DIGITALCAMPUS
guidiamo l'innovazione

CSI
your digital partner

Corso NIS2 Mastering Compliance per Organi di Amministrazione e Direttivi

MODULO 2

Enzo Veiluva – Resp. CYBERSECURITY e Business Continuity – CSI Piemonte

11 giugno 2026

ASL AL
REGIONE PIEMONTE

Contenuti – Modulo 2

B) Competenze decisionali del manager: il “Cosa” chiedere ed il “Come” attuare

1. **Cosa significa “Fare Sicurezza”: impostare un Sistema Difensivo**
    - Le 3 Fasi Temporali: Prevenzione, Rilevamento, Reazione
    - L’impostazione del MOGS (modello Organizzativo di gestione della Sicurezza ICT)
    - La gestione del piano di rischi aziendali (metodologia e azioni)
    - Il monitoraggio delle attività: l’interazione degli organi direttivi con il CISO, il DPO, il responsabile Formazione, Ufficio Legale/contratti, il fornitore IT
2. **Applicazione della NIS 2 in pratica (le azioni di valutazione degli Organi Direttivi)**
    - La security by design: cosa significa e cosa comporta.
    - L’impianto documentale da mantenere: il governo dei processi e regolamenti, elenchi, mappature
    - La Data Protection: perché non solo la Cybersecurity
    - Il piano formativo Cyber per i dipendenti.
    - La gestione degli incidenti: obblighi di notifica e azioni da attivare

Come fare sicurezza

Le azioni da mettere in campo

Assessment & Gap analysis

- Identificare i principali gap attraverso un **assessment** generale
- Eseguire **Vulnerability Assessment e Penetration Test** periodicamente
- Condurre l'attività di **Threat Intelligence** per verificare esposizione ai rischi cyber
- **Phishing Campaign**

Piano strategico delle iniziative Cyber

- Identificare le **azioni correttive** per coprire i gap individuati con le attività precedenti
- **Disegnare un percorso sostenibile** per le iniziative dell'Ente in ambito Security
- **Formazione** del personale
- Adozione di **misure tecniche** ed **organizzative**

BIA ed impostazione Piano di ripartenza dei servizi

- Eseguire la **Business Impact Analysis (BIA)** al fine di identificare i principali sistemi critici
- Redigere il **piano di risposta agli incidenti** e di **ripartenza dei servizi** sulla base dei risultati della **BIA**
- Definire il modello e i **processi di gestione della crisi ICT**

La Direttiva NIS2 – Approccio metodologico

Misure di sicurezza di base

41 misure di sicurezza → 10 ambiti di sicurezza NIS

- 36 per soggetti essenziali e importanti.
- 5 addizionali solo per i soggetti essenziali.

Struttura misura: codice + descrizione + requisiti

- Il codice identificativo e la descrizione della misura fanno riferimento al FNSC.
- I requisiti indicano ciò che è richiesto ai fini dell'implementazione.

116 requisiti → Proporzionalità

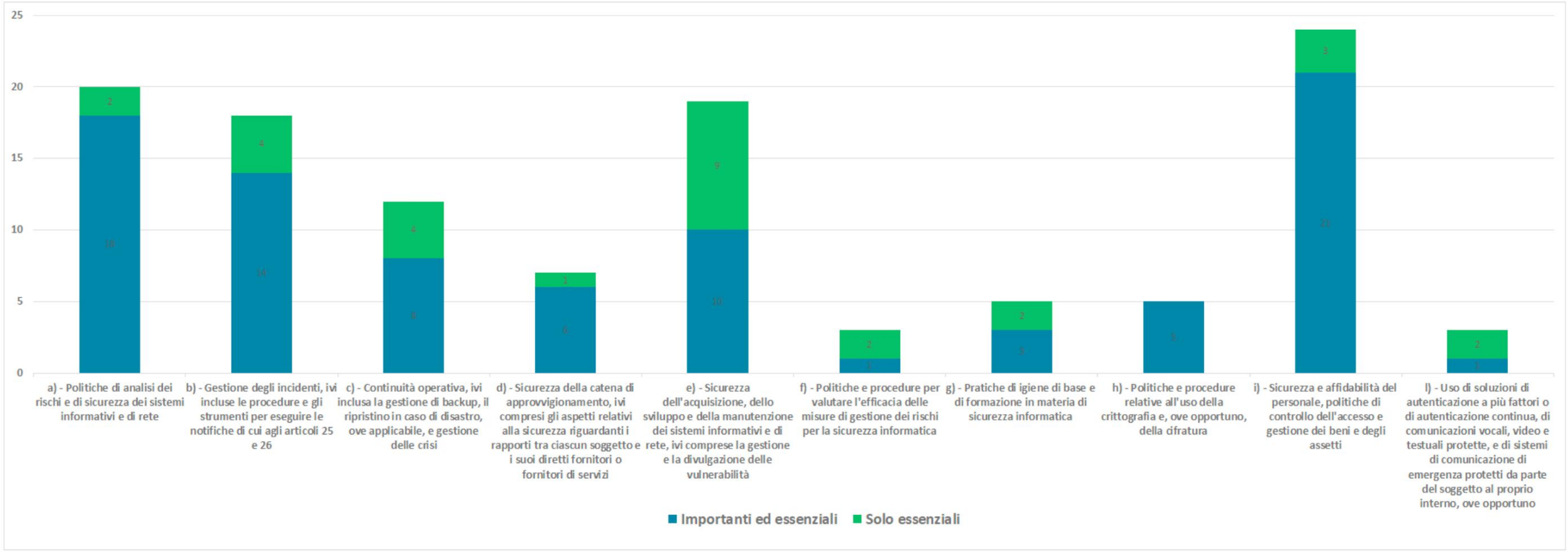
- 82 per soggetti essenziali e importanti.
- 34 addizionali solo per i soggetti essenziali.

La Direttiva NIS2 – Focus Misure di Sicurezza: Ambiti

a) Politiche di analisi dei rischi e di sicurezza dei sistemi informativi.	b) Gestione degli incidenti.	c) Continuità operativa, inclusa la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi.	d) Sicurezza catena di approvvigionamento, compresi aspetti relativi sicurezza rapporti con diretti fornitori o fornitori di servizi.	e) Sicurezza acquisizione, sviluppo e manutenzione sistemi informativi e di rete, ivi compresa gestione e divulgazione vulnerabilità.
f) Politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza.	g) Pratiche di igiene informatica di base e formazione in materia di cybersicurezza.	h) Politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura.	i) Sicurezza risorse umane, strategie di controllo dell'accesso e gestione degli assetti.	j) Uso di soluzioni di autenticazione a più fattori o di autenticazione continua e di sistemi di comunicazione protetti.

Elementi obblighi in materia di misure di gestione dei rischi per la sicurezza informatica (art. 24, c. 2 d.lgs. 138/2024)

La Direttiva NIS2 – Mappatura Requisiti art. 24



Evidenze documentali

Elenchi

Personale dell'organizzazione di sicurezza informatica, *configurazioni di riferimento*, sistemi ai quali è possibile accedere da remoto.

Inventari

Apparati fisici, servizi, sistemi e applicazioni software, *flussi di rete*, servizi erogati dai fornitori, fornitori

Piani

Gestione del rischio, business continuity e disaster recovery, trattamento del rischio, gestione delle vulnerabilità, adeguamento, *valutazione dell'efficacia delle misure di gestione del rischio*, formazione in materia di sicurezza informatica, risposta agli incidenti

Politiche

definite per almeno i requisiti riportati nella tabella 1 in appendice all'Allegato 1, per i soggetti importanti, e all'allegato 2, per i soggetti essenziali, della determina 164179/2025

Procedure

In relazione agli specifici requisiti per i quali sono richieste.

Registri

Esiti del riesame delle politiche, attività formazione dei dipendenti, *manutenzioni effettuate*.

La Direttiva NIS2 – Approccio basato sul rischio

Ambito	Livello di rischio	Proporzionalità	Approccio	Clausole
Le misure di sicurezza si applicano a tutti i sistemi informativi e di rete del soggetto.	Ogni sistema informativo e di rete è caratterizzato da un proprio livello di rischio.	L'art. 31 del decreto prevede che si tenga conto, nello stabilire gli obblighi, del grado di esposizione dei soggetti ai rischi.	Le misure di sicurezza sono state sviluppate secondo un approccio basato sul rischio.	Previsione per i requisiti di maggiore complessità di specifiche clausole.

La Direttiva NIS2 – Approccio basato sul rischio

14 requisiti per i soggetti importanti
e **19** per i soggetti essenziali

6 requisiti per i soggetti importanti
e **9** per i soggetti essenziali

Facoltà di limitare l'ambito di applicazione per specifici requisiti ai sistemi informativi di rete la cui compromissione determina un impatto significativo su R, I, D delle attività e servizi per i quali il soggetto rientra nell'ambito di applicazione del decreto NIS.

“ **... per almeno i sistemi informativi e di rete rilevanti ...** ”

“ **... in accordo agli esiti della della valutazione del rischio di cui alla misura ...** ”

Possibilità di adattare le modalità di attuazione di specifici requisiti sulla base degli esiti della valutazione del rischio.

Deroga all’applicazione del requisito se sussistono vincoli normativi (ad esempio, leggi o regolamenti) o tecnici (ad esempio, limiti tecnologici o operativi) che non ne permettano l’implementazione.

“ **... fatte salve motivate e documentate ragioni normative o tecniche ...** ”

“ **... forniture con potenziali impatti sulla sicurezza ...** ”

Sono considerate le forniture la cui eventuale compromissione può determinare effetti sulla sicurezza dei sistemi informativi e di rete.

8 requisiti per i soggetti importanti
e **10** per i soggetti essenziali

3 requisiti per i soggetti importanti
e per i soggetti essenziali

Sistemi Informativi e di Rete «RILEVANTI»

In linea di principio, le misure di sicurezza si applicano a tutti i sistemi informativi e di rete del soggetto NIS (per la definizione di "**sistema informativo e di rete**" si faccia riferimento all'articolo 2, comma 1, lettera p) del decreto NIS). Ove, tuttavia, la disposizione di un requisito, o di parte di esso, contiene la dicitura **«per almeno i sistemi informativi e di rete rilevanti»,** il soggetto NIS ha la facoltà di **limitare l'ambito di applicazione** della disposizione **ai sistemi informativi e di rete la cui compromissione comporterebbe un impatto significativo sulla confidenzialità, integrità e disponibilità** delle attività e servizi **per i quali il soggetto NIS rientra nell'ambito di applicazione del decreto NIS**.

Sistemi Informativi e di Rete «RILEVANTI» Art. 2 Comma 1 Lett. P

"**sistema informativo e di rete**"

1) una rete di comunicazione elettronica ai sensi dell'articolo 2, comma 1, lettera vv), del decreto legislativo 1° agosto 2003, n. 259;

*i **sistemi di trasmissione**, basati o meno su un'infrastruttura permanente o una capacità di amministrazione centralizzata e, se del caso, **le apparecchiature di commutazione o di instradamento** e altre risorse, inclusi gli **elementi di rete non attivi**, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti mobili e fisse (a commutazione di circuito e a commutazione di pacchetto, compresa internet), **i sistemi per il trasporto via cavo della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti utilizzate per la diffusione radiotelevisiva e le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato**;*

2) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali;

3) i dati digitali conservati, elaborati, estratti o trasmessi per mezzo di reti o dispositivi di cui ai numeri 1) e 2), per il loro funzionamento, uso, protezione e manutenzione;

Sistemi Informativi e di Rete «RILEVANTI»: esempi di valutazione

4. Criteri pratici per individuare i sistemi rilevanti

Criterio ACN	Domande da porsi	Esempi tipici
Impatto sul servizio	Se il sistema si ferma, il servizio NIS2 smette di funzionare?	Core-banking, portali anagrafici, sistemi SCADA
Dati trattati	Contiene o trasmette dati personali/sanitari/critici?	Database cittadini, repository referti medici
Interconnessioni	Serve da ponte tra reti interne ed esterne?	VPN, firewall, API gateway
External dependency	È un servizio cloud o di terza parte senza il quale l'ente non opera?	SaaS ERP, servizi DNS, CDN
Privilegi e identità	Gestisce autenticazione e autorizzazioni?	Active Directory, IdP, HSM

ESEMPIO DI SISTEMI RILEVANTI PER ASL/ASO

1. Sistemi sanitari e clinici
Cartella Clinica Elettronica (CCE), Fascicolo Sanitario Elettronico (FSE), Sistema Informativo Ospedaliero (HIS), CUP e prenotazioni, Pronto Soccorso, Ricoveri e dimissioni, Prescrizione elettronica, Refertazione digitale, Telemedicina, RIS, PACS, LIS, Anagrafe assistiti.

2. Dispositivi medici e diagnostici connessi
TAC, RMN, Ecografi, Mammografi, PET, Angiografi, Sistemi radiologici digitali, Ventilatori polmonari, Monitor multiparametrici, Pompe infusionali, Defibrillatori connessi, Robot chirurgici, Dispositivi IoMT.

3. Infrastruttura IT e rete
Server fisici e virtuali, Hypervisor, Storage, Sistemi di backup, Sistemi di disaster recovery, Data center, Cloud (IaaS, PaaS, SaaS), LAN/WAN/Wi-Fi, Switch, Router, DNS/DHCP, Bilanciatori di carico.

4. Sicurezza informatica e gestione accessi
Firewall e WAF, IDS/IPS, VPN, SIEM/SOAR, EDR/XDR, Antivirus e antimalware, DLP, IAM, PAM, MFA, Active Directory, PKI, Vulnerability Management, Patch Management.

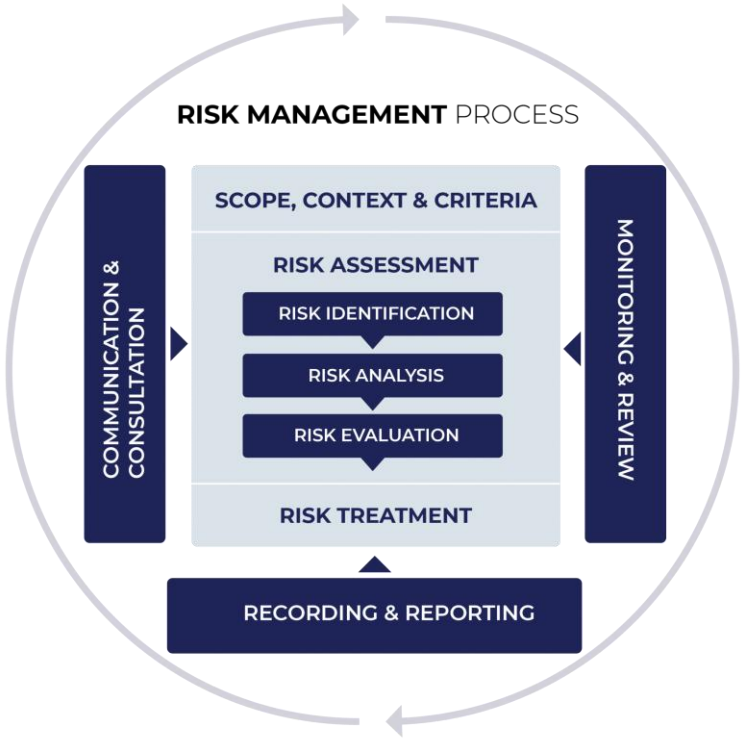
5. Sistemi amministrativi e di supporto
ERP, Contabilità e bilancio, Acquisti e magazzino, Gestione farmaci, Protocollo informatico, Gestione documentale, Firma digitale, Gestione del personale, Presenze e turnazioni, Payroll, Conservazione digitale.

6. Comunicazioni, servizi digitali e impianti
Posta elettronica e PEC, VoIP e centralino IP, Videoconferenza, Portale istituzionale, Portale cittadini, Portale dipendenti, API e servizi web, Building Management System (BMS), SCADA, Controllo accessi fisici, Videosorveglianza, Gestione UPS e gruppi elettrogeni, Gestione gas medicali e impianti tecnologici.

Concetti base di RISK Management

Il processo secondo la linea guida ISO 31000

- Aver chiari gli **obiettivi del business**
- Definire le **soglie di tolleranza**
  - Risk appetite (propensione al rischio)
  - Risk tolerance (devianza tollerabile rispetto alla propensione)
  - Risk capacity (massimo livello di rischio sopportabile)
- Fare un Risk assessment
  - Identificare le **minacce** e le **opportunità**
  - **Analizzare** il rischio (Probabilità e Impatti)
  - **Ponderare** il rischio rispetto alle soglie
- Scegliere le azioni **di trattamento** dei rischi valutati
- Identificare gli **indicatori di rischio** e i parametri di controllo (**KRI**)
- **Reporting e approvazione** da parte del management
- **Monitoraggio, miglioramento** e **revisione** periodica



Il rischio è….

L’**effetto** dell’**incertezza** sugli **obiettivi**

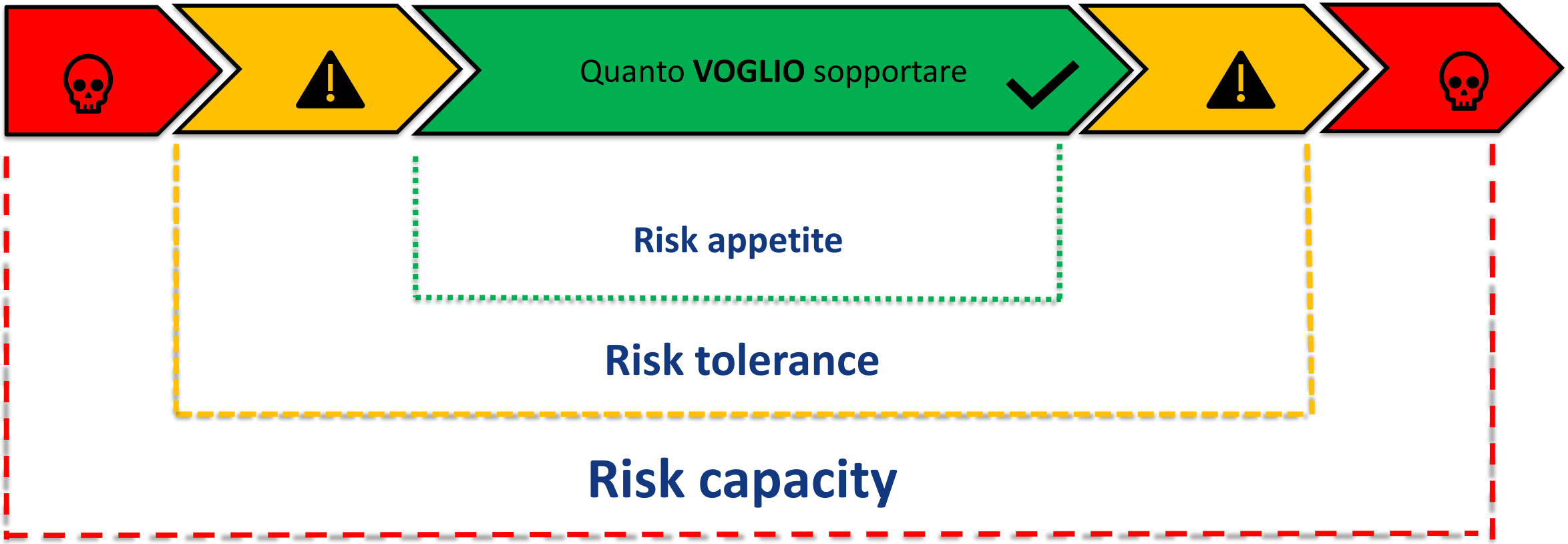
Obiettivi del business

- **S** SPECIFIC
- **M** MEASURABLE
- **A** ACHIEVABLE
- **R** RELEVANT
- **T** TIME-BASED

Stabilire le soglie di tolleranza al rischio

Piano strategico

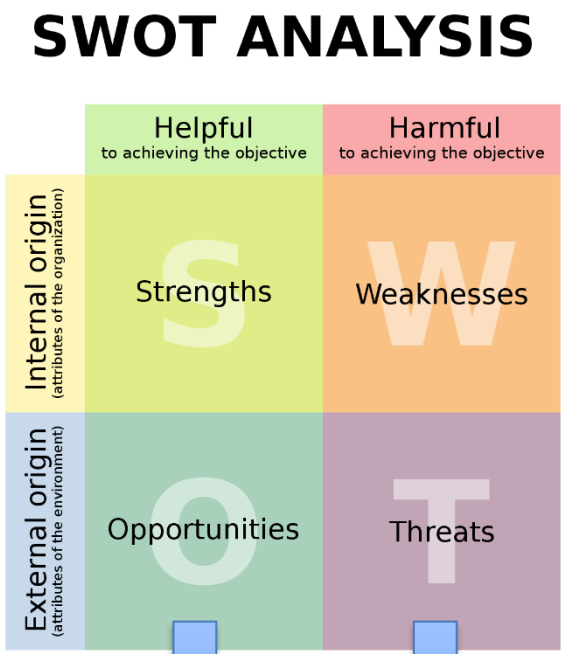
Quanto **POSSO DISCOSTARMI** dai miei **obiettivi**



Identificare le minacce e le opportunità | Swot analysis

Piano strategico

- Obiettivo a
- Obiettivo b
- Obiettivo c
- Obiettivo d
- Obiettivo ...

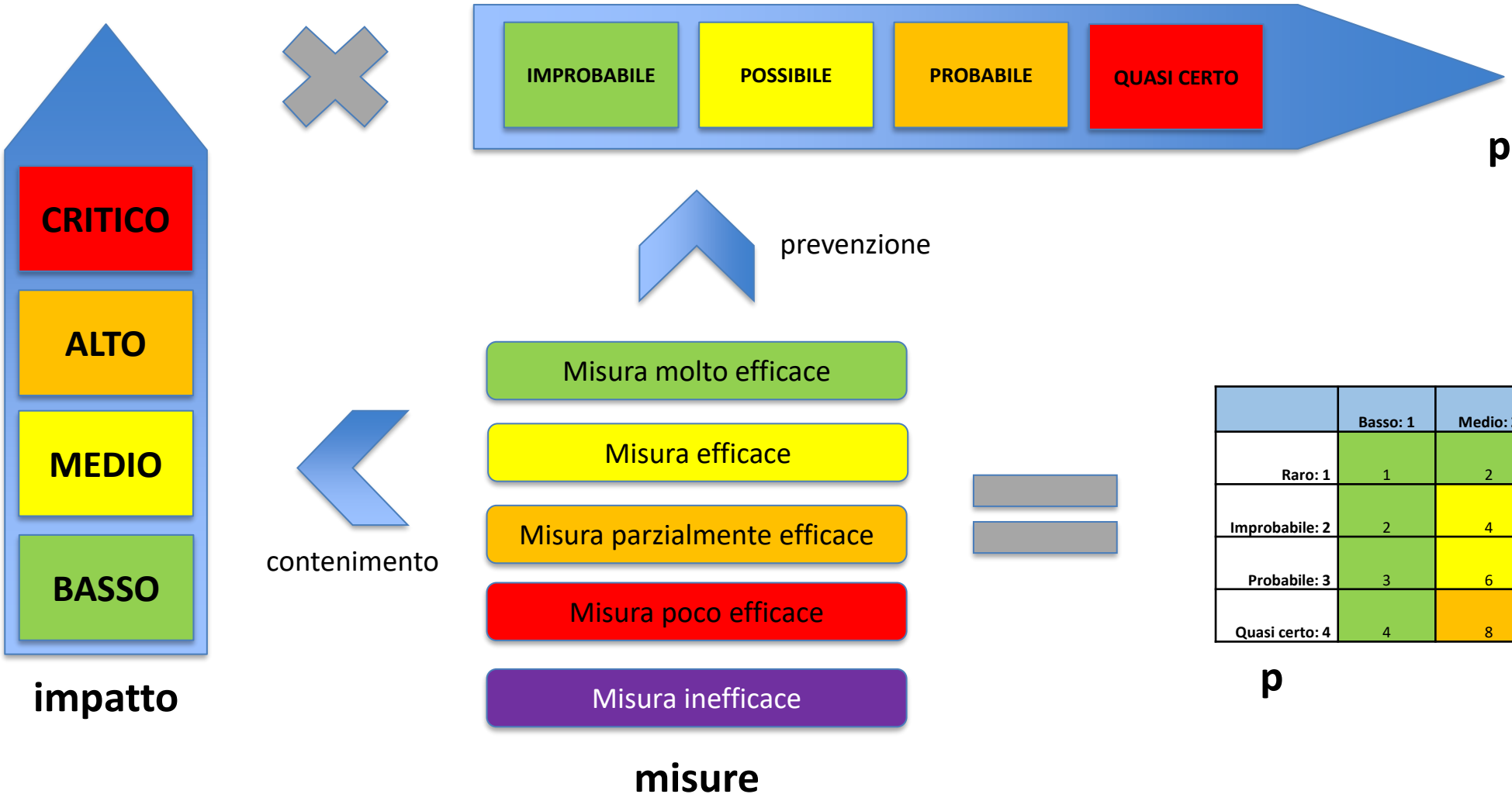


prendo coscienza dei punti forza e debolezza dell'organizzazione

li confronto con le minacce e le opportunità del contesto

agisco di conseguenza per garantire il raggiungimento degli obiettivi di business

Analizzare il rischio | Dal rischio inerente al rischio attuale



	Basso: 1	Medio: 2	Alto: 3	Critico: 4
Raro: 1	1	2	3	4
Improbabile: 2	2	4	6	8
Probabile: 3	3	6	9	12
Quasi certo: 4	4	8	12	16

p

i

Analizzare il rischio | probabilità e impatto

Matrice 4 x 4

Per limitare la soggettività e per facilitare la focalizzazione sugli elementi rilevanti

Probabilità/verosimiglianza	Livello
4	Quasi certo
3	Probabile
2	Possibile
1	Improbabile

Impatto	Livello
4	Critico
3	Alto
2	Medio
1	Basso

Impatto per asset										
Dati			Hardware	Software	Rete e comunicazioni	Fisici	Persone	Finanziari	Processi	Immateriali
R	I	D								

Per il calcolo del rischio si utilizza il valore di impatto relativo all'asset sul quale la minaccia potrebbe produrre il **massimo impatto**

Valutazione impatto | criteri

		Economico	Compliance	Reputazionale	Livello di Servizio	Sicurezza del dato e delle informazioni		
Impatto	**Livello**					**Integrità**	**Disponibilità**	**Riservatezza**
4	Critico	Impatto economico pari o superiore al 10% del valore della produzione.	Condanna penale nei confronti del management, ovvero sospensione temporanea dell'attività d'impresa.	Danno d'immagine con esposizione mediatica sovraregionale e teporalmente rilevante (> 5 giorni)	La violazione degli SLA contrattualizzati comporta la perdita del cliente.	I dati gestiti sono oggetto di transazioni economiche, finanziarie o sanitarie o segreti aziendali. La mancanza di integrità dei dati ha impatti molto elevati sulle attività operative (superiore a 1 FTE).	L'indisponibilità dei dati oltre agli SLA e ai tempi di RTO e RPO definiti contrattualmente può comportare interruzioni a servizi pubblici essenziali con effetto domino su altri servizi.	I dati sono di tipo particolare ad elevato interesse pubblico o nazionale e l'eventuale diffusione può compromettere in maniera permanente il business e i diritti degli interessati.
3	Alto	Impatto economico superiore al 5% e inferiore al 10% del valore della produzione.	Sanzione amministrativa di natura pecuniaria.	Danno d'immagine con esposizione mediatica regionale e temporalmente rilevante (4-5 giorni)	La violazione degli SLA contrattualizzati comporta la perdita del servizio.	I dati gestiti sono oggetto di transazioni economiche, finanziarie o sanitarie. La mancanza di integrità dei dati ha elevati impatti sulle attività operative (fino a 1 FTE).	L'indisponibilità dei dati oltre agli SLA e ai tempi di RTO e RPO definiti contrattualmente può comportare interruzioni a servizi pubblici essenziali.	I dati sono di tipo particolare e l'eventuale diffusione a terzi può compromettere significativamente il business e i diritti degli interessati.
2	Medio	Impatto economico superiore al 1% e inferiore al 5% del valore della produzione.	Contezioso in sede civile per violazione di termini contrattuali o dovuto ad altre forme di risarcimento del danno.	Danno d'immagine con esposizione mediatica locale (provincia) e temporalmente limitata (2-3 giorni).	La violazione degli SLA contrattualizzati comporta l'applicazione di penali.	I dati gestiti non fanno parte di transazioni economiche, finanziarie o sanitarie. La mancanza di integrità dei dati ha elevati impatti sulle attività operative (tra 0,1 e 0,5 FTE).	L'indisponibilità dei dati oltre agli SLA e ai tempi di RTO e RPO definiti contrattualmente può comportare interruzioni a servizi pubblici non essenziali.	I dati sono di tipo personale e l'eventuale diffusione a terzi può compromettere il business e i diritti degli interessati.
1	Basso	Impatto economico inferiore al 1% del valore della produzione.	Violazione di norma volontaria, policy e procedure interne.	Danno d'immagine moderato o a diffusione interna.	Nessuno SLA definito, ovvero non vi sono penali in caso di violazione degli SLA contrattualizzati.	I dati gestiti non fanno parte di transazioni economiche, finanziarie o sanitarie. La mancanza di integrità dei dati non ha elevati impatti sulle attività operative (< 0,1 FTE).	L'indisponibilità dei dati oltre agli SLA e ai tempi di RTO e RPO definiti contrattualmente può comportare contestazioni da parte dei soggetti interessati.	I dati sono di natura interna e l'eventuale diffusione a terzi non ha significativi impatti sul business e sui diritti degli interessati.

Valutazione probabilità o verosimiglianza | criteri

Probabilità/verosimiglianza	Livello	Criterio connesso alla possibilità	Criterio probabilistico	Serie storiche
4	Quasi certo	E' quasi certo che l'evento possa verificarsi nei prossimi 5 anni e la probabilità è così alta che potrebbe verificarsi già entro il prossimo anno (es. furto nei supermercati; attacco cyber ad aziende con dati ritenuti di valore).	Probabilità > 60% nei prossimi 5 anni	L'evento si è verificato oltre le 5 volte negli ultimi 5 anni o più di 2 volte nell'ultimo anno.
3	Probabile	E' probabile il verificarsi dell'evento nei prossimi 5 anni e l'occorrere di tale evento è prevedibile secondo le fonti di informazione disponibili (es. aumento dei costi dell'energia a fronte di conflitti in determinate aree del mondo)	30% < Prob < 60% nei prossimi 5 anni	L'evento si è verifiato da 4 a 5 volte negli ultimi 5 anni.
2	Possibile	E' possibile il verificarsi dell'evento nei prossimi 5 anni e l'occorrere di tale evento non susciterebbe sorpresa (es. terremoto in aree considerate significativamente sismiche)	10% < Prob < 30% nei prossimi 5 anni	L'evento si è verificato da 2 a 3 volte negli ultimi 5 anni
1	Improbabile	E' improbabile che possa verificarsi, se non in condizioni straordinarie ad oggi imprevedibili (es. alluvione in sito lontano da corsi d'acqua)	0% < Prob <10% nei prossimi 5 anni	L'evento si è verificato non più di 1 volta negli ultimi 5 anni.

Valutazione presidi | criteri

Efficacia delle misure		Range medio di mitigazione	Coefficiente di mitigazione	Criterio
Molto efficace (strutturato)	**4**	3,5 - 4	0,9	La misura si dimostra di assoluta e comprovata efficacia, tale da ridurre in maniera consistente e definitiva la minaccia. Tale risultato può essere desunto in virtù di incident occorsi, nell'adozione di tale misura, all'ente o a realtà terze in virtù di dati storici, oppure in ragione di valutazioni empiriche.
Efficace (Definito)	**3**	2,5 - 3,49	0,75	La misura si dimostra efficace e capace di ridurre in maniera significativa la minaccia, seppur in maniera non del tutto risolutiva. Tale risultato può essere desunto in virtù di incident occorsi, nell'adozione di tale misura, all'ente o a realtà terze in virtù di dati storici, oppure in ragione di valutazioni empiriche.
Parzialmente efficace (Basato su prassi)	**2**	2,0 - 2,49	0,5	La misura dimostra un certo grado di efficacia ma non tale da garantire un presidio puntuale della minaccia, la quale continua a presentare punti di significativa vulnerabilità. Tale risultato può essere desunto in virtù di incident occorsi, nell'adozione di tale misura, all'ente o a realtà terze in virtù di dati storici, oppure in ragione di valutazioni empiriche.
Poco efficace (Iniziale)	**1**	1,0 - 1,99	0,25	La misura si è dimostrata poco efficace a contenere la minaccia, o la sua efficacia non è dimostrata / dimostrabile sulla base dei dati storici e/o per via empirica o dovuta all'applicazione in contesti simili, anche presso realtà terze. La misura è stata adottata ma

Ponderazione QUALITATIVA del rischio

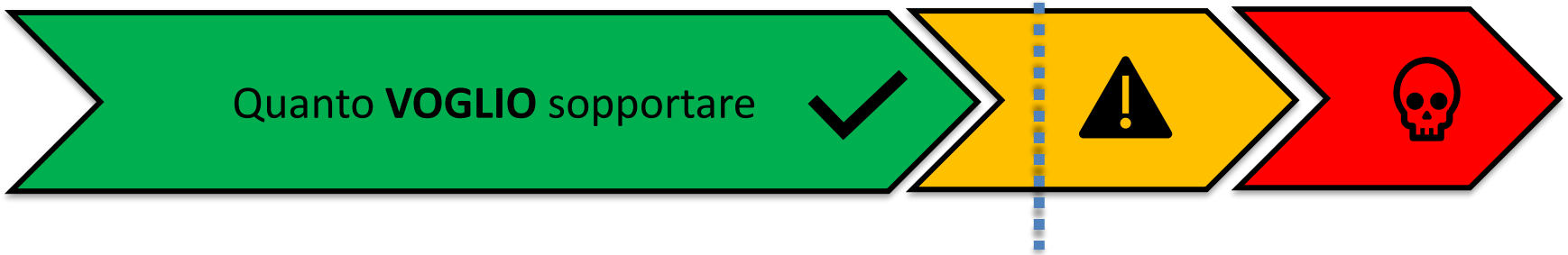
Confrontare il risultato…

	Basso: 1	Medio: 2	Alto: 3	Critico: 4
Raro: 1	1	2	3	4
Improbabile: 2	2	4	6	8
Probabile: 3	3	6	9	12
Quasi certo: 4	4	8	12	16

6 = oltre la soglia di accettazione (risk appetite) ma entro la soglia di tolleranza (risk tolerance)

… con le soglie di accettabilità definite

PROFILO DI RISCHIO



Risk Appetite Framework

Definisce le priorità di trattamento del rischio

Probabilità/Impatto	Basso: 1	Medio: 2	Alto: 3	Critico: 4
Raro: 1	Risk Acceptance	Risk Acceptance	Risk Tolerance	Risk Capacity
Improbabile: 2	Risk Acceptance	Risk Tolerance	Risk Tolerance	Risk Capacity
Probabile: 3	Risk Acceptance	Risk Tolerance	Risk Capacity	Out of risk
Quasi certo: 4	Risk Acceptance	Risk Capacity	Out of risk	Very critical

Priorità	livello di rischio	Azioni di controllo
1	Very critical	da implementare entro 1 mese
2	Out of risk	da implementare entro 6 mese
3	Risk Capacity	da implementare entro 1 anno
4	Risk Tolerance	da implementare entro 3 anni
5	Risk Acceptance	non richieste

Ponderazione QUANTITATIVA del rischio

Costo Totale del rischio (€)

Costi diretti delle perdite

+

Costi indiretti delle perdite

+

Costi per la protezione

+

Costi per la prevenzione

+

Costi per il trasferimento

ATTENZIONE

Il trasferimento non deve essere la prima opzione di trattamento del rischio. Le assicurazioni non coprono tutti i costi… e costano.

Trasferisco solo ciò che non posso / voglio / mi conviene mitigare.

Mitigare il rischio = Riduzione del premio assicurativo!

… confronto con le soglie di accettabilità definite (€)

Decidere le misure di trattamento

- [**ACCEPT**] Ritenuto, ovvero il suo impatto considerato sopportabile (risk capacity)
- [**AVOID**] Evitato, eliminando la causa, ad esempio rinunciando all'obiettivo connesso
- [**MITIGATE**] Mitigato, attraverso un'azione di trattamento che vada a ridurre la probabilità, agendo in prevenzione del danno o l'impatto, agendo in contenimento del danno
- [**TRANSFER**] Trasferito a terzi, ad esempio ad un fornitore o ad una compagnia assicurativa

Monitoraggio, miglioramento e revisione

Essenziali per:

- valutare la corretta applicazione delle misure e dei controlli
- rilevare gli scostamenti rispetto ai piani previsti
- supportare le decisioni
- garantire efficacia e miglioramento continuo
- recepire le variazioni del contesto e delle minacce
- mantenere la coerenza dei controlli nel tempo, al mutare del contesto

Fonti di informazione:

- Analisi degli incident e degli eventi
- Key performance indicator
- Key risk indicator
- Audit e Riesami

Concetti base di Continuità Operativa

Business Continuity Management System (BCMS)

BCM

Business Continuity Management

E’ un processo gestionale che:

- permette di identificare le possibili minacce per l’organizzazione e gli impatti che avrebbero su di essa se si verificassero;
- permette di creare una strategia organizzativa volta alla sopravvivenza dell’organizzazione in caso di evento sfavorevole;
- salvaguarda gli interessi degli stakeholders dell’organizzazione fornendo una maggiore sicurezza di continuità operativa.

Obiettivo: la Resilienza Operativa

BCMS

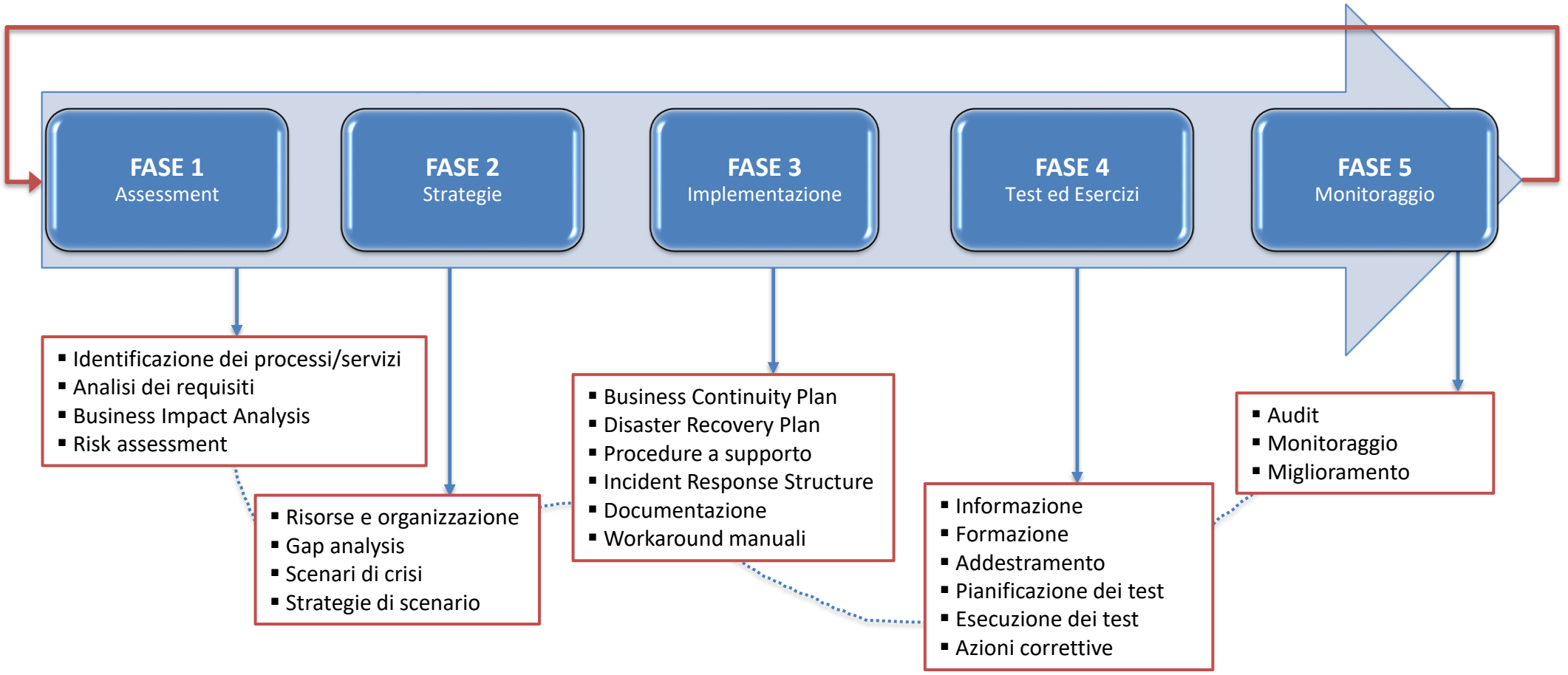
Business Continuity Management System

E’ il sistema di gestione generale dell’organizzazione incentrato sulla continuità operativa.

Propone di:

- ✓ stabilire, implementare, controllare e migliorare continuamente il BCM;
- ✓ garantire il rispetto delle policy di continuità operativa dichiarate dall’organizzazione;
- ✓ dimostrare conformità ai terzi;
- ✓ ottenere una certificazione/registrazione del proprio BCMS da un ente certificatore terzo
- ✓ redigere un’auto-dichiarazione di conformità nel rispetto dell’ISO di riferimento.

BC nella ISO 22301: Processo iterativo




Coffee
Time!

Applicazione della NIS 2 in pratica

Complessità

- ✓ Impatta sui processi aziendali (esistenti e ne necessita di nuovi)
- ✓ Impatta sulle responsabilità aziendali e sull'organizzazione
- ✓ Impatta sui comportamenti dei singoli (a tutti i livelli)
- ✓ Impatta economicamente su misure organizzative e tecnologiche
- ✓ Impatta sulla gestione dei fornitori

Il progetto

L’applicazione deve essere affrontata come un progetto estremamente complesso.

Questo implica che siano definiti e formalizzati:

- Sponsor del vertice aziendale
- Obiettivi chiari
- Ruoli chiari
- Risorse e Budget
- Metodologia rigorosa
- Corretto passaggio in esercizio

CISO – DPO – RISK Man– CO - ORGANIZZAZIONE – FORMAZIONE - ACQUISTI - LEGAL & CONTRATTI - Linee di PRODUZIONE – INFRASTRUTTURE…

Le fasi

L’attuazione richiede in sintesi una serie di passi operativi:

- «Commitment» aziendale
- Definizione di un team
- Analisi del perimetro
- Definizione di un piano di progetto
- Attuazione dei sotto-progetti
- Verifica tenuta del sistema
- Monitoraggio periodico

Individuare il team corretto

Il Team NIS 2:

- CISO
- DPO
- *RISK Manager*
- ORGANIZZAZIONE
- FORMAZIONE
- ACQUISTI
- LEGAL & CONTRATTI
- *Linee di PRODUZIONE*
- SI-INFRASTRUTTURE…

Due figure chiave per il TOP Management

Punto di contatto

Il **Punto di contatto NIS 2** è l'interlocutore ufficiale con l'ACN. Cura registrazione, aggiornamento dati e dichiarazione NIS sulla piattaforma, gestisce comunicazioni e deleghe, coordina il flusso informativo interno e supporta l'attuazione degli obblighi. Raccoglie dati tecnici (IP, domini, servizi), coinvolge sostituto e utenti di supporto e informa i vertici, che mantengono la responsabilità ultima.

Referente CSIRT

Il **Referente CSIRT** è la figura incaricata di coordinare le comunicazioni operative con CSIRT Italia in caso di incidente informatico. Raccoglie e valida le evidenze tecniche, predispone e aggiorna le notifiche, presidia eventuali richieste di integrazione e coordina le attività di analisi, contenimento e ripristino con team interni e fornitori. Assicura inoltre il flusso informativo verso Punto di contatto NIS 2 e vertici aziendali, mantenendo tracciabilità di decisioni e azioni intraprese.

Identikit del Responsabile Cybersecurity(CISO) responsabilità e attività

La figura responsabile della sicurezza informatica riporta al senior management aziendale e solitamente si occupa di:

- Definire, verificare, sviluppare e comunicare la **visione e la strategia di cybersecurity aziendale**, ivi comprese le policy e le procedure, in accordo con la normativa cogente
- Implementare programmi per la protezione del patrimonio informativo, comprese le azioni di **risposta a possibili incidenti o attacchi** agli archivi informativi aziendali;
- Disegnare e attuare processi per **mitigare i rischi correlati all'adozione delle tecnologie digitali**;
- Gestire il **flusso informativo verso le autorità**, in merito ad eventuali obblighi in ambito cybersecurity;
- Sviluppare iniziative di awareness e formazione per **promuovere e sviluppare una cultura aziendale** consapevole degli aspetti di cybersecurity;
- **Dialogare** ad intervalli regolari sia con il top-management sia con il servizio IT, Amministrazione e Controllo, Ricerca & Sviluppo, Responsabili delle varie Unità operative;
- Definire, in accordo con i vertici aziendali, il **budget in ambito cybersecurity** e monitorare l'utilizzo delle risorse
- Suggerire **policies e soluzioni** ai manager dell'organizzazione

Altra figura chiave: il DPO

Un addendum ai compiti del DPO

Nel caso in cui i titolari del trattamento si trovino a dover applicare la NIS2 ai compiti esplicitamente citati ed assegnati ai DPO dall'articolo 39 del GDPR, si dovrebbero aggiungere anche quelli riportati a seguire:

- Valutazione degli adempimenti richiesti dalla NIS2 che **impattano sulla compliance al GDPR**;
- Valutazione degli adempimenti richiesti dal GDPR già implementati e che già soddisfano i requisiti della NIS2;
- **Promozione dell'equilibrio fra sicurezza IT e protezione dei dati personali**, mediante il bilanciamento fra le esigenze di sicurezza d'impresa e di tutela dei diritti delle persone;
- Consulenza nella definizione delle politiche in materia di cybersicurezza integrate con le procedure in materia di protezione dei dati personali;
- Coinvolgimento nella fase di **realizzazione della valutazione dei rischi** cibernetici;
- Coinvolgimento nella fase di implementazione, di **revisione e controllo periodico delle misure** tecniche, operative e organizzative adeguate alla gestione dei rischi;
- Collaborazione alla diffusione di prassi in materia di cybersecurity attraverso l'attività di formazione al personale.

Il Modello Organizzativo Cyber: Le Misure specifiche per gi Organi Direttivi e Amministrativi

Documenti da approvare da parte dei CDA

Agenzia per la Cybersicurezza Nazionale

Appendice C – documenti approvati dagli organi di amministrazione e direttivi

La seguente tabella elenca i documenti che devono essere approvati dagli organi di amministrazione e direttivi e i riferimenti ai requisiti che ne richiedono l'approvazione.

Documento	Riferimento requisito
Organizzazione per la sicurezza informatica.	GV.RR-02 punto 1.
Politiche di sicurezza informatica.	GV.PO-01 punto 1.
Valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete.	ID.RA-05 punto 3.
Piano di trattamento del rischio.	ID.RA-06 punto 3.
Piano di gestione delle vulnerabilità.	ID.RA-08 punto 4.
Piano di adeguamento.	ID.IM-01 punto 1.
Piano di continuità operativa.	ID.IM-04 punto 1.
Piano di ripristino in caso di disastro.	ID.IM-04 punto 1.
Piano di gestione delle crisi.	ID.IM-04 punto 1.
Piano di formazione.	PR.AT-01 punto 1.
Piano per la gestione degli incidenti di sicurezza informatica.	RS.MA-01 punto 2.

ESEMPIO DI PIANIFICAZIONE

GV: La politica per la gestione del rischio di cybersecurity è stabilita in base al contesto organizzativo, alla strategia di cybersecurity e alle priorità, ed è comunicata e applicata.

GV.OC-04	È mantenuto un elenco aggiornato dei sistemi informativi e di rete rilevanti.
GV.RR-02	È definita, approvata **dagli organi di amministrazione e direttivi**, e resa nota alle articolazioni competenti del soggetto NIS, l'organizzazione per la sicurezza informatica e ne sono stabiliti ruoli e responsabilità.

GV: La politica per la gestione del rischio di cybersecurity è stabilita in base al contesto organizzativo, alla strategia di cybersecurity e alle priorità, ed è comunicata e applicata.

2

GV.PO-01

Sono adottate e documentate politiche di sicurezza informatica per almeno i seguenti ambiti:

a) gestione del rischio;
b) ruoli e responsabilità;
c) affidabilità delle risorse umane;
d) conformità e audit di sicurezza;
e) gestione dei rischi per la sicurezza informatica della catena di approvvigionamento;
f) gestione degli asset;
g) gestione delle vulnerabilità;
h) continuità operativa, ripristino in caso di disastro e gestione delle crisi;
i) gestione dell'autenticazione, delle identità digitali e del controllo accessi;
j) sicurezza fisica;
k) formazione del personale e consapevolezza;
l) sicurezza dei dati;
m) sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete;
n) protezione delle reti e delle comunicazioni;
o) monitoraggio degli eventi di sicurezza;
p) risposta agli incidenti e ripristino.

Le politiche di cui al punto 1 sono approvate **dagli organi di amministrazione e direttivi.**

ID.RA: Le risposte al rischio sono scelte, prioritizzate, pianificate, monitorate e comunicate.

3

ID.RA-06

È definito, documentato, eseguito e monitorato **un piano di trattamento del rischio** che comprende almeno:

a) le opzioni di trattamento e le misure da attuare in merito al trattamento di ciascun rischio individuato e le relative priorità;

b) le articolazioni competenti per l'attuazione delle misure di trattamento dei rischi e le tempistiche per tale attuazione;

c) la descrizione e le ragioni che giustificano l'accettazione di eventuali rischi residui al trattamento.

Il piano di cui al punto 1, ivi compresa l’accettazione di eventuali rischi residui, è approvato **dagli organi di amministrazione e direttivi.**

ID.RA Sono stabiliti processi per la ricezione, l'analisi e la risposta alle divulgazioni di vulnerabilità.

ID.RA-08

È definito, attuato, aggiornato e documentato **un piano di gestione delle vulnerabilità** che comprende almeno:

a) le modalità per l'identificazione delle vulnerabilità di cui alla misura ID.RA-01 e la relativa pianificazione delle attività;

b) le modalità per monitorare, ricevere, analizzare e rispondere alle informazioni sulle vulnerabilità;

c) le procedure, i ruoli, le responsabilità per lo svolgimento delle attività di cui alle lettere a) e b).

Il piano di cui al punto sopra è approvato **dagli organi di amministrazione e direttivi.**

ID.IM: Sono identificati miglioramenti in esito alle valutazioni.

5

1 In accordo agli esiti del riesame di cui al punto 1 della misura GV.PO-02, è definito, attuato, documentato e approvato **dagli organi di amministrazioni e direttivi** un **piano di adeguamento che identifichi gli interventi necessari ad assicurare l'attuazione delle politiche di sicurezza**.

ID.IM-01

2 Gli organi di amministrazione e direttivi sono informati mediante apposite relazioni periodiche sugli esiti dei piani di cui al punto 1.

3 È definito, attuato, aggiornato e documentato un **piano per la valutazione dell'efficacia delle misure di gestione** del rischio per la sicurezza informatica che comprenda l'indicazione delle misure da valutare e i relativi metodi di valutazione.

4 Gli organi **di amministrazione e direttivi sono informati** mediante apposite relazioni periodiche sul piano di valutazione dell'efficacia di cui al punto 3.

ID.IM I piani di risposta agli incidenti e gli altri piani di cybersecurity che impattano le operazioni sono stabiliti, comunicati, mantenuti e migliorati.

6

ID.IM-04

1 Per almeno **i sistemi informativi e di rete rilevanti** è definito, attuato, aggiornato e documentato **un piano di continuità operativa**, che comprende almeno:

a) le finalità e l'ambito di applicazione;
b) i ruoli e le responsabilità;
c) i contatti principali e i canali di comunicazione (interni ed esterni);
d) le condizioni per l'attivazione e la disattivazione del piano;
e) le risorse necessarie, ivi compresi i backup e le ridondanze.

2 Per almeno **i sistemi informativi e di rete rilevanti è definito**, attuato, aggiornato e documentato un **piano di ripristino** in caso di disastro, che comprende almeno:

a) le finalità e l'ambito di applicazione;
b) i ruoli e le responsabilità;
c) i contatti principali e i canali di comunicazione (interni ed esterni);
d) le condizioni per l'attivazione e la disattivazione del piano;
e) le risorse necessarie, ivi compresi i backup e le ridondanze;
f) l'ordine di ripristino delle operazioni;
g) le procedure di ripristino per operazioni specifiche, compresi gli obiettivi di ripristino.

ID.IM I piani di risposta agli incidenti e gli altri piani di cybersecurity che impattano le operazioni sono stabiliti, comunicati, mantenuti e migliorati.

Per almeno i sistemi informativi e di rete rilevanti è definito, attuato, aggiornato e documentato **un piano per la gestione delle crisi** che comprende almeno:

ID.IM-04

3 a) i ruoli e responsabilità del personale e, se opportuno, dei fornitori, specificando l'assegnazione dei ruoli in situazioni di crisi, comprese le procedure specifiche da seguire;
b) le modalità di comunicazione tra i soggetti e le autorità competenti.

4 I piani di cui ai punti 1, 2 e 3 sono approvati **dagli organi di amministrazione e direttivi.**

5 I piani di cui ai punti 1, 2 e 3 sono riesaminati e, se opportuno, aggiornati periodicamente e comunque almeno ogni due anni, nonché qualora si verifichino incidenti significativi o mutamenti dell'esposizione alle minacce e ai relativi rischi.

PR.AT: Il personale è sensibilizzato e formato in modo da possedere le conoscenze e le competenze per svolgere compiti di carattere generale tenendo conto dei rischi di cybersecurity.

7

È definito, attuato, aggiornato e documentato un piano di formazione in materia di sicurezza informatica del personale, ivi inclusi gli organi di amministrazione e direttivi, che comprende almeno:

PR.AT

1 a) la pianificazione delle attività di formazione previste con l'indicazione dei contenuti della formazione fornita;
b) le eventuali modalità di verifica dell'acquisizione dei contenuti.

2 Il piano di formazione di cui al punto 1 è approvato dagli organi di amministrazione e direttivi.

3 È mantenuto un registro aggiornato recante l'elenco dei dipendenti che hanno ricevuto la formazione di cui al punto 1, i relativi contenuti e l'elenco delle verifiche svolte laddove previste.

RS.MA: Il piano di risposta agli incidenti è eseguito in coordinamento con le terze parti interessate una volta dichiarato un incidente.

8

È definito, attuato, aggiornato e documentato un **piano per la gestione degli incidenti** di sicurezza informatica e la notifica al CSIRT Italia, in accordo a quanto previsto dall'articolo 25 del decreto NIS, che comprende almeno:

RS.MA

1 a) le fasi e le procedure di gestione e notifica degli incidenti con l'indicazione dei relativi ruoli e delle responsabilità;
b) le procedure per la predisposizione e la trasmissione delle relazioni di cui all'articolo 25, comma 5, lettere c), d) ed e) del decreto NIS;
c) le informazioni di contatto per la segnalazione degli incidenti;
d) le modalità di comunicazione interna, anche con riguardo al coinvolgimento degli organi di amministrazione e direttivi, ed esterna;
e) la reportistica da utilizzare per la documentazione dell'incidente.

2 Il piano di cui al punto 1 è approvato dagli **organi di amministrazione e direttivi.**

3 Il piano di cui al punto 1 è riesaminato e, se opportuno, aggiornato periodicamente e comunque almeno ogni due anni, nonché qualora si verifichino incidenti significativi, integrando le relative lezioni apprese, o mutamenti dell'esposizione alle minacce e ai relativi rischi.

Verso un piano cyber

Politiche di cybersecurity

1.4.1. **GV.PO-01**: La politica per la gestione del rischio di cybersecurity è stabilita in base al contesto organizzativo, alla strategia di cybersecurity e alle priorità, ed è comunicata e applicata.

1. Sono adottate e documentate politiche di sicurezza informatica per almeno i seguenti ambiti:
   a) gestione del rischio;
   b) ruoli e responsabilità;
   c) affidabilità delle risorse umane;
   d) conformità e audit di sicurezza;
   e) gestione dei rischi per la sicurezza informatica della catena di approvvigionamento;
   f) gestione degli asset;
   g) gestione delle vulnerabilità;
   h) continuità operativa, ripristino in caso di disastro e gestione delle crisi;
   i) gestione dell'autenticazione, delle identità digitali e del controllo accessi;
   j) sicurezza fisica;
   k) formazione del personale e consapevolezza;
   l) sicurezza dei dati;
   m) sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete;
   n) protezione delle reti e delle comunicazioni;
   o) monitoraggio degli eventi di sicurezza;
   p) risposta agli incidenti e ripristino.
2. Per gli ambiti di cui al punto 1 sono incluse almeno le politiche in relazione ai requisiti indicati nella tabella 1 in appendice al presente allegato.
3. Le politiche di cui al punto 1 sono approvate dagli organi di amministrazione e direttivi.

3.3.3. **PR.DS-11**: I backup dei dati sono creati, protetti, mantenuti e verificati.

1. In accordo alle esigenze di continuità operativa e di ripristino in caso di disastro individuate nei piani di cui alla misura ID.IM-04, sono effettuati periodicamente i backup dei dati e delle configurazioni e, per almeno i sistemi informativi e di rete rilevanti, sono anche conservate copie di backup offline.
2. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.

Politiche di cybersecurity

Tabella 1: Requisiti di cui al punto 2 della misura GV.PO-01.

Ambiti Politiche	Requisiti
a) Gestione del rischio.	GV.OC-04: punto 1. GV.RM-03: punto 1. ID.RA-05: punti 1, 2 e 3. ID.RA-06: punti 1, 2 e 3.
b) Ruoli e responsabilità.	GV.RR-02: punti 1, 2, 3 e 4.
c) Affidabilità delle risorse umane.	GV.RR-04: punti 1 e 2.
d) Conformità e audit di sicurezza.	GV.PO-01: punti 1, 2 e 3. GV.PO-02: punti 1 e 2. ID.IM-01: punti 1 e 2.
e) Gestione dei rischi per la sicurezza informatica della catena di approvvigionamento.	GV.SC-01: punto 1. GV.SC-02: punto 1. GV.SC-04: punto 1. GV.SC-05: punto 1. GV.SC-07: punti 1 e 2.
f) Gestione degli asset.	ID.AM-01: punto 1. ID.AM-02: punto 1. ID.AM-04: punto 1.
g) Gestione delle vulnerabilità.	ID.RA-01: punto 1. ID.RA-08: punti 1, 2, 3 e 4.
h) Continuità operativa, ripristino in caso di disastro e gestione delle crisi.	ID.IM-04: punti 1, 2, 3, 4 e 5.
i) Gestione dell'autenticazione, delle identità digitali e del controllo accessi.	PR.AA-01: punti 1, 2 e 3. PR.AA-03: punti 1 e 2. PR.AA-05: punti 1 e 2. PR.IR-01: punti 1 e 2.
j) Sicurezza fisica	PR.AA-06: punto 1.
k) Formazione del personale e consapevolezza.	PR.AT-01: punti 1, 2 e 3.
l) Sicurezza dei dati.	PR.DS-01: punti 1 e 2. PR.DS-02: punto 1. PR.DS-11: punto 1.
m) Sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete.	PR.PS-02: punti 1, 2. PR.PS-04: punti 1, 2 e 3. PR.PS-06: punto 1.
n) Protezione delle reti e delle comunicazioni.	PR.IR-01: punto 3.
o) Monitoraggio degli eventi di sicurezza.	DE.CM-01: punti 1 e 2. DE.CM-09: punto 1.
p) Risposta agli incidenti e ripristino.	RS.MA-01: punti 1, 2 e 3. RS.CO-02: punti 1 e 2. RC.RP-01: punto 1.

La Direttiva NIS2 – Focus Catena di Fornitura D.LGS 138/2024

- **Valutazione e gestione del rischio nella catena di fornitura:** Le organizzazioni devono effettuare una valutazione approfondita dei rischi associati ai loro fornitori e subappaltatori. Questo implica l'analisi delle vulnerabilità specifiche che possono derivare dai rapporti con terze parti e l'adozione di misure adeguate per mitigare tali rischi.

- **Integrazione della sicurezza nei contratti con i fornitori**: È obbligatorio includere clausole contrattuali che impongano ai fornitori il rispetto di determinati standard di sicurezza informatica. Questo assicura che i fornitori adottino misure di sicurezza coerenti con quelle dell'organizzazione principale, garantendo una protezione uniforme lungo tutta la catena di approvvigionamento.

La Direttiva NIS2 – Focus Catena di Fornitura D.LGS 138/2024

- **Monitoraggio continuo e audit dei fornitori:** Le organizzazioni devono implementare processi per monitorare continuamente le pratiche di sicurezza dei loro fornitori. Questo può includere audit periodici e la richiesta di reportistica regolare per assicurarsi che i fornitori mantengano elevati standard di cybersecurity.

- **Piani di continuità operativa e gestione delle crisi:** È fondamentale che le organizzazioni sviluppino e mantengano piani di continuità operativa che considerino potenziali interruzioni derivanti dalla catena di fornitura. Questi piani devono includere procedure per il backup dei dati, il ripristino in caso di emergenza e la gestione delle crisi, garantendo la resilienza dell'intera filiera.

Acquisti: DPCM n. 102 del 5 maggio 2025

Regola l’acquisizione di beni e servizi informatici da parte delle pubbliche amministrazioni e degli enti pubblici, con particolare focus su quelli utilizzati **in ambiti sensibili per la sicurezza nazionale.**

L’obiettivo è garantire che tali acquisizioni rispettino elevati standard di sicurezza informatica, riducendo i rischi legati a vulnerabilità e minacce cibernetiche.

Acquisti: DPCM n. 102 del 5 maggio 2025

Principali elementi che disciplina il Decreto:

- ✓ gli **elementi essenziali di cybersicurezza** dei beni e dei servizi informatici (allegato 1), distinti fra:
  - requisiti relativi alle **proprietà** dei beni e dei servizi informatici
  - requisiti di **gestione delle vulnerabilità**

- ✓ le **specifiche categorie tecnologiche di beni e servizi informatici** per cui sono necessari elementi di cybersicurezza (allegato 2)

- ✓ i casi in cui, per la tutela della sicurezza nazionale, devono essere previsti **criteri di premialità** per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'UE o di Paesi aderenti all'Alleanza atlantica (NATO) o di Paesi terzi

- ✓ l'e**lenco dei paesi terzi** tra quelli che sono parte di accordi di collaborazione sia con l'UE, sia con la NATO, in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione (allegato 3).

La gestione degli incidenti

La Direttiva NIS2 – Focus Obblighi di base D.LGS 138/2024

Art. 25 – Obblighi in materia di notifica di incidente

I soggetti essenziali e i soggetti importanti devono notificare, senza ingiustificato ritardo, allo CSIRT **ogni incidente che ha un impatto significativo sulla fornitura dei loro servizi**.

- senza ingiustificato ritardo, e comunque **entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo**, una **pre-notifica** che, ove possibile, indichi se l'incidente significativo possa ritenersi il risultato di atti illegittimi o malevoli oppure possa avere un impatto transfrontaliero;

- senza ingiustificato ritardo, e comunque **entro 72 ore** (24 ore nel caso di un prestatore di servizi fiduciari) **da quando sono venuti a conoscenza dell'incidente significativo**, **una notifica dell'incidente** che, ove possibile, aggiorni le informazioni già trasmesse nella pre-notifica e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione;

- una **relazione finale entro un mese** dalla trasmissione della notifica di incidente.

La Direttiva NIS2 – Focus Obblighi di base D.LGS 138/2024

IS-1	Il soggetto NIS ha evidenza della perdita di riservatezza, verso l'esterno, di dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.
IS-2	Il soggetto NIS ha evidenza della perdita di integrità, con impatto verso l'esterno, di dati di sua proprietà o sui quali esercita il controllo, anche parziale.
IS-3	Il soggetto NIS ha evidenza della violazione dei livelli di servizio attesi dei suoi servizi e/o delle sue attività, sulla base dei livelli di servizio atteso (SL) definiti ai sensi della misura DE.CM-01.
IS-4	Il soggetto NIS ha evidenza, anche sulla base di parametri quali-quantitativi definiti ai sensi della misura DE.CM-01, dell'accesso, non autorizzato o con abuso dei privilegi concessi, a dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.

Soggetti importanti ed essenziali
3 tipologie di incidenti

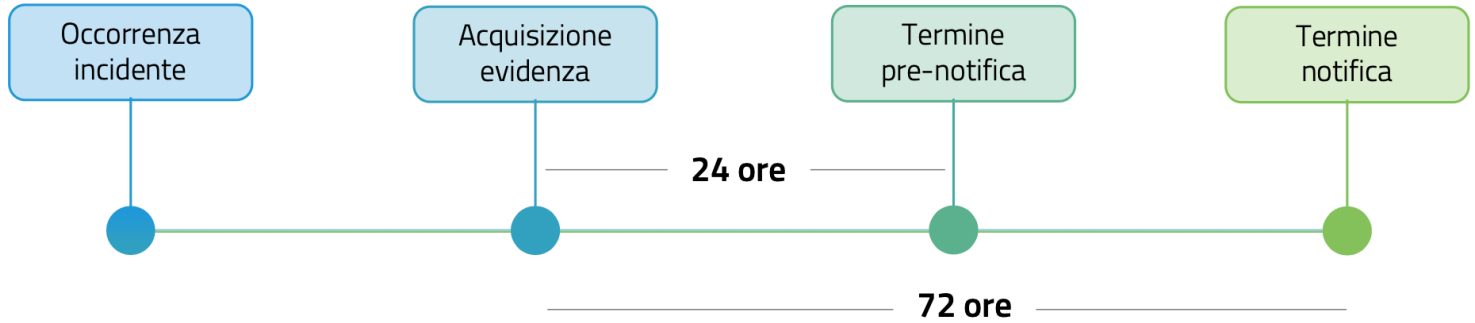
Solo soggetti essenziali
1 tipologia di incidente

La Direttiva NIS2 – Focus Obblighi di base D.LGS 138/2024

Evidenza dell'incidente

Ai fini dell'adempimento dell'obbligo di notifica degli incidenti ciò che rileva è che il soggetto abbia evidenza (In tutte le tipologie di incidente previste negli allegati è infatti riportata la dicitura "Il soggetto NIS ha evidenza …".) del verificarsi di una delle tipologie di incidente indicate.

L'acquisizione dell'evidenza definisce il momento dal quale decorre il termine per l'obbligo di notifica.



Abuso dei privilegi concessi

Fattispecie in cui un operatore abbia l'autorizzazione tecnica (ossia la disponibilità di credenziali che sono configurate per accedere ai dati) per accedere a determinati dati ma tale acceso sia effettivamente illecito in quanto, ad esempio, effettuato in violazione delle politiche del soggetto o risulti strumentale al perseguimento di scopi estranei alle necessità funzionali di accesso..

Incident Response: Supply Chain

- Le pratiche per la cybersecurity siano stabilite, seguite, mantenute e documentate **ma soprattutto condivise**
- Il personale responsabile delle attività di cybersecurity della supply chain ICT/OT **possegga le competenze e le conoscenze necessarie per svolgere i ruoli e responsabilità assegnati**
- Le **responsabilità e l'autorità** per lo svolgimento delle attività di cybersecurity della supply chain ICT/OT **siano definite ed assegnate al personale**
- **Importanti dipendenze** dai fornitori IT e OT (ovvero soggetti esterni da cui dipende l'erogazione della funzione, inclusi i partner operativi) **devono essere identificate**

Incident Response: Supply Chain

- Devono essere **noti a priori i punti di contatto** (CISO, DPO, SOC, etc..) di tutti i soggetti al fine di ridurre i tempi operativi -> **gestione del rapporto «preventiva»**
- Coinvolgere la Supply Chain in esercitazioni «table top» di **simulazioni incidenti** al fine di testare procedure e tempi di reazione
- Istituzione di un **tavolo di crisi congiunto** durante un indicente al fine di coordinare anche il corretto livello di comunicazione
- **monitorare i cambiamenti nel profilo di rischio di un fornitore,** poiché il panorama delle minacce e la superficie di attacco sono in continua evoluzione e cambiamento

DIGITALCAMPUS
guidiamo l'innovazione

CSI
your digital partner

Grazie

Sonia.schena@csi.it

pierpaolo.gruero@csi.it

enzo.veiluva@csi.it

EDIH European Digital Innovation Hubs Network

Co-funded by the European Union

Ministero delle Imprese e del Made in Italy

Finanziato dall'Unione europea NextGenerationEU

CIRCULAR HEALTH EDIH