero di incidenti di sicurezza delle informazioni, e con la loro progressiva crescita di efficienza e aggressività, diventa necessaria una preparazione per una risposta rapida ed efficace, salvaguardando i dati delle organizzazioni e, soprattutto, di quelli personali. In questo articolo vediamo una possibile organizzazione di un modello di risposta partendo dagli standard e dalle best practices mondiali.

Abstract

With the increasing number of information security incidents, and with their progressive growth in efficiency and aggression, preparation for a rapid and effective response becomes necessary, safeguarding the data of organizations and, above all, personal data. In this article we see a possible organization of a response model starting from world standards and best practices.

1 – Introduzione

Spesso si è portati a pensare che gli incidenti "capitino" ad altri e che non ci si debba preparare per questa eventualità. Un po' come per le automobili, facciamo la polizza ma senza convinzione, in modo scaramantico, senza curarci troppo nel dettaglio di cosa sia incluso ed escluso, salvo poi scoprire di essere "non coperti" per quel caso che davamo per "scontato".
In questo articolo proviamo a costruire, con l'aiuto delle norme e standard esistenti, un sistema di risposta efficace in caso di incidenti alla sicurezza delle informazioni e definire quali siano gli elementi principali di cui tener conto.

2 – Una questione di termini

La terminologia utilizzata dagli standard non sempre è allineata al linguaggio comune. Questo è uno dei casi tipici.

Dalla ISO/IEC 27000:2018 [1] traiamo le definizioni di evento di sicurezza delle informazioni:

- information security event, identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that can be security relevant

e di incidente di sicurezza delle informazioni:

- information security incident, single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

Interessante notare che in nessuno dei due casi è dato per scontato che le informazioni siano state compromesse in termini di perdita di riservatezza, integrità e disponibilità.

Eppure, nell'accezione comune, si parla di incidente quando le informazioni sono state compromesse.

Ciò significa che esiste un livello successivo: la violazione. Cioè il momento in cui ciò che aveva una "significativa probabilità" di accadere si è concretizzato, compromettendo la riservatezza, l'integrità e/o la disponibilità delle informazioni.

Se poi la violazione riguarda informazioni (o dati) personali allora siamo di fronte a un *data breach*.

Quindi possiamo avere almeno 4 livelli di situazioni, di gravità crescente:

1. eventi di sicurezza delle informazioni (indicano una possibilità di compromissione)
2. incidenti di sicurezza delle informazioni (indica una significativa probabilità di compromissione)
3. violazioni di sicurezza delle informazioni (indica la certezza della compromissione)
4. data breach (indica la certezza di compromissione di dati personali).

In questo articolo, per comodità di esposizione, ci riferiremo al termine incidente come situazione generica che può includere tutte le situazioni sopra elencate.

3 – Ma è anche una questione di impatti

Ognuna delle 4 situazioni descritte non ci indica però la gravità, la portata delle conseguenze. Anche qui esistono innumerevoli modalità di classificazione. Alcune sono basate sul tipo di conseguenza, ad es. reputazionale, legale, economica, finanziaria ecc. e possono essere espresse in termini qualitativi (Alto, Medio, Basso) oppure quantitativi con scale numeriche da 1 a n oppure in base al valore del danno espresso in valuta locale.

Ma dove possiamo trovare una classificazione consolidata e riconosciuta in qualche modo?

ENISA nel 2016 ha pubblicato un documento dal titolo "Article 19 Incident reporting" [2], che riprende ed espande l'Articolo 19 del Regolamento eIDAS, fornendo un interessante riferimento per la classificazione di un incidente sulla base degli effetti. La scala proposta dal documento è la seguente:

1. No impact
2. Insignificant impact - provider assets were affected but no impact on core services
3. Significant impact - part of the customers/services is affected
4. Severe impact - large part of the customers/services is affected
5. Disastrous - the entire organisation, all services, all certificates are affected

Vero che si riferisce ai servizi eIDAS ma è anche vero che costituisce un'ottima base di partenza riferibile anche alla direttiva NIS [3] e facilmente adattabile a quasi tutte le realtà. Il documento ENISA fornisce anche esempi ed altre informazioni utili (tra l'altro ENISA pubblica un report annuale degli incidenti censiti a livello Europeo [4] utilizzando proprio questa classificazione).

Un altro valido riferimento, anche se forse più articolato, può essere costituito dal documento NIST SP-800-61-r2 [5] che fornisce una scala a 4 valori di impatto "funzionale":

- None - No effect to the organization's ability to provide all services to all users
- Low - Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
- Medium - Organization has lost the ability to provide a critical service to a subset of system users
- High - Organization is no longer able to provide some critical services to any users

Da integrare con gli impatti sulle informazioni:

- None - No information was exfiltrated, changed, deleted, or otherwise compromised
- Privacy Breach - Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated
- Proprietary Breach - Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated
- Integrity Loss - Sensitive or proprietary information was changed or deleted

E con il grado di "effort" necessario per il recupero:

- Regular - Time to recovery is predictable with existing resources
- Supplemented - Time to recovery is predictable with additional resources
- Extended - Time to recovery is unpredictable; additional resources and outside help are needed
- Not Recoverable - Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation

Il risultato finale costituisce, probabilmente, una delle valorizzazioni più complete e articolate basate su standard pubblici. In particolare, l'effort per il ripristino può essere di particolare interesse per tutte quelle organizzazioni sensibili a fenomeni come: l'interruzione di pubblico servizio, il pagamento penali, la violazione di leggi e regolamenti ecc.

Ovviamente nessuno vieta di integrare la classificazione degli impatti di ENISA con gli impatti sulle informazioni e l'effort di ripristino di NIST, generando così una matrice applicabile anche alle casistiche Europee più comuni.

Come ultimo esempio di classificazione vediamo quello proposto dalla ISO/IEC 27035-2, basato su 3 fattori di impatto:

1. importanza del sistema informativo
    - especially important
    - important
    - ordinary
2. perdita del business
    - especially serious
    - serious
    - considerable
    - minor
3. impatto sociale
    - especially important
    - important
    - considerable
    - minor

Sulla base dei 3 fattori di impatto gli incidenti possono essere classificati in una scala di "gravità" del tipo:

- emergency – severe impact
- critical – medium impact
- warning – low impact
- information – no impact

La risultante dei fattori di impatto e della gravità dà luogo alle 4 classi di classificazione degli incidenti:

- Very serious (class IV)
- Serious (class III)
- Less Serious (class II)
- Small (class I)

Da notare come le classificazioni siano su scale con numero di elementi tendenzialmente pari, in modo da disincentivare l'uso di posizioni mediane (il fattore umano è comunque preponderante in questo tipo di analisi).

Anche in questo caso una integrazione con i criteri ENISA e NIST è comunque possibile, sempre in funzione delle necessità dell'organizzazione.

Ciò che salta all'occhio, in tutti questi approcci, è la presenza costante di un "impatto" riferito alle conseguenze di un incidente sull'organizzazione.

4 – L'interazione con i sistemi di business continuity e di disaster recovery

La definizione dell'impatto di un incidente non può (e non deve) essere relegata alla sola funzionalità di un sistema e/o di un servizio, serve anche per capire le conseguenze a livello di organizzazione. Per questo abbiamo bisogno di riferirci ad una Business Impact Analysis (o BIA) [6] [7] che, coinvolgendo il top management, permette di identificare gli scenari di impatto critici per il business e, di conseguenza, i prodotti/servizi, i processi e le attività coinvolte.

Grazie a questa analisi possiamo effettivamente assegnare il corretto impatto ad un incidente della sicurezza delle informazioni. Non necessariamente un disservizio o un incidente della sicurezza delle informazioni è in grado di compromettere la continuità del business (non la continuità operativa!). Forse è anche per questo che un CEO (Chief Executive Officer) ed un CISO (Chief Information Security Officer) parlano lingue diverse. Il primo guarda al business e all'impresa, il secondo alla sicurezza delle informazioni. Ecco perché c'è bisogno di una BIA, per unificare il linguaggio e definire parametri comuni.

Parlare di effort di recupero ha senso solo se il recupero è fondamentale per il business, altrimenti il recupero fine a sé stesso è di poca rilevanza, se non giustificato e argomentato in modo adeguato. Esistono organizzazioni in grado di continuare ad operare senza i sistemi informativi, garantendo la continuità del business a livelli adeguati anche per lunghi periodi, per queste organizzazioni gli aspetti ICT sono meno rilevanti ma non per questo la Business Continuity non è applicabile!

La BIA ed una adeguata valutazione dei rischi possono fornire informazioni indispensabili per la corretta classificazione degli incidenti, secondo gli esempi visti nei paragrafi precedenti.

Da qui dovrebbe essere chiaro che la valutazione dei rischi prescinde dalle minacce e vulnerabilità, così come chiariscono la ISO 22301 [8], la ISO/IEC 27001 [9] e la ISO/IEC 27005 [10].

Questo perché, nel caso della sicurezza delle informazioni, minacce e vulnerabilità sarebbero in gran parte riconducibili solo a situazioni legate all'ICT ma non necessariamente un incidente è legato all'ICT. Si pensi all'interruzione del sistema di prenotazioni per le vaccinazioni, sebbene l'origine possa essere nell'ICT, le conseguenze sono ben lontane da valutazioni tecniche e possono implicare aspetti reputazionali, di immagine, economici, legali ecc. a dispetto di fattori tecnologici.

È quindi di fondamentale importanza predisporre di Business Continuity Plan (BCP) specifici per le varie tipologie e conseguenze di incidenti, e non di documenti tecnici isolati e indipendenti dalle strategie aziendali.

Da chiarire che non sempre un incidente "scala" al punto di dover "invocare" un BCP. In gran parte dei casi gli incidenti vengono gestiti prima di arrivare al punto in cui viene messa in gioco la continuità del business.

Un altro elemento da chiarire è la posizione del Disaster Recovery Plan (o DRP). Spesso sento dire che questo è parte della Business Continuity. Questo non è esattamente vero.

Il Disaster Recovery, almeno a livello normativo, non è parte della Business Continuity (ISO 22301) ma può ovviamente essere associato, laddove possibile e necessario.

Il Disaster Recovery e il DRP si riferiscono ai soli fenomeni ICT; pertanto, ha senso associarli alla Business Continuity se esiste una correlazione tra gli impatti sul business e la necessità di ripristino dei sistemi ICT. Ad esempio, per fornitori di servizi in cloud, internet provider, servizi tecnologici e di assistenza in outsourcing.

Potremmo sintetizzare il concetto in questo modo: laddove finisce la Business Continuity inizia il Disaster Recovey (almeno per l'ICT).

Questa immagine probabilmente riesce a chiarire il concetto appena espresso:

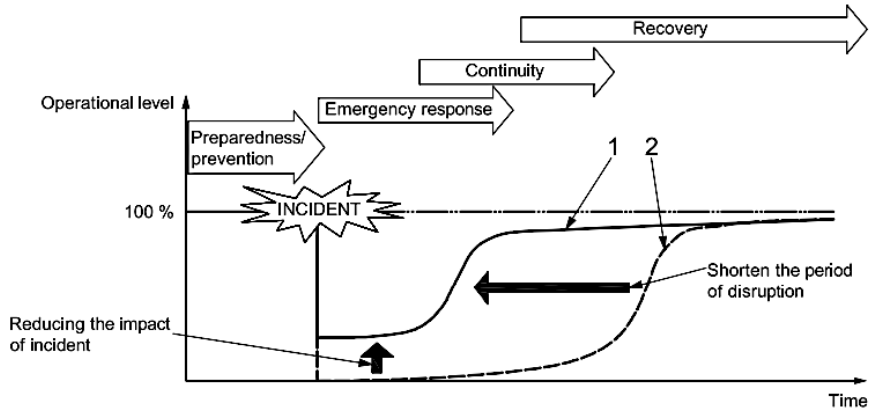

Figura 1 – Preparazione agli incidenti e gestione della business continuity (ISO/PAS 22399:2007)

In questo senso la figura seguente ben rappresenta l'interazione tra Business Continuity e Disaster Recovery, dove quest'ultimo è uno degli elementi dell'organizzazione:

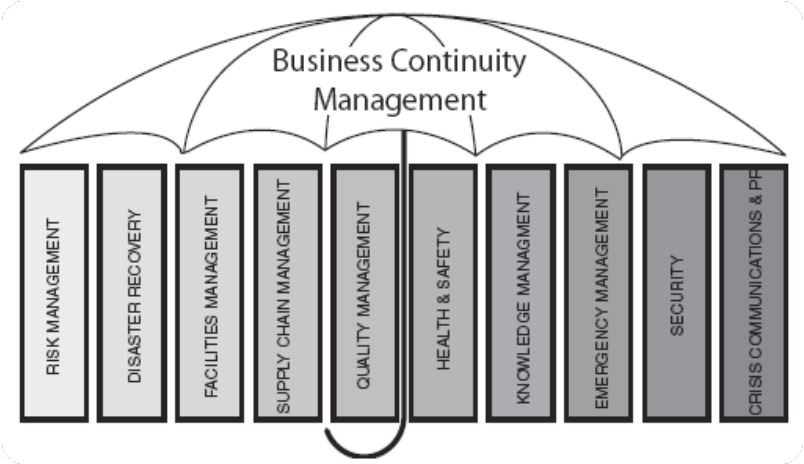

Figura 2 – Integrated Business Continuity Management

5 – La corretta sequenza

Alla luce di quanto fin qui esposto l'approccio sistemico migliore potrebbe essere:

1. Business Impact Analysis - per la corretta individuazione degli scenari di impatto sul business, con particolare attenzione a quelli derivanti da violazioni della sicurezza delle informazioni (perdita di riservatezza, integrità e/o disponibilità).
2. Risk Assessment - per la comprensione degli elementi che possono contribuire alla determinazione di uno scenario, in particolare per calcolo dei rischi derivanti da perdita di riservatezza, integrità e/o disponibilità delle informazioni.
3. Gestione degli incidenti - per la definizione del set di processi necessari a gestire gli incidenti, ivi inclusa l'attivazione delle unità di crisi in funzione della classificazione degli incidenti.
4. Definizione degli eventuali BCP, per assicurare la continuità del business anche nel corso degli incidenti.
5. Definizione degli eventuali DRP, per il recupero delle informazioni nel caso in cui i BCP non riescano a garantire la continuità minima necessaria o nel caso in cui l'incidente ha reso impossibili le attività di Business Continuity.

La sequenza da 3 a 5 è la stessa da applicare per ogni incidente; al termine di ciascun incidente la *post incident review* e le *lessons learned* riattivano l'intero ciclo a partire dal punto 1.

La comprensione della corretta sequenza implica però la conoscenza dei principi di Business Continuity e di alcune misure specifiche, come: RTO, MBCO e MTPD, RPO descritte in sintesi nella tabella seguente:

Tabella 1 - Misure in uso per la Business Continuity (ISO/TS 22317:2015).

Term	Definition
Maximum Acceptable Outage (MAO) or Maximum Tolerable Period of Disruption (MTPD)	Time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable.
Minimum Business Continuity Objective (MBCO)	Minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during a disruption. *Note: This should not be confused with BC objectives in ISO 22301:2012, 6.2 which refer to BC programme objectives*
Recovery Time Objective (RTO)	Target time following an incident for: Product or service delivery resumption, or Activity resumption, or Resources recovery *NOTE For products, services and activities, the recovery time objective must be less than the time it would take for the adverse impacts that would arise as a result of not providing a product/service or performing an activity to become unacceptable.*
Recovery Point Objective (RPO) or Maximum Data Loss (MDL)	Point to which information used by an activity must be restored to enable the activity to operate on resumption.

La figura sottostante rappresenta uno scenario tipico di business continuity (nel caso specifico lo scenario pandemico) e delle misure appena citate:

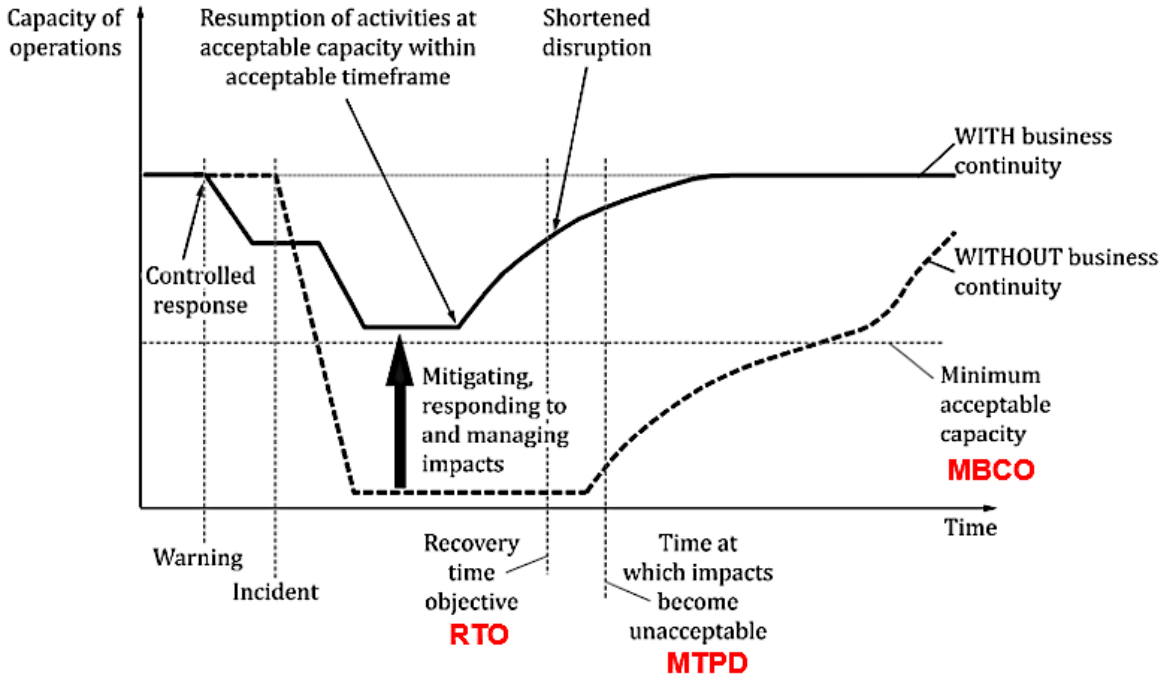

Figura 3 – Business Continuity e misure specifiche (ISO 22313:2020)

Come è possibile notare in questo caso non compare l'RPO che compare, invece, negli scenari tipi legati all'ICT, come vedremo nell'esempio successivo.

Per l'integrazione del processo di gestione degli incidenti della sicurezza delle informazioni, della Business Continuity e del Disaster Recovery può essere utile la ISO/IEC 27031 [11] dalla quale otteniamo questa rappresentazione della sequenza corretta per l'ambito ICT:

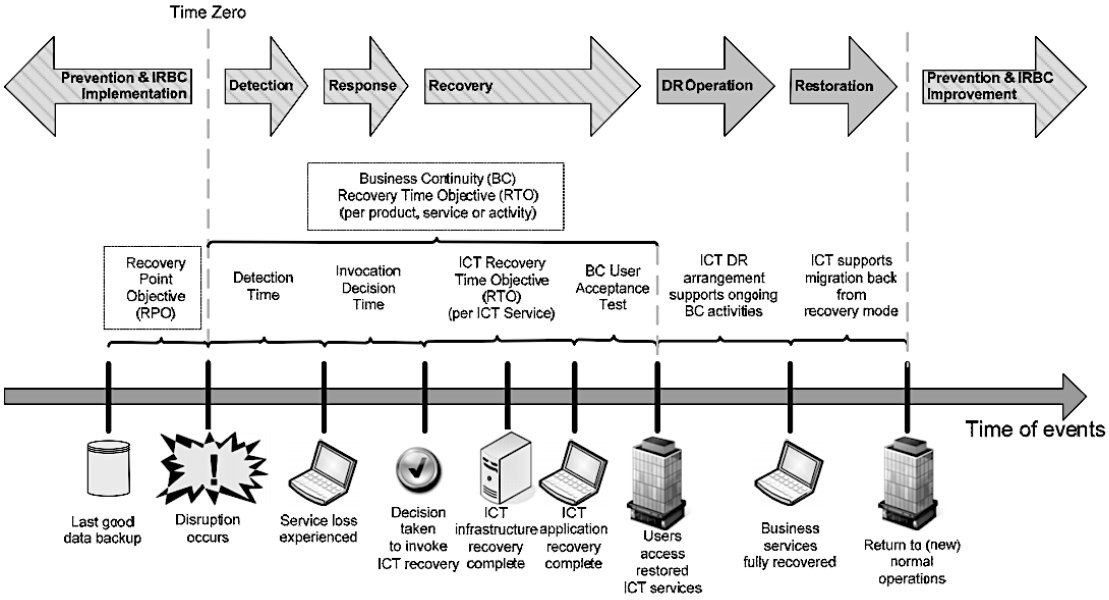

Figura 4 – Integrazione Gestione Incidenti, Business Continuity e Disaster Recovery (ISO/IEC 27031:2011)

Dove la sigla IRBC sta per Incident Response & Business Continuity.

6 – La gestione degli incidenti è un set di processi

Di nuovo dalla ISO/IEC 27000:2018 abbiamo una definizione fondamentale:

- information security incident management, set of processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents

Dunque, siamo di fronte ad un "set" di processi (interagenti) e non di fronte ad attività isolate e indipendenti, come spesso si pensa.

A tal fine la ISO/IEC 27035 [12] fornisce una guida completa per la progettazione, realizzazione, controllo e miglioramento di tale set di processi. La ISO/IEC 27035-3 (che richiama il documento NIST Sp-800-61 r2) definisce un set di processi coordinati e interagenti in grado di

preparare e supportare un'organizzazione nella gestione degli incidenti di sicurezza delle informazioni.

Lo schema proposto dalla ISO/IEC 27035 è il seguente:

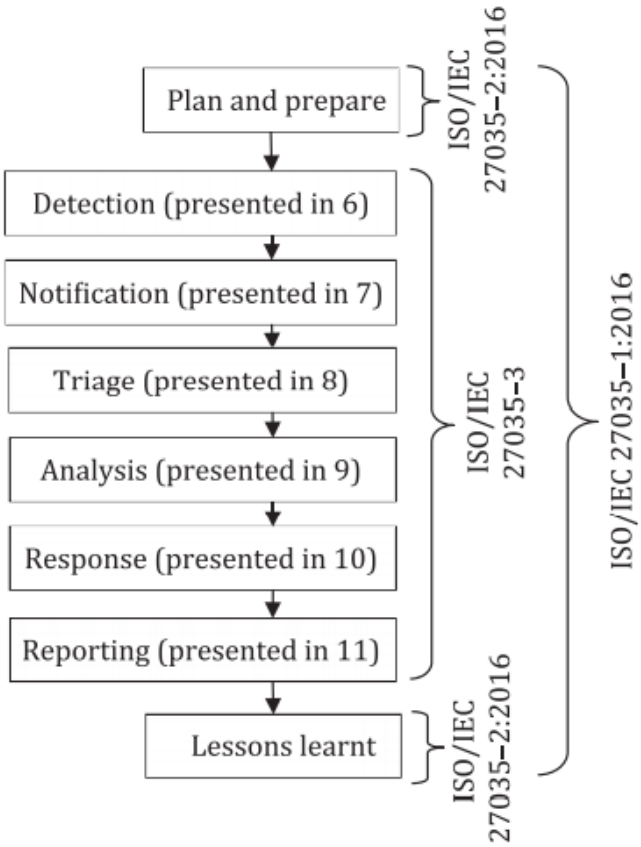

Figura 5 - Ciclo di vita delle operazioni di risposta agli incidenti (ISO/IEC 27035-3:2020)

Da quanto descritto è evidente la necessità di "pianificazione e preparazione", prima di qualsiasi altra attività. La gestione di un incidente non si può improvvisare, deve essere pianificata, testata e aggiornata sulla base delle esperienze (proprie ed altrui). Dalla non efficace applicazione di questo processo, probabilmente, dipendono i tempi indefiniti di risoluzione e ripristino di incidenti cui abbiamo assistito nel 2021 (ad es, attacco alla Regione Lazio e successivo attacco all'Ospedale San Giovanni di Roma).

6.1 – Aspetti caratteristici

Per la creazione di un efficace sistema di gestione degli incidenti abbiamo bisogno di chiarire alcuni aspetti caratteristici degli incidenti di sicurezza delle informazioni.

Prima di tutto le relazioni tra gli elementi tipici:

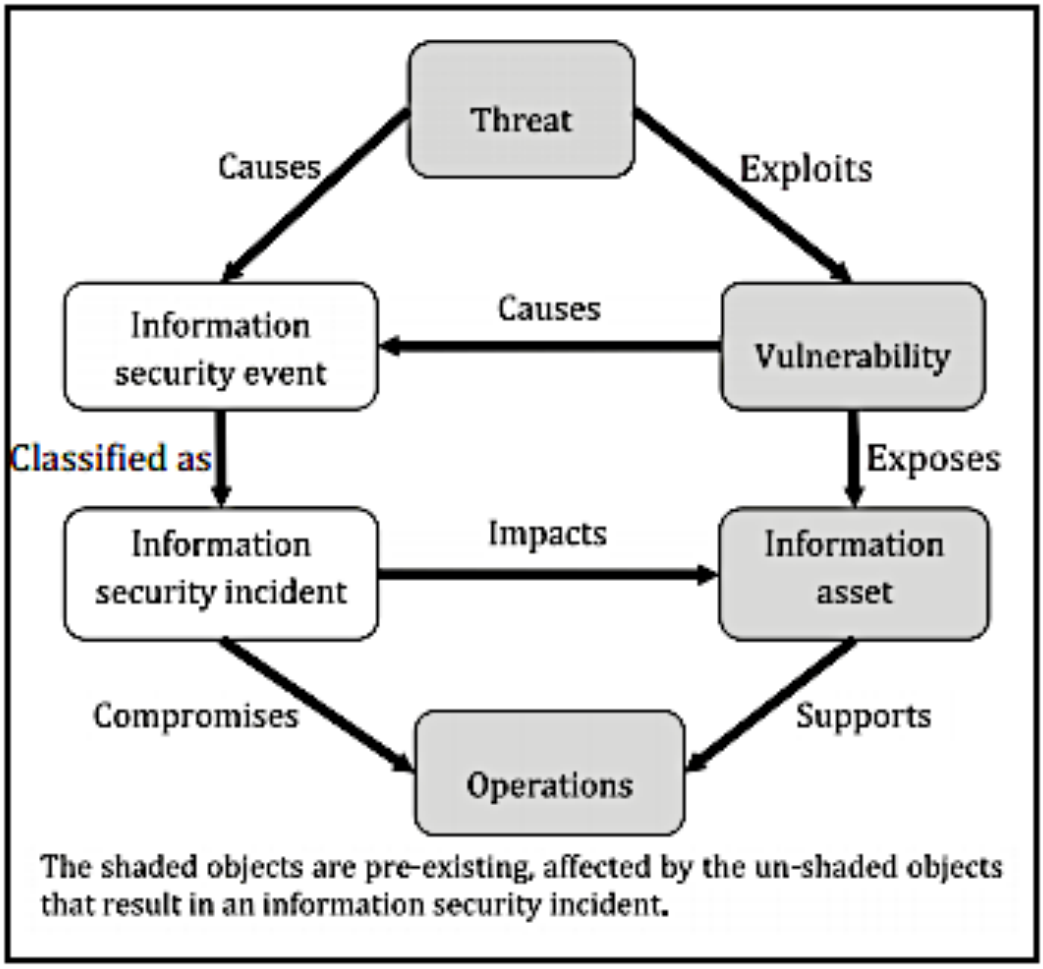

Figura 6 – Relazioni tra gli elementi tipici di un incidente (ISO/IEC 27035-1:2016)

In secondo luogo, dobbiamo chiarire la gestione degli incidenti in relazione ad un Sistema di Gestione per la Sicurezza delle Informazioni (o SGSI):

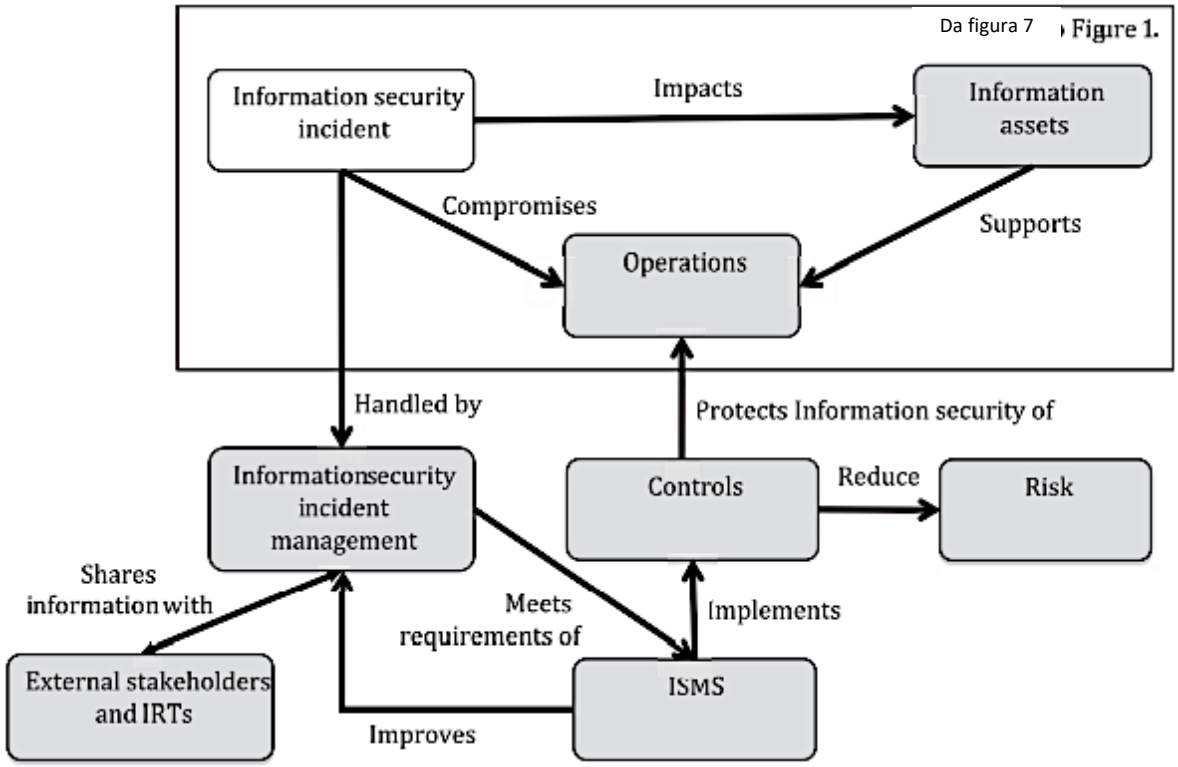

Figura 7 – Gestione degli incidenti e SGSI (ISO/IEC 27035-1:2016)

6.2 – Il collegamento con la ISO/IEC 27001

L'Annex A della ISO/IEC 27001:2013 prevede un controllo specifico (A.16) per la gestione degli incidenti relativi alla sicurezza delle informazioni (ma anche di eventi e debolezze del Sistema), il cui obiettivo è "*Assicurare un approccio coerente ed efficace per la gestione degli incidenti relativi alla sicurezza delle informazioni, incluse le comunicazioni relative agli eventi di sicurezza ed ai punti di debolezza*."

Il controllo propone i seguenti elementi:

- Devono essere stabilite le responsabilità e le procedure di gestione per assicurare una risposta rapida, efficace ed ordinata agli incidenti relativi alla sicurezza delle informazioni.
- Gli eventi relativi alla sicurezza delle informazioni devono essere segnalati il più velocemente possibile attraverso appropriati canali gestionali.
- Deve essere richiesto a tutto il personale ed ai collaboratori che utilizzano i sistemi informativi ed i servizi dell'organizzazione di registrare e segnalare ogni punto di debolezza relativo alla sicurezza delle informazioni che sia stato osservato o sospettato nei sistemi o nei servizi.
- Gli eventi relativi alla sicurezza devono essere valutati e deve essere deciso se classificarli come incidenti relativi alla sicurezza delle informazioni.
- Si deve rispondere agli incidenti relativi alla sicurezza delle informazioni in accordo alle procedure documentate.
- La conoscenza acquisita dall'analisi e dalla soluzione degli incidenti relativi alla sicurezza delle informazioni deve essere utilizzata per ridurre la verosimiglianza o l'impatto degli incidenti futuri.
- L'organizzazione deve definire ed applicare opportune procedure per l'identificazione, la raccolta, l'acquisizione e la conservazione delle informazioni che possono essere impiegate come evidenze.

Come di consueto non tutti gli elementi del controllo sono strettamente applicabili a tutte le organizzazioni anche se sarebbe opportuno farlo.

La soddisfazione di questo controllo può includere quanto descritto dalla ISO/IEC 27035 ottenendo così un set di processi coordinati ed efficaci per il fine specifico di gestire gli incidenti di sicurezza delle informazioni.

6.3 – Il set di processi

La figura che segue evidenzia il set di processi e le fasi per la gestione degli incidenti:

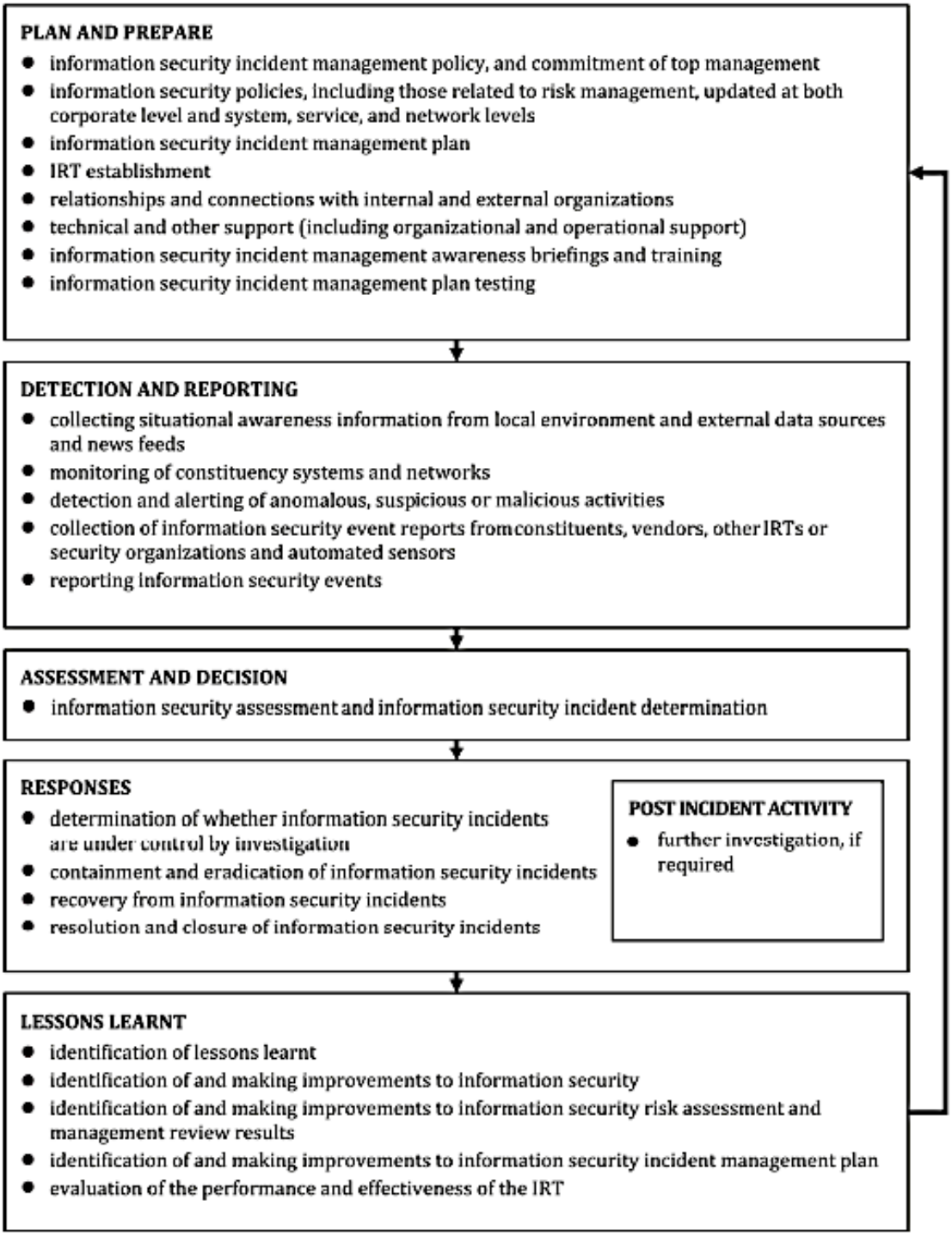

Figura 8 – Processi e fasi della gestione degli incidenti (ISO/IEC 27035-1:2016)

Come appare evidente dallo schema il processo di pianificazione e preparazione risulta essere quello più corposo e propedeutico alla gestione operativa degli incidenti. È altrettanto evidente che le lezioni apprese alimentano la pianificazione e preparazione per assicurarne l'allineamento continuo alle esigenze e alle esperienze effettive dell'organizzazione.
Il seguente schema mostra invece un tipico flusso di gestione di un evento/incidente (secondo i processi e le fasi dello schema precedente):

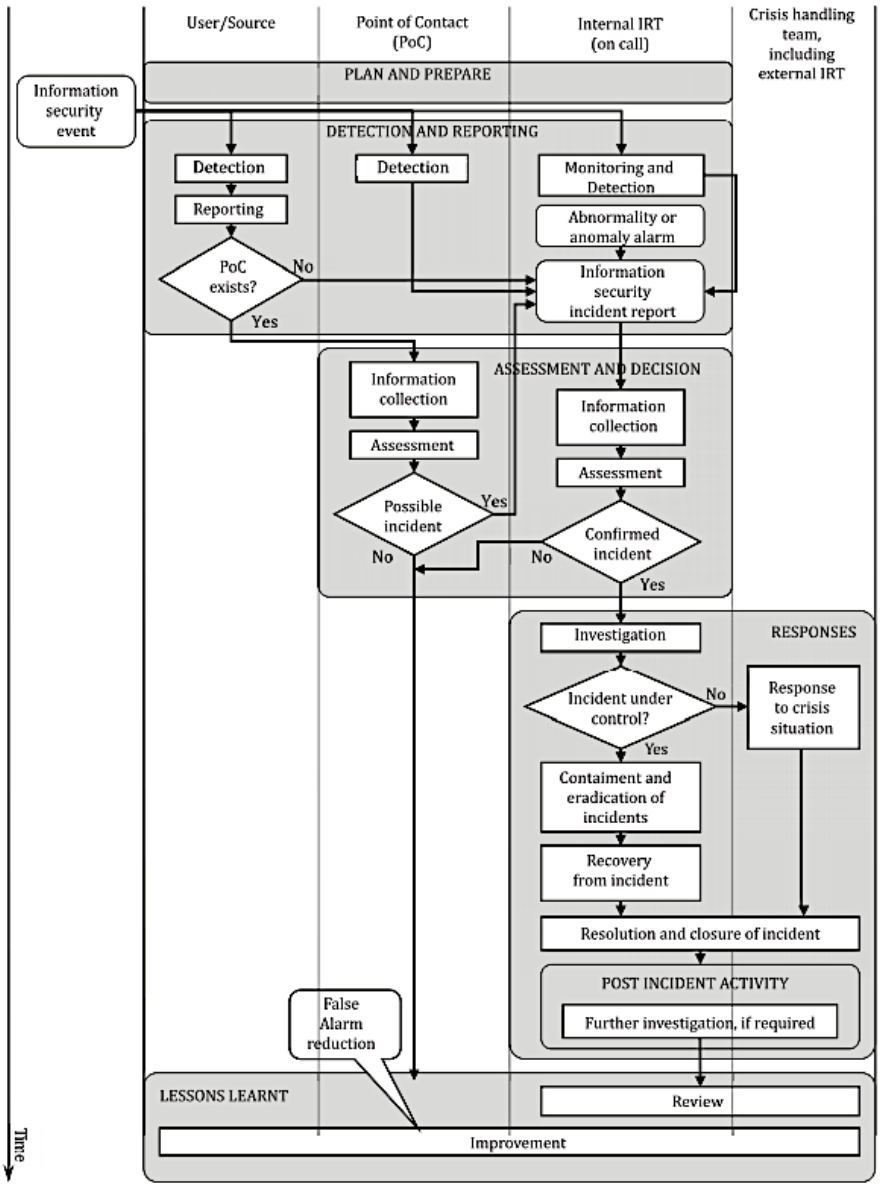

Figura 9 – Flusso di gestione di un evento/incidente (ISO/IEC 27035-1:2016)

7 – La pianificazione e la preparazione

In questo articolo non scenderemo nei dettagli dei processi sottostanti, essendo essi ampiamente documentati e supportati da tool e metodologie disponibili sul mercato.

Lo scopo di questo articolo è dimostrare la necessità di una fase preparatoria e di pianificazione della gestione degli incidenti e non la sola applicazione di regole raccolte da questa o quella fonte.

Il processo di gestione degli incidenti è troppo critico per poterlo lasciare all'inventiva di qualche tecnico o (peggio) di qualche fornitore. È un processo strategico che necessita di una pianificazione e una preparazione tagliate su misura, continuamente aggiornate per mantenere il passo con il mondo circostante e con le esperienze vissute (internamente ed esternamente).

Da quanto illustrato finora una gestione efficace degli incidenti di sicurezza delle informazioni richiede adeguate pianificazione e preparazione. Per mettere in atto un processo di gestione degli incidenti di sicurezza delle informazioni efficace, un'organizzazione dovrebbe completare una serie di attività preparatorie, vale a dire:

1. formulare e produrre una politica di gestione degli incidenti di sicurezza delle informazioni e ottenere il massimo impegno del top management verso tale politica.
2. Aggiornare le politiche di sicurezza delle informazioni, comprese quelle relative alla gestione del rischio e quelle ai vari livelli (strategiche, tattiche e operative).
3. Definire e documentare un piano dettagliato di gestione degli incidenti di sicurezza delle informazioni, inclusi gli argomenti riguardanti le comunicazioni e la divulgazione di informazioni. Il piano può essere costituito da più documenti, template, elementi organizzativi e tool.
4. Istituire l'Incident Response Team (o IRT) identificando:
    a. i ruoli, le responsabilità e l'autorità per la gestione degli incidenti,
    b. le competenze necessarie, tecniche e non (ad es.: soft skill),
    c. eventuali posizioni di staff.

5. Progettare, sviluppare e mantenere aggiornato un adeguato programma di formazione per l'IRT, assicurando che tutto il personale coinvolto raggiunga le competenze necessarie.
6. Instaurare e preservare adeguati rapporti e collegamenti con:
    a. gli enti interni (ad es. altre unità aziendali)
    b. gli enti esterni (ad es. forze dell'ordine e Autorità)
    c. organizzazioni (ad es. clienti e fornitori) che sono direttamente coinvolte in eventi, incidenti e vulnerabilità di sicurezza delle informazioni.
7. Stabilire, attuare e far funzionare meccanismi tecnici, organizzativi e operativi a supporto del piano di gestione degli incidenti e dell'IRT.
8. Sviluppare e distribuire sistemi informativi necessari per supportare l'IRT, compresa una banca dati sulla sicurezza delle informazioni (questi meccanismi e sistemi hanno lo scopo di prevenire il verificarsi di incidenti o ridurre la probabilità che si verifichino incidenti).
9. Progettare e sviluppare un programma di sensibilizzazione e formazione per eventi/incidenti sulla sicurezza delle informazioni e gestione delle vulnerabilità;
10. Testare l'uso del piano di gestione degli incidenti di sicurezza delle informazioni, dei suoi processi e procedure.
11. Misurare la gestione degli incidenti per assicurarne la capacità di risposta.
12. Identificare le lessons learned sulla base degli eventi, incidenti e vulnerabilità gestite.
13. Identificare i miglioramenti da apportare a:
    a. gestione dei rischi
    b. implementazione dei controlli
    c. risultati per il riesame della direzione
    d. piano di gestione degli incidenti.
14. Valutare l'IRT per identificare eventuali aspetti formativi necessari ad ampliarne/completarne le competenze.

Di fatto un vero e proprio Sistema di Gestione con tanto di PDCA a supporto!

Solo dopo aver eseguito e completato con successo ogni fase di questo processo possiamo procedere con la gestione degli incidenti. Farlo prima innescherebbe una sorta di roulette russa.

8 - I benefici di un approccio strutturato

Da quanto esposto possiamo quindi desumere quali siano i benefici di una gestione strutturata e integrata degli incidenti:

- Miglioramento complessivo della sicurezza delle informazioni
- Riduzione degli impatti sul business
- Rafforzamento dell'attenzione alla prevenzione degli incidenti
- Miglioramento della classificazione degli incidenti
- Raccolta delle prove digitali e supporto alle analisi forensi
- Miglior definizione del budget e giustificazione delle risorse
- Miglioramento della gestione del rischio e dei risultati di gestione
- Raccolta di informazioni per i programmi di consapevolizzazione e formazione
- Raccolta di elementi per l'aggiornamento delle politiche e della documentazione.

Sono tutti benefici sicuramente superiori a quelli di un comune Sistema di Gestione o di Sistemi di Gestione indipendenti, più vicini ad una governance, o meglio ad una visione strategica del tema, visto che quest'ultima contempla la lingua del top management e le voci di budget necessarie.

9 – Conclusioni

Sebbene un approccio come quello descritto risulti articolato e basato su conoscenze piuttosto vaste, i benefici che ne derivano giustificano ampiamente gli sforzi necessari alla sua implementazione.

Il risultato finale è qualcosa di più di una mera procedura di gestione degli incidenti. È un processo integrato che fornisce ad una organizzazione una visione strategico-tattica del significato di incidente e dell'importanza di *essere preparati*.

Un processo che integra elementi spesso distanti e in contrapposizione come la Sicurezza delle Informazioni, la Business Continuity e il Disaster Recovery.

Una visione di insieme che permette notevoli economie di scala nella gestione operativa degli incidenti, con processi efficaci e coordinati, basati su criteri solidi e condivisi.

Le basi per un'organizzazione resiliente.

10 – Bibliografia

[1] - ISO,"ISO/IEC 27000:2018 INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — INFORMATION SECURITY MANAGEMENT SYSTEMS — OVERVIEW AND VOCABULARY", *Terms and Definition*

[2] - ENISA, "Article 19 Incident reporting", *Scenarios/examples of security incidents in the context of eIDAS article 19,*

Par. 4.2.1 - pag. 21, Dicembre 2016

[3] - Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[4] - ENISA, "Trust Services Security Incidents 2020 - Annual Report", Luglio 2021

[5] - NIST,"Computer Security Incident Handling Guide",Incident Prioritization, par. 3.2.6 – Pag. 31, Agosto 2012

[6]. -ISO, **“**ISO/TS 22317:2015 SOCIETAL SECURITY — BUSINESS CONTINUITY MANAGEMENT SYSTEMS — GUIDELINES FOR BUSINESS IMPACT ANALYSIS (BIA)”

[7] - BCI,”The BCI Good Practice Guidelines (GPG)”, 2018

[8] - ISO, “ISO 22301:2019 SECURITY AND RESILIENCE — BUSINESS CONTINUITY MANAGEMENT SYSTEMS — REQUIREMENTS”

[9] - ISO, “ISO/IEC 27001:2013 INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — INFORMATION SECURITY MANAGEMENT SYSTEMS — REQUIREMENTS”

[10] - ISO, “ISO/IEC 27005:2018 INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — INFORMATION SECURITY RISK MANAGEMENT”, *Introduction*, pag. VI, Luglio 2018

[11] - ISO, “ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity”

[12] - ISO,

- “ISO/IEC 27035-1:2016 INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — INFORMATION SECURITY INCIDENT MANAGEMENT — PART 1: PRINCIPLES OF INCIDENT MANAGEMENT”
- “ISO/IEC 27035-2:2016 INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — INFORMATION SECURITY INCIDENT MANAGEMENT — PART 2: GUIDELINES TO PLAN AND PREPARE FOR INCIDENT RESPONSE”
- “ISO/IEC 27035-3:2020 INFORMATION TECHNOLOGY — INFORMATION SECURITY INCIDENT MANAGEMENT — PART 3: GUIDELINES FOR ICT INCIDENT RESPONSE OPERATIONS”