Basis
Information Technology

NIS2 e la necessità di un approccio end-to-end alla cybersecurity

Christian Callegari, BU Manager – IT & Cybersecurity

Cybersecurity in **Italia**

+65%

Attacchi in crescita rispetto al 2022

Nettamente superiore al +11% raggiunto a livello globale

11%

Gli attacchi gravi globali mappati dal Clusit in Italia

Il 7,6% nel 2022

81%

Gli attacchi di severità “critica” o “grave” nel 2023

Contro il 47% del 2019

CRITICITÀ

I 10 settori più attaccati

Government / Military / Forze dell'Ordine
19%

Finance / Insurance
9%

Manufacturing
13%

Retail
9%

Logistica e trasporti
12%

ICT
6%

Multiple Targetsal
11%

Healthcare, Professional / Scientific / Technical e Organizations
4%

I costi principali di un attacco informatico riguardano:

- Rilevamento
- Perdita di business
- Risposta post violazione
- Assistenza legale

Il **costo** di un attacco

Secondo l'edizione 2022 del “Cost of a data breach report” di IBM, in Italia, nel 2022 il costo medio di un cyberattacco è stato di

3,7

Milioni di euro

In vigore dal 17 Gennaio 2023

Normativa **NIS2**

Importante passo verso la definizione della strategia per la cyber sicurezza dell'unione europea

La Direttiva si inserisce a pieno titolo partendo dal presupposto secondo il quale, i sistemi informatici e di rete usati per fornire servizi essenziali in settori chiave, occupano una porzione centrale nel percorso sempre più rapido di trasformazione digitale e di interconnessione della società (ricordiamo che NIS è, per l'appunto, l'acronimo di Network and Information Security).

Direttiva NIS2

Direttiva UE 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 sulla sicurezza delle reti e delle informazioni

NIS2 - **Perché "critici"**

Fornitori di servizi in cloud

I fornitori di servizi cloud devono affrontare sfide uniche in termini di sicurezza informatica, tra cui la **violazione dei dati e gli accessi** non autorizzati alle informazioni sensibili. Per questo la Direttiva NIS 2 impone l'obbligo di migliorare la loro resilienza di tali servizi.

Settore sanitario

Il settore sanitario archivia ed elabora grandi quantità di **informazioni sensibili e riservate**, è questo che rende questo settore un obiettivo primario per attacchi informatici. Viene automatico che le violazioni della sicurezza informatica nel settore sanitario possono avere gravi conseguenze, fra cui la compromissione dei dati dei pazienti, l'interruzione dei servizi medici e danni alla reputazione del Paese.

Settore energetico

Il settore energetico è **fondamentale per il funzionamento** della società e dell'economia; ed ecco che attraverso misure di sicurezza adeguate, valutazioni periodiche del rischio, e collaborazione con le parti interessate, le aziende interessate possono salvaguardare la continuità della fornitura energetica.

Quali sono gli elementi **più critici**

OT/ICS - Sistemi di controllo industriale

Il ruolo fondamentale nella gestione e nel controllo delle infrastrutture critiche e dei processi industriali fa sì che la Direttiva NIS2 imponga requisiti e obblighi di conformità specifici alle organizzazioni che utilizzano sistemi di controllo industriale, al fine di garantirne la sicurezza e l'affidabilità.

Dispositivi IoT

Autenticazione debole, protocolli di comunicazione non sicuri, e mancanza di aggiornamenti del firmware, sono i principali rischi insiti nei dispositivi IoT; di conseguenza sono ciò da cui partire per innalzare il livello di cybersecurity in conformità alla Direttiva NIS 2.

NIS2

La strada verso la conformità

Da una visione strategica alla pianificazione di azioni "tattiche" ben precise

Comprendere I requisiti

Creare un team di conformità Interfunzionale

Gap Analysis

Sviluppare una strategia Informatica completa e un quadro governance

Implementare solide pratiche di gestione della sicurezza delle informazioni

Migliorare le misure di sicurezza della catena di approvvigionamento

Testare, rivedere e migliorare

NIS2 - **Le misure tecniche minime previste**

Le misure sono basate su un approccio **multirischio** mirante a proteggere i sistemi informatici e di rete e il loro ambiente fisico da incidenti e comprendono almeno gli elementi seguenti:

Politiche di **analisi dei rischi e di sicurezza** dei sistemi informatici

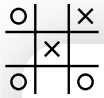
Gestione degli incidenti

Continuità operativa, come la gestione del backup e il ripristino in caso di disastro e gesione delle crisi

Sicurezza della **catena di approvvigionamento** compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi

Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la **Gestione** e la divulgazione **delle vulnerabilità**

NIS2 - **Le misure tecniche minime previste**



Strategie e procedure per **valutare l'efficacia** delle misure di gestione dei rischi di cibersicurezza

Pratiche di igiene informatica di base e **formazione** in materia di cibersicurezza

Politiche e procedure relative all'uso della **crittografia** e, se del caso, della **cifratura**

Sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi

Uso di soluzioni di **autenticazione a più fattori** o di autenticazione continua , di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso.

NIS2 Approccio Multirischio

Poiché le minacce alla sicurezza dei sistemi informatici e di rete possono avere origini diverse, le misure di gestione dei rischi di cibersicurezza dovrebbero essere basate su un approccio **multirischio** mirante a **proteggere i sistemi informatici** e di rete e il loro ambiente fisico da **eventi** quali furti, incendi, inondazioni, problemi di telecomunicazione o interruzioni di corrente, o da qualsiasi **accesso fisico** non autorizzato nonché dai danni alle informazioni detenute dai soggetti essenziali o importanti e agli impianti di trattamento delle informazioni di questi ultimi e dalle **interferenze** con tali informazioni o impianti che possano compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informatici e di rete o accessibili attraverso di essi.

NIS2 Approccio Multirischio

Le misure di gestione dei rischi di cibersicurezza dovrebbero pertanto **affrontare anche la sicurezza fisica** e dell'ambiente dei sistemi informatici e di rete includendo misure volte a proteggere detti sistemi da **guasti** del sistema, **errori** umani, **azioni malevole** o **fenomeni naturali**, in linea con le norme europee e internazionali, come quelle di cui alla serie **ISO/IEC 27000**.

A tale riguardo, i soggetti essenziali e importanti dovrebbero altresì, nell'ambito delle loro misure di **gestione dei rischi** di cibersicurezza, affrontare la questione della **sicurezza delle risorse umane** e disporre di strategie adeguate di controllo dell'accesso. Tali misure dovrebbero essere coerenti con la direttiva (UE) 2022/2557 (Direttiva CER – Resilience of Critical Entities)

IL GIUSTO APPROCCIO

La necessità di un approccio sistemico

Per affrontare efficacemente il problema, è fondamentale adottare un approccio sistemico alla **cybersecurity OT**, che comprenda i seguenti punti:

- Valutazione del rischio
- Protezione
- Monitoraggio e risposta
- Educazione e consapevolezza
- Miglioramento continuo

La necessità di un approccio sistemico

L'approccio sistemico alla cybersecurity è una metodologia olistica che considera la sicurezza informatica come un sistema complesso composto da persone, processi e tecnologie. Questo approccio si contrappone a un approccio puntuale che si concentra solo su singoli aspetti della sicurezza, come la tecnologia o la formazione degli utenti.

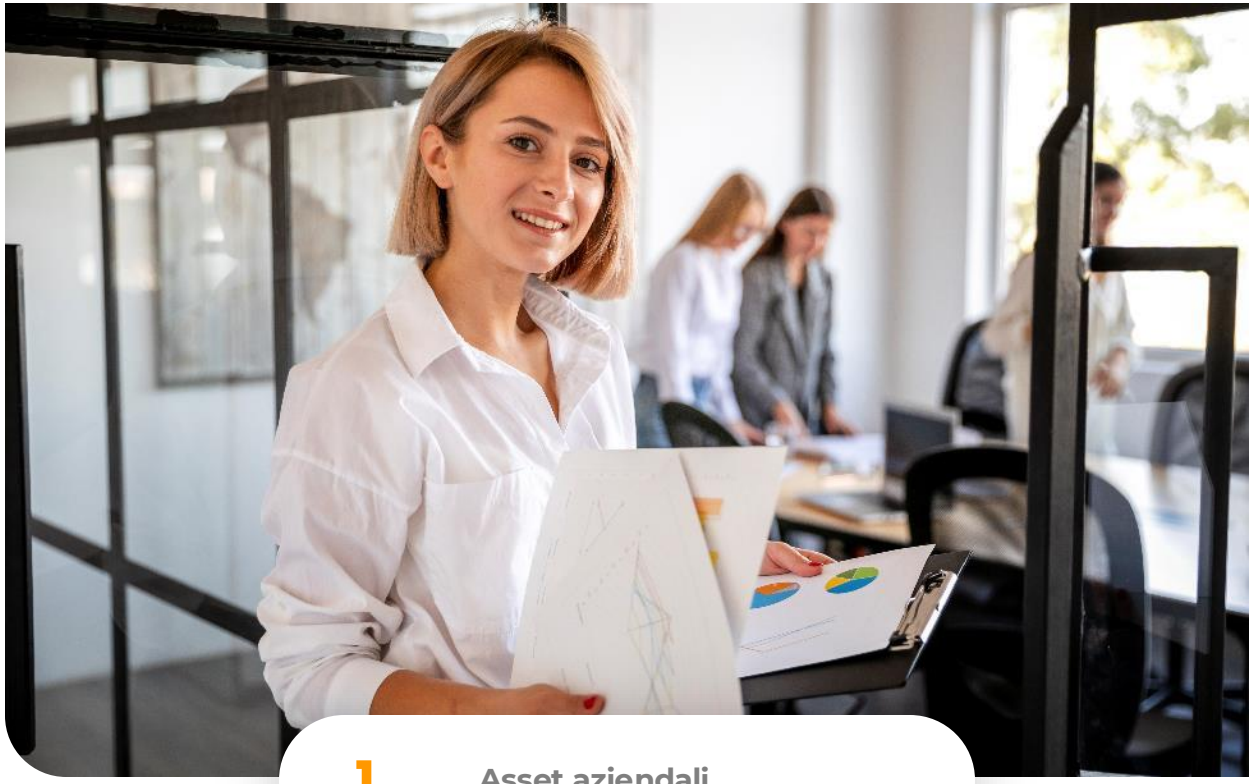
Considerare la sicurezza informatica come un processo continuo

Adottare una visione olistica

Gestire i rischi

Adottare un approccio basato sulle evidenze

Comunicare e collaborare



Fase di **Pre- assessment**

Oltre alla definizione del perimetro, definizione di un documento di gap analysis che evidenzi le misure tecniche necessarie per raggiungere la compliance con la norma.

1 Asset aziendali

2 GAP

3 Roadmap

Fase di **Pre-assessment**

Asset Aziendali

Elenco di tutti gli asset aziendali che rientrano nel perimetro della norma (ad esempio i server che gestiscono l'erogazione del servizio sicuramente rientreranno nel perimetro, mentre i PC dei dipendenti potrebbero non essere di interesse, così come non lo saranno molto probabilmente stampanti/telecamere etc.)

GAP

La lista di tutti i gap tecnici/tecnologici/procedurali che sono stati riscontrati per il raggiungimento della compliance alla norma, con una spiegazione del perché rappresentano un elemento di non compliance con la norma

Roadmap

Una roadmap per il raggiungimento e il successivo mantenimento della compliance

Profilo di rischio aziendale

Basato su intervista al responsabile IT e ad interviste (random) agli impiegati:

- Identificazione **asset critici**
- Identificazione **dati critici**
- Identificazione verosimiglianza attacchi hacker
- Definizione del livello di rischio

Valutazione del **rischio ambientale**

Valutazione **della consapevolezza del rischio cyber aziendale**

Output:

Report di risk assessment report, contenente la "risk matrix**"**

RISK ASSESSMENT MATRIX

SEVERITY	CONSEQUENCES				INCREASING LIKELIHOOD				
	PHYSICAL	INTELLECTUAL	HUMAN	FINANCIAL	1	2	3	4	5
					Never happened	Heard of it happening to other organizations	Has happened to my organization at least one time in the past	Has happened to my organization more than once	Has happened to my organization more than once per year
1	No damage	No effect	No effect	No effect	Continuously monitor and make improvements as needed				
2	Minor damage	Minor effect	Minor effect	Minor effect					
3	Moderate damage	Moderate effect	Moderate effect	Moderate effect			Mitigate impact to as reasonably possible		
4	Major damage	Major effect	Major effect	Major effect					
5	Destroyed	Massive effect	Massive effect	Massive effect			Identify and enact critical changes needed to protect and maintain operations		

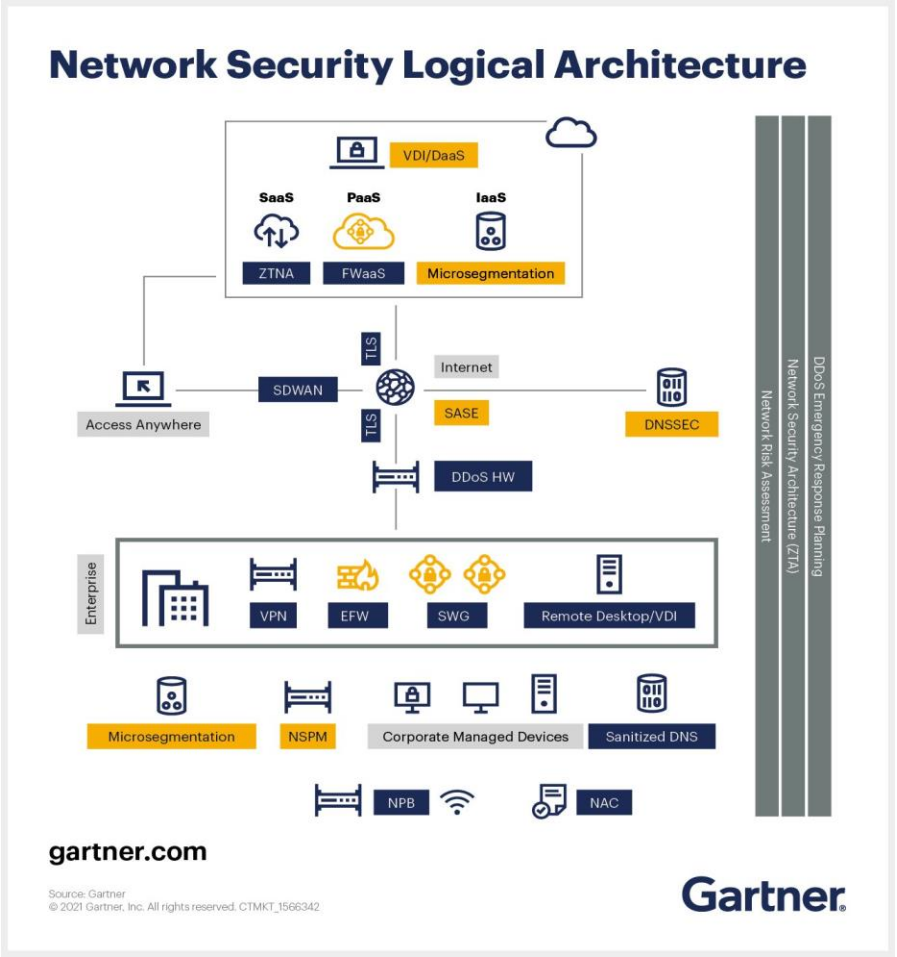
Assessment **Architettura IT**

01 **Analisi dell'architettura dell'infrastruttura IT dal punto di vista della cybersecurity**

02 **Verifica Best Practises**

- Posizionamento e configurazione degli apparati di cybersecurity
- Segmentazione della rete
- Analisi configurazione Smart working
- Analisi tecnologie di accesso remoto (VPN, etc.)
- Analisi dei firewall
- Etc.

Output: report del security assessment contenente delle linee guida per rendere l'infrastruttura più sicura



Gestione **Vulnerabilità**

Principale elemento di sicurezza proattiva

Identificazione delle vulnerabilità:

Valutazione delle vulnerabilità:

Correzione delle vulnerabilità

1 - Identificazione delle **Vulnerabilità**

La prima fase consiste nell'identificare le vulnerabilità presenti nei sistemi e nelle reti.
Questo può essere fatto utilizzando una varietà di metodi, tra cui:

Scansione delle vulnerabilità:

Strumenti automatici che scansionano i sistemi e
le reti per identificare vulnerabilità note.

Test di penetrazione:

Simulazioni di attacchi informatici condotti da esperti di sicurezza per iden tificare vulnerabilità non ancora note.

Analisi del codice sorgente:

Revisione del codice sorgente dei softwa re per identificare potenziali vulnerabilit à.

2 - Valutazione delle **Vulnerabilità**

Una volta identificate le vulnerabilità, è necessario valutarne il rischio potenziale. Questo implica la considerazione di diversi fattori, tra cui:

La gravità della vulnerabilità:

Il potenziale impatto che la vulnerabilità potrebbe avere sui sistemi e sui dati aziendali.

La facilità di exploit:

La facilità con cui un malintenzionato può sfruttare la vulnerabilità per lanciare un attacco.

La disponibilità di exploit:

L'esistenza di codice o strumenti che possono essere utilizzati per sfruttare la vulnerabilità.

3 - Correzione delle **Vulnerabilità**

In base alla valutazione del rischio, le vulnerabilità devono essere corrette o mitigate. Questo può essere fatto in diversi modi, tra cui:

Applicare patch di sicurezza:

i fornitori di software rilasciano regolarmente patch per correggere le vulnerabilità note.

Aggiornare il software:

Installare le ultime versioni del software per beneficiare delle correzioni di sicurezza più recenti.

Implementare controlli di sicurezza compensativi:

Mettere in atto misure di sicurezza aggiuntive per mitigare il rischio di una vulnerabilità che non può essere immediatamente corretta.

Gestione Vulnerabilità

Il processo di vulnerability management è
un ciclo continuo che deve essere ripetuto regolarmente per garan
tire che i sistemi e le reti rimangano protetti dalle ultime minacce.

Business **Continuity (BC)**

L'obiettivo è minimizzare l'impatto negativo sull'azienda, proteggendo i suoi beni, la sua reputazione e la sua capacità di generare profitti.

Ecco i 3 punti chiave della Business Continuity:

Pianificazione

Implementazione

Monitoraggio e Miglioramento

Pianificazione (BC)

01

La BC inizia con la creazione di un piano di continuità aziendale –BCP – completo.

02

Il BPC deve identificare i rischi potenziali per l'azienda, le strategie di mitigazione e le procedure di risposta per ogni tipo evento di interruzione.

03

Il piano deve includere dettagli su come mantenere le operazioni critiche, come la comunicazione, la gestione dei dati e la supply chain.

Implementazione (BC)

Formazione dei dipendenti sulle procedure di BC, l'implementazione di sistemi di backup e ripristino (Disaster Recovery) e la messa in atto di controlli di sicurezza per proteggere i dati e le infrastrutture aziendali.

04

05

È fondamentale testare regolarmente il BCP per assicurarne l'efficacia e aggiornarlo periodicamente per riflettere i cambiamenti nell'ambiente aziendale.

Monitoraggio e miglioramento (BC)

La BC è un processo continuo che richiede monitoraggio e miglioramenti costanti.

06

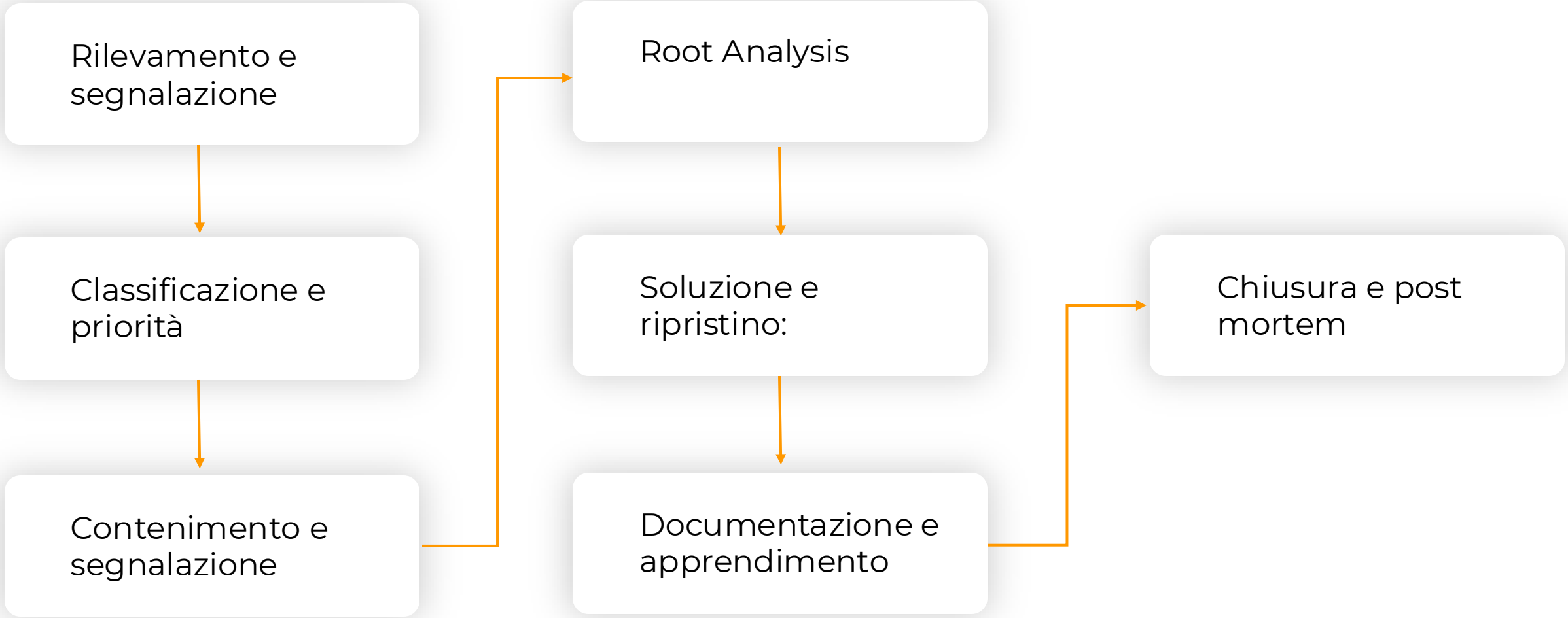
07

Importante valutare regolarmente l’efficacia del BCP e identificare le aree di miglioramento.

Business **Continuity (BC)**

Le lezioni apprese dagli eventi di interruzione passati devono essere utilizzate per aggiornare il BCP e rafforzare la resilienza aziendale.

Gestione incidenti



Gestione incidenti

Un team di risposta agli incidenti dedicato

Comunicazione efficace

Un piano di risposta agli incidenti (IRP)

Test e esercitazioni regolari

Strumenti di automazione (SIEM)

Grazie!

Manager – BU IT & Cybersecurity
Christian Callegari
christian.callegari@basisgroup.com
+39 335 676 4948

Senior Sales Account – BU IT & Cybersecurity
Mario Reggiani
mario.reggiani@basisgroup.com
+39 3938029432

Sede Operativa
Via Valentini, 14 - 59100 Prato (PO)
www.basisinformationtechnology.com

Grazie!

Manager – BU IT & Cybersecurity
Christian Callegari
christian.callegari@basisgroup.com
+39 335 676 4948

Sede Operativa
Via Valentini, 14 - 59100 Prato (PO)
www.basisinformationtechnology.com