aruba.it

Aruba – Soluzioni Cloud

Gestione del rischio per la sicurezza delle informazioni

01.01.2022

SOMMARIO

1 DEFINIZIONI

Nel presente capitolo sono riportate alcune definizioni considerate significative per la rappresentazione del modello di calcolo e gestione del Rischio per la Sicurezza delle Informazioni.

BIA (Business Impact Analysis): Analisi degli impatti economici, normativi e reputazionali per il Business legati alla perdita di Riservatezza, Integrità e Disponibilità delle informazioni relative ad un dato processo/servizio e all'interruzione dello stesso.

Disponibilità: Garantire che i sistemi di informazione e i dati necessari siano disponibili per l'uso quando sono necessari.

Gestione del rischio per la sicurezza delle informazioni: Insieme di attività e processi di business volti ad individuare, misurare, mitigare e monitorare i rischi connessi alla perdita di Riservatezza, Integrità e Disponibilità (RID) dei dati e dei servizi.

Impatto: La conseguenza negativa per l'azienda del realizzarsi di una o più minacce.

Incidente: Un evento connesso alla sicurezza informatica che ha una significativa probabilità di compromettere le operazioni di business e/o minacciare la sicurezza delle informazioni.

Integrità: S'intende la protezione dei dati e delle informazioni dalle modifiche di un contenuto, accidentali oppure effettuate volontariamente.

Minaccia: La potenziale causa (deliberata o accidentale) di un incidente che può danneggiare un sistema o una organizzazione generando degli impatti sulla **R**iservatezza, **I**ntegrità e **D**isponibilità delle informazioni.

Le minacce possono essere:

- Di natura "informatica" - provocano degli impatti negativi sull'azienda mediante:
    - l'uso del sistema informativo o di suoi componenti (es: attacco da parte di hacker);
    - lo svolgimento di attività di gestione del sistema informativo (es: danneggiamenti ad opera di personale interno);
- Di natura "non informatica" - provocano impatti negativi sul sistema informatico dell'azienda attraverso:
    - impatti diretti sull'erogazione dei servizi del sistema informativo (es: disastri naturali, interruzione dei servizi di supporto);
    - effetti sulle modalità di gestione del sistema informativo (es. modalità di implementazione dei processi IT).

Per caratterizzare i rischi associati ad ogni minaccia è necessario conoscere:

- Le vulnerabilità delle componenti del sistema informativo, ovvero laddove le minacce possono concretizzarsi;

- L'esposizione delle componenti alla minaccia, ovvero la facilità con cui la minaccia può concretizzarsi (ad esempio, un server che espone un servizio web ai clienti è maggiormente esposto ad attacchi veicolati da internet);
- Le tipologie di conseguenze, considerato che alcune minacce possono essere a loro volta "vettori" di altre minacce (ad esempio, l'accesso non autorizzato ad un server web può consentire ad un intruso il furto di dati, ma anche la loro cancellazione, alterazione, l'esecuzione di frodi, ecc.).

Possibilità o probabilità di accadimento: Si definisce possibilità di accadimento di una minaccia, la probabilità con cui una minaccia può verificarsi su una o più componenti IT, per causare un impatto negativo per l'azienda, in un determinato periodo di tempo.

Rischio per la sicurezza delle informazioni (nel seguito anche "rischio"): Il prodotto tra la probabilità di verificarsi di una minaccia e l'impatto arrecato all'azienda in relazione agli asset coinvolti nell'analisi. In base al momento di misurazione, il rischio si differenzia in:

- Rischio potenziale o rischio inerente (**rRp**):

  Rappresenta il massimo rischio cui è soggetto un determinato asset in termini di possibilità di realizzazione di una minaccia che possa arrecare un impatto a fronte della perdita di Riservatezza, Integrità o Disponibilità delle informazioni. Concorrono nella determinazione del rischio inerente tutte le componenti che afferiscono al servizio in analisi: processi, applicazioni, dati, infrastrutture e, non ultimi, i fattori umani.

  È sostanzialmente rappresentato da un valore, differentemente calcolato secondo le metodologie applicate, dato dalla sommatoria di tutte le possibili minacce a cui è sottoposto un asset, considerate le rispettive probabilità di accadimento e i relativi impatti.

  In altre parole è il rischio a cui può essere esposto un asset considerata semplicemente la sua natura e le minacce ad esso correlate. A titolo esemplificativo, si consideri il caso di un computer esposto su rete pubblica senza alcuna misura di protezione.

- Rischio residuo o finale (**rRf**):

  Rappresenta il rischio riscontrabile su un servizio in seguito all'applicazione di contromisure atte a determinare una riduzione del rischio inerente.

- Rischio Finale Accettabile (**rRfa**):

  Rappresenta la soglia massima di rischio accettabile dall'Organizzazione.

Tutti i valori di rischio sopra esposti sono da considerarsi dinamici, perché variano nel tempo, in quanto sono influenzati ad esempio dai seguenti elementi:

- Evoluzione delle minacce;
- Modifica dei livelli di servizio richiesti;
- Variazione delle disposizioni di legge o regolamenti di riferimento;

- Modifiche organizzative che possono impattare sulle debolezze o sulla probabilità di realizzarsi delle minacce, o modificare gli impatti conseguenti;
- Rafforzamento o indebolimento delle contromisure di sicurezza.

Rischi Elementari: S'intendono i rischi informatici per la sicurezza delle informazioni associati a ciascun asset ed a ciascuno scenario di rischio.

Riservatezza o confidenzialità: S'intende la protezione di dati e informazioni al fine di mitigare i rischi connessi all'accesso o all'uso non autorizzato delle informazioni.

RPO (Recovery Point Objective): Perdita dati accettabile, è il periodo massimo di tempo che intercorre tra l'ultimo salvataggio dei dati di un processo e il verificarsi dell'evento che causa l'arresto del processo.

RTO (Recovery Time Objective): Periodo di tempo dopo un incidente all'interno del quale:

- Il Prodotto o il Servizio devono essere ripresi, o
- L'attività deve essere ripresa, o
- Le risorse devono essere recuperate.

Scenario di Rischio: Unione di due o più minacce che permette la classificazione delle stesse.

Vulnerabilità: Debolezza intrinseca di un processo, di un servizio, di un asset, che, qualora sfruttata da una o più minacce, consente la violazione degli obiettivi di Sicurezza delle Informazioni (Riservatezza, Integrità e Disponibilità). Esempi possono essere:

- Reti non segregate;
- Uso di protocolli privi di protezione crittografica;
- Sistemi operativi non regolarmente aggiornati;
- Basi dati con dati "sensitive" non criptate;
- Definizioni di virus non aggiornate;
- Accessi fisici non presidiati;
- Mancanza di sistemi antincendio automatici;
- Insufficienza dei sistemi di energia suppletiva;
- ecc.

2 I PRINCIPALI STANDARD DI RIFERIMENTO

I principali standard adottati per garantire l'aderenza delle attività erogate alle best practices internazionali in ambito security sono quelli descritti nei paragrafi seguenti.

2.1 ISO/IEC 27001 Standard

La norma ISO/IEC 27001 costituisce, quale standard internazionale di sicurezza, un vero modello di riferimento per la valutazione del livello di sicurezza delle informazioni in grado di analizzare sia le componenti tecnologiche che quelle organizzative che contribuiscono a definire un Sistema di Gestione della Sicurezza delle Informazioni (SGSI).
Lo standard definisce i requisiti di un SGSI ed aiuta a identificare, a gestire e a minimizzare la varietà di minacce alle quali le informazioni sono regolarmente soggette. Tale standard stabilisce inoltre i controlli di sicurezza da adottare per proteggere le informazioni rendendo sicure le parti interessate, inclusi i clienti dell'organizzazione.

2.2 ISO/IEC 27002 Standard

Lo standard ISO/IEC 27002 definisce le linee guida e i principi generali volti all'implementazione di un adeguato Sistema di Gestione della Sicurezza delle Informazioni all'interno di un'organizzazione.
In particolare la norma ISO/IEC 27002 costituisce, quale standard internazionale di sicurezza, un vero modello di riferimento per la valutazione degli aspetti organizzativi, procedurali, tecnologici e normativi della sicurezza di un sistema informativo condotta con lo scopo di:

- Effettuare un esame critico dei servizi e delle funzionalità di cui il sistema in esame già dispone o dovrà disporre;
- Evidenziare le vulnerabilità del sistema;
- Indicare le azioni opportune per raggiungere il livello di sicurezza definito negli obiettivi.

Si sottolinea che l'ISO/IEC 27002 identifica i controlli di sicurezza che un'organizzazione dovrebbe considerare, ma non sostituisce l'attività di Analisi dei Rischi propriamente detta.

2.3 ISO/IEC 27005 Standard

La ISO/IEC 27005 descrive il processo di gestione del rischio in materia di sicurezza delle informazioni e le azioni associate, supportando i principi generali contenuti nella ISO/IEC 27001.
La norma - in linea con la ISO 31000 - ha lo scopo di aiutare le imprese a gestire il rischio relativo alla sicurezza delle informazioni in maniera simile al modo in cui gestiscono altre tipologie di rischio.
In Figura 1 è rappresentato lo schema proposto dalla ISO/IEC 27005 del processo di gestione del rischio a cui si ispira il modello adottato e sviluppato dal Gruppo Aruba.

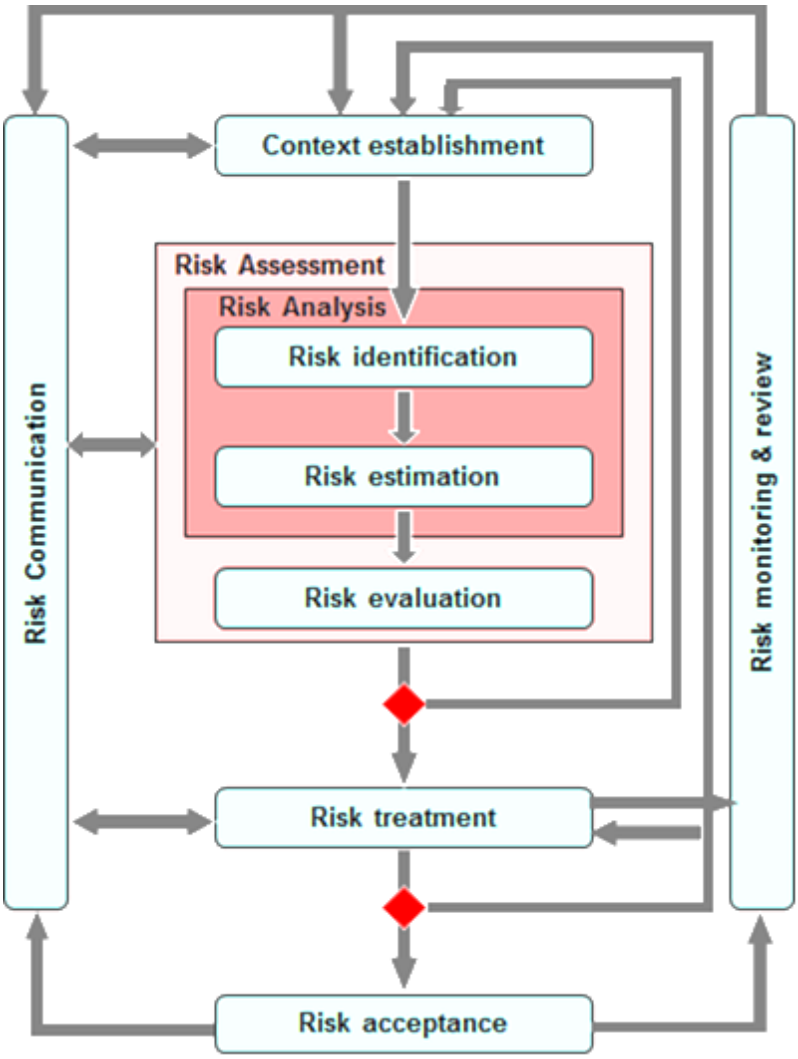

Figura 1 – ISO/IEC 27005: Processo di gestione del rischio

3 METODOLOGIA DI GESTIONE DEI RISCHI PER LA SICUREZZA DELLE INFORMAZIONI

Per il Gruppo Aruba S.p.A. l'informazione rappresenta un patrimonio la cui attenta gestione è strategica per la tutela e lo sviluppo del business aziendale.

In tale contesto, può essere definito rischio informatico ogni evento incerto che possa compromettere una o più delle seguenti tre principali proprietà del patrimonio informativo aziendale:

- **R**iservatezza (i dati sono accessibili a persone non autorizzate);
- **I**ntegrità (i dati possono subire modifiche non autorizzate e risultare alterati);
- **D**isponibilità (il sistema informatico non è utilizzabile);

secondo livelli di gravità strettamente dipendenti dalla tipologia delle informazioni impattate.

La valutazione del rischio è effettuata tenendo conto dei possibili impatti di tipo:

- Economico;
- Normativo;
- Reputazionale.

La gestione dei rischi relativi alla sicurezza delle informazioni è un processo che consente di valutare le interrelazioni tra gli asset, le minacce e le vulnerabilità riguardanti una certa organizzazione. Questo processo analitico ha l'obiettivo di identificare i rischi associati alle vulnerabilità e alle minacce riscontrate sugli asset e fornire le basi per definire un programma di sicurezza efficiente.

Le categorie di rischio prese in considerazione devono essere in linea con tipologie applicabili al contesto. I rischi presi in considerazione pertanto possono essere sia derivanti da minacce interne che esterne o ambientali, sia da atti deliberati che da gestioni organizzative inadeguate o negligenze dei singoli.

Il valore del rischio è inteso come funzione del valore degli asset in ambito, del valore delle minacce e delle vulnerabilità.

I risultati dell'analisi dei rischi sono documentati e includono:

- Una chiara identificazione dei rischi fondamentali;
- Una valutazione dei potenziali impatti che ognuno dei rischi individuati potrebbe avere sul business;
- Un piano di azioni raccomandate per ridurre i rischi e ricondurli ad un livello accettabile.

Il Gruppo Aruba stabilisce un modello di analisi di tipo qualitativo, perché in grado di fornire nel breve periodo un elevato grado di consapevolezza sui maggiori rischi ICT impattanti l'ambiente tecnologico di riferimento.

La metodologia adottata è:

- Utilizzata dal Gruppo al fine di stimare il valore delle informazioni nei processi di competenza ed il livello di rischio cui sono sottoposte, per permettere l'individuazione delle adeguate misure di protezione;
- Applicabile anche nel caso di sviluppo di nuove soluzioni infrastrutturali o applicative che hanno impatto sulla sicurezza dei dati gestiti. In tal caso la metodologia permette di valutare la criticità dei dati e le minacce cui sono sottoposti, consentendo alle funzioni responsabili dell'analisi dei rischi, nei processi di sviluppo e acquisizione dei sistemi informatici, di implementare le idonee misure di protezione per ridurre al minimo le vulnerabilità.

La valutazione dei rischi e l'analisi delle correlazioni fra asset, minacce e contromisure è effettuata con il supporto di un tool sviluppato internamente, alimentato con le informazioni raccolte nel corso di specifici incontri con le diverse figure coinvolte nei processi oggetto di analisi.
La metodologia utilizzata consente di realizzare un modello aziendale dove sono descritti tutti gli elementi base necessari alle successive analisi, le loro caratteristiche, la loro struttura gerarchica e le relative connessioni.

4 IL PROCESSO DI GESTIONE DEI RISCHI

Di seguito si descrivono le principali fasi del modello di analisi per la gestione dei rischi relativi alla sicurezza delle informazioni adottato ed applicato dal Gruppo Aruba S.p.A.

4.1 FASE 1 – Context Establishment

La definizione del contesto di analisi, prevede la modellizzazione della realtà aziendale e l'individuazione dei principali servizi di business, processi, macro processi e asset coinvolti.

Per l'identificazione delle risorse, così come suggerito dallo standard ISO/IEC 27005 «Information technology – Security techniques – Information security risk management», sono state considerate due distinte tipologie:

- **Risorse primarie** – informazioni, processi, macro processi e servizi di business;
- **Risorse secondarie o asset** – hardware, software, personnel, network, location ed organization.

4.1.1 Individuazione dei servizi, dei processi e dei macro processi

Per l'individuazione dei servizi e dei processi dell'Organizzazione sono presi come riferimenti iniziali gli assetti organizzativi pubblicati e resi disponibili mediante lo strumento di comunicazione aziendale interno.
Successivamente i singoli processi, che concorrono all'erogazione dei servizi, sono raggruppati in macro-processi specifici per il contesto analizzato.

4.1.2 Identificazione degli asset

Al fine di garantire un'accurata individuazione dei propri asset, si procede per step successivi:

1. **Individuazione delle categorie** di asset informativi (es. hardware, software, location, etc.), secondo la classificazione definita all'interno dello standard ISO/IEC 27005;
2. **Ponderazione delle categorie** di asset informativi in funzione della strategia di sicurezza aziendale e dei requisiti di business, legali e contrattuali;
3. **Individuazione delle dipendenze** fra le categorie di asset così censite.

4.1.3 Legame parentale macro processi – asset

Identificati gli asset, sono state definite le dipendenze tra gli stessi e i macro processi.

Tali dipendenze permettono di associare ad ogni categoria di asset i valori di impatto RID (determinati mediante le interviste di BIA), consentendo di calcolare i rischi informatici elementari associati ad ogni asset.

4.2 FASE 2 – Risk Analysis

4.2.1 Valutazione degli impatti

La valutazione degli impatti (Business Impact Analysis) è effettuata, come da metodologia adottata oltre che dai principali standard internazionali (ISO 27005, ISO 22301), dai referenti di Business.
Mediante uno strumento sviluppato internamente per la raccolta delle informazioni, i Responsabili delle diverse funzioni aziendali valutano, in fase di intervista di BIA, la perdita di Riservatezza, di Integrità e di Disponibilità delle informazioni gestite all'interno della propria area di competenza in termini di impatto economico, normativo e reputazionale, secondo scale di valutazione ben definite.

I singoli processi, come specificato in FASE 1, sono poi raggruppati in macro processi specifici per il contesto analizzato. Gli impatti associati a tali macro processi sono calcolati come il *"worst case"* dei singoli impatti dei processi che li compongono.

4.2.2 Individuazione e valorizzazione degli asset

L'individuazione degli asset è la base di partenza senza cui non è possibile poter procedere ad una corretta ed efficace gestione della sicurezza aziendale. L'inventario è infatti il punto di partenza per la classificazione degli asset aziendali e per l'analisi del livello di rischio cui essi sono sottoposti.

Obiettivo di questa fase operativa è quello di garantire l'elaborazione, o la formalizzazione in virtù di metodologie già in essere, dell'inventario degli asset informativi, ritenuti dall'azienda "mission critical" al fine di raggiungere i propri obiettivi di business, di rispettare i propri obblighi contrattuali e, infine, di rispettare le norme e la legislazione cui le proprie attività sono sottoposte.
Il valore centrale di un asset è rappresentato solitamente dalle informazioni (o dati) che il sistema tratta, lasciando il compito agli altri asset di elaborarli o proteggerli.

In tale logica, il valore è assegnato, in fase di intervista di BIA, per ogni asset e per ognuna delle dimensioni RID (riservatezza, integrità e disponibilità) di sicurezza applicabili al contesto.

Sfruttando le informazioni raccolte durante le interviste di BIA, è quindi possibile associare a ciascun asset, gli impatti derivanti i macro processi cui sono impiegati.

4.2.3 Analisi delle minacce e valutazione delle probabilità di accadimento

La metodologia utilizzata nel processo di gestione dei rischi per la sicurezza delle informazioni definisce un passaggio puntuale per la determinazione delle minacce che interessano gli asset in perimetro. Le minacce rappresentano tutti quegli elementi o eventi che possono arrecare un danno ad un asset.
Obiettivo di questa attività è l'individuazione delle minacce e delle vulnerabilità che insistono sugli asset individuati e recepiti all'interno del processo di analisi e gestione del rischio e la valutazione delle probabilità di accadimento delle stesse.
A garanzia dell'esaustività dell'elenco di minacce, è presa come riferimento la lista di minacce dello standard ISO/IEC 27005, a cui si aggiungono le considerazioni prodotte e pubblicate da ENISA a valle dei suoi studi in materia.
Le singole minacce, sono successivamente raggruppate in scenari di rischio realistici per il contesto analizzato.

4.2.4 Analisi delle contromisure

Obiettivo di questa attività è l'individuazione delle contromisure ritenute necessarie per coprire gli scenari di rischio sugli asset individuate nello step precedente.
A garanzia dell'esaustività dell'elenco, il Gruppo Aruba S.p.A. adotta una lista di contromisure basata sulle best practices dello standard ISO/IEC 27001 Annex A. Le valutazioni, a seconda della tipologia di servizio analizzato, possono essere arricchite per specifiche tematiche dall'analisi di ulteriori controlli suggeriti da fonti autorevoli, quali ENISA, AgID, NIST, etc.
Definito l'elenco dei controlli di sicurezza, gli stessi sono stati mappati rispetto agli scenari di rischio, su cui possono agire in termini di riduzione della probabilità di accadimento delle minacce che li compongono o dell'impatto.
Le contromisure sono state suddivise in:

- **Reattive** (r), atte a ridurre l'impatto;
- **Preventive** (p), atte a ridurre la probabilità di accadimento.

4.3 FASE 3 – Risk Evaluation

4.3.1 Metodologia e modello del rischio

Il valore del rischio è inteso come funzione $R = f(A, M, V)$, con A il valore degli asset in ambito, M il valore delle minacce e V le vulnerabilità.
Attraverso la FASE 2, del processo di gestione dei rischi per la sicurezza delle informazioni, è stato possibile definire il modello di rischio (*Threat Modeling*). Quest'ultimo rappresenta un processo con cui identificare potenziali minacce e

vulnerabilità, valutare quanto sono probabili nel caso specifico, metterle in una scala di priorità, e ridurre il rischio che si avverino implementando delle idonee contromisure.

Definito il contesto di base, il processo di *Threat Modeling* consiste nel:

- Fare una lista delle possibilità di attacco/vulnerabilità che contempla i modi in cui è possibile compromettere la Riservatezza, l'Integrità e la Disponibilità dei dati;
- Valutare quelli che sono gli attacchi/vulnerabilità più probabili, scartare quelli improbabili o comunque quasi impossibili da rimediare, e su tutti gli altri applicare dei controlli, ovvero delle contromisure che possono essere tecniche o procedurali.

4.3.2 Requisiti di sicurezza applicabili e livello di conformità

A valle dell'identificazione dei requisiti di sicurezza ritenuti applicabili nell'ambito dell'analisi (vd. par. "Analisi delle contromisure"), è svolta una valutazione del livello di copertura dei requisiti relativi ai 14 ambiti identificati nello standard ISO/IEC 27001 Annex A.

Il grado di compliance di ogni contromisura è espressa secondo una scala di valori ben definita che va da 0, in caso di contromisura inesistente, a 4 per una contromisura completamente implementata.

Per l'analisi del livello di conformità dei controlli richiesti dall'Annex A dello Standard ISO/IEC 27001, si utilizzano le informazioni e le evidenze raccolte mediante specifiche attività di assessment condotte internamente.

4.3.3 Calcolo dei rischi elementari inerenti e residui

Durante questa fase è calcolato il valore dei rischi di sicurezza elementari RID inerenti e residui (AS-IS, Pianificati e TO-BE) associati al servizio in analisi.
Il calcolo dei rischi elementari inerenti per ciascun asset e per ciascuno scenario, associato secondo le logiche descritte in precedenza, si effettua considerando la probabilità di accadimento dei singoli scenari di rischio ed il potenziale impatto che gli stessi potrebbero comportare.
Una volta determinati i rischi inerenti, per ottenere i rischi residui (AS-IS, Pianificato e TO-BE), si prendono in considerazione i valori associati, in fase di audit interno, alle contromisure di sicurezza necessarie per contrastare gli scenari di rischio individuati, sia in termini di riduzione della probabilità di accadimento delle minacce che li compongono sia in termini di riduzione dell'impatto.

4.4 FASE 4 – Risk Treatment

4.4.1 Analisi del rischio accettato

Uno dei concetti che è fondamentale affrontare per il risk management è il rischio accettato. Con questo termine si indicano in modo generico quei rischi che per qualche motivo non è conveniente o possibile trattare e che semplicemente vengono accettati.

Obiettivo di questa attività è pertanto la definizione di un criterio in base al quale le coppie minaccia-asset che implicano un rischio di bassa entità possano semplicemente essere accettate. Al di là dei singoli casi dunque, si definisce una soglia al di sotto della quale un certo rischio viene considerato semplicemente un costo e non viene dunque trattato.

4.4.2 Risultato dell'analisi: rischio residuo AS-IS

Il lavoro di analisi del rischio e la valutazione dello stesso considerando le contromisure applicate (rischio residuo), è svolto conducendo le seguenti attività:

- Assessment dei controlli di sicurezza rispetto alle best practices dell'Annex A dello Standard ISO/IEC 27001;
- Analisi degli impatti a fronte di una perdita di disponibilità, riservatezza e integrità delle informazioni per i servizi in ambito;
- Analisi delle vulnerabilità e delle minacce sugli asset;
- Valutazione del rischio as-is della sicurezza delle informazioni e identificazione di una scala di priorità.

4.4.3 Analisi dei gap e selezione delle contromisure da implementare

A valle del lavoro di analisi svolto, al fine di indirizzare eventuali rischi/issues rilevanti nell'ambito dei servizi erogati dal Gruppo Aruba S.p.A e/o nell'ottica di perseguire il miglioramento continuo del SGSI, si elaborano i dati ottenuti dalle analisi effettuate nel tool di Risk Analysis per identificare le aree di rischio per le quali definire opportuni interventi di sicurezza.

Per individuare le azioni ritenute migliorative e ridurre i rischi è quindi definita, di volta in volta, un gap analysis volta a valutare la distanza tra il livello di applicazione attuale delle contromisure di sicurezza e il livello massimo applicabile.

4.4.4 Piano di Trattamento del Rischio - Razionalizzazione degli interventi

Le azioni identificate nel gap analysis sono poi raggruppate in specifiche iniziative progettuali e documentate all'interno del Piano di Trattamento del Rischio.

5 FREQUENZA DI ANALISI

Il processo di gestione dei rischi per la sicurezza delle informazioni deve essere eseguito ogni 12 mesi, o prima in caso di eventi significativi, quali a titolo esemplificativo ma non esaustivo:

- Nuovi asset che entrano a far parte dell'ambito del Risk Management;
- Nuove minacce presenti sia all'esterno che all'interno dell'organizzazione e che non sono state valutate;
- Possibilità che nuove o aumentate vulnerabilità possano essere sfruttate da minacce;
- Riesame delle vulnerabilità già identificate per determinare quelle che potrebbero essere maggiormente esposte a nuove o riemergenti minacce;
- Aumentati impatti o conseguenze delle minacce sugli asset, vulnerabilità e rischi che aggregati determinano un livello complessivo di rischio inaccettabile;

- Incidenti di sicurezza di particolare gravità.

Inoltre, possono essere svolte attività di analisi con frequenza diversa, ad esempio in relazione alla rispondenza a particolari norme o esigenze di certificazione.

STORICO VERSIONI

VERSIONE 1.0 DEL 01/01/2022	***NATURA DELLE MODIFICHE: Prima emissione***