POLIMI SCHOOL OF MANAGEMENT | osservatori.net digital innovation

Clusit Associazione Italiana per la Sicurezza Informatica

12.05.2025

Osservatorio Cybersecurity & Data Protection

NIS2, le istruzioni per l'uso:

tutto quello che c'è da sapere, e che volevate chiedere, sugli obblighi di base e le informazioni da fornire entro il 31 maggio.

L'agenda dell'incontro

09:20 Benvenuto e introduzione

Gabriele Faggioli, *Responsabile Scientifico, Osservatorio Cybersecurity & Data Protection – Presidente Onorario CLUSIT*

Giorgia Dragoni, *Ricercatrice Senior, Osservatorio Cybersecurity & Data Protection*

09:30 Interventi a cura di:

Milena Antonella Rizzi, *Capo Servizio Regolazione dell'Agenzia per la Cybersicurezza Nazionale*

Vincenzo Allia, *Vice Capo della Divisione Perimetro di Sicurezza Nazionale Cibernetica (PSNC) e discipline nazionali dell'Agenzia per la Cybersicurezza Nazionale*

10:30 Sessione di Q&A

Luca Bechelli, *Senior Advisor, Osservatorio Cybersecurity & Data Protection, CD Clusit*

Alessio Pennasilico, *Senior Advisor, Osservatorio Cybersecurity & Data Protection, CS Clusit*

11:45 Chiusura dei lavori e Cocktail

L'agenda dell'incontro

09:20 Benvenuto e introduzione

Gabriele Faggioli, *Responsabile Scientifico, Osservatorio Cybersecurity & Data Protection – Presidente Onorario CLUSIT*

Giorgia Dragoni, *Ricercatrice Senior, Osservatorio Cybersecurity & Data Protection*

09:30 Interventi a cura di:

Milena Antonella Rizzi, *Capo Servizio Regolazione dell'Agenzia per la Cybersicurezza Nazionale*

Vincenzo Allia, *Vice Capo della Divisione Perimetro di Sicurezza Nazionale Cibernetica (PSNC) e discipline nazionali dell'Agenzia per la Cybersicurezza Nazionale*

10:30 Sessione di Q&A

Luca Bechelli, *Senior Advisor, Osservatorio Cybersecurity & Data Protection, CD Clusit*

Alessio Pennasilico, *Senior Advisor, Osservatorio Cybersecurity & Data Protection, CS Clusit*

11:45 Chiusura dei lavori e Cocktail

POLIMI SCHOOL OF MANAGEMENT | osservatori.net digital innovation

Clusit Associazione Italiana per la Sicurezza Informatica

Gabriele Faggioli

Responsabile Scientifico

Giorgia Dragoni

Ricercatrice Senior

Osservatorio Cybersecurity & Data Protection

Mission e obiettivi dell'Osservatorio

Mission: Comprendere e affrontare le principali problematiche della Cybersecurity e della Data Protection e supportare, attraverso la creazione e diffusione di conoscenza, le aziende nel cogliere le opportunità della cybersecurity a difesa del proprio patrimonio informativo

RICERCA

Sviluppare una conoscenza approfondita del **mercato cybersecurity italiano e internazionale**, monitorando i percorsi di trasformazione **tecnologica e organizzativa** delle aziende e l'impatto della trasformazione digitale in temini di minacce e opportunità di cybersecurity

NETWORKING

Stimolare il **confronto pre-competitivo** tra decisori e C-Level della domanda, dell'offerta e delle istituzioni. Creare occasioni di interazione in cui **collaborare e sviluppare relazioni**

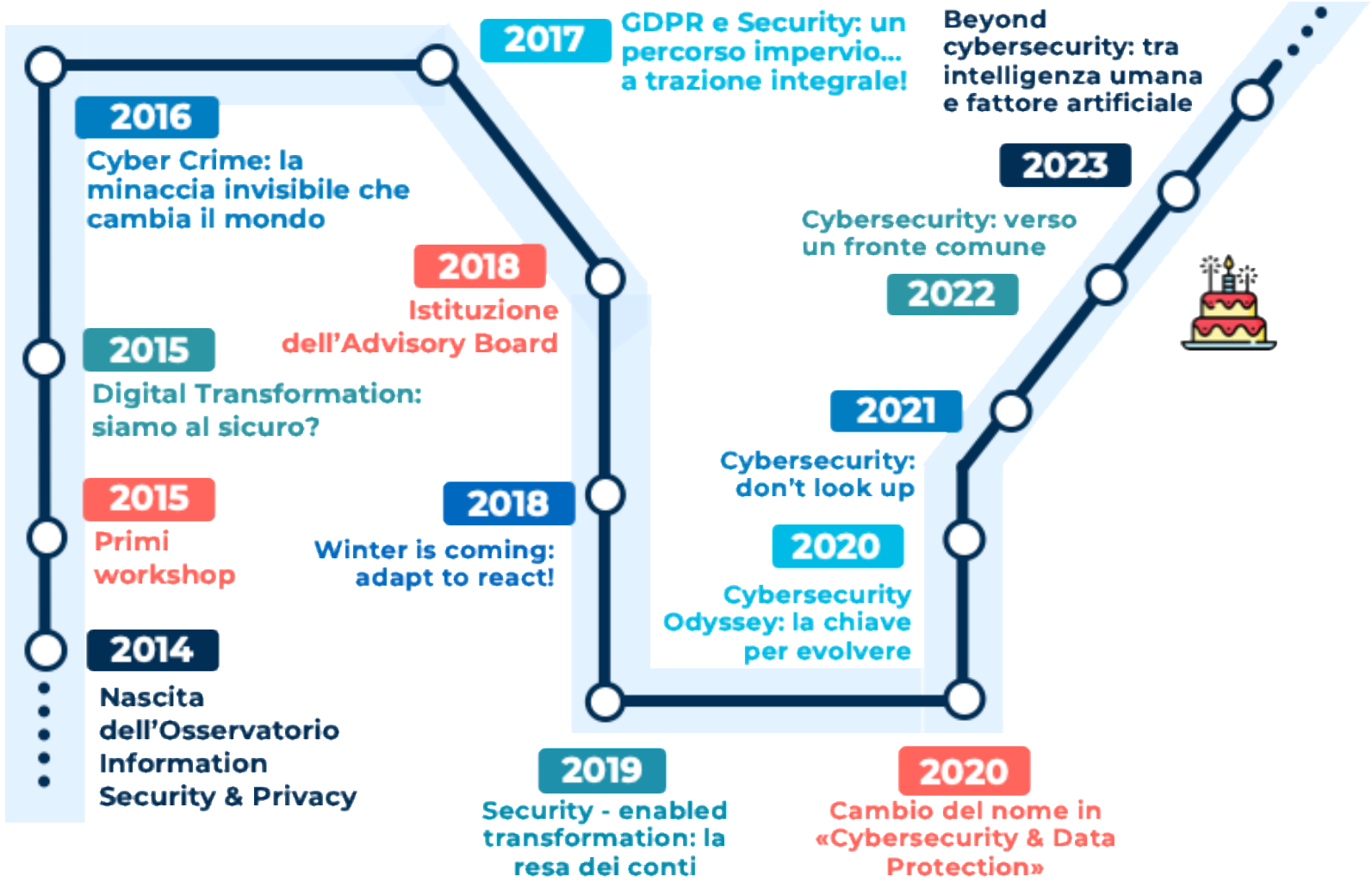
COMUNICAZIONE

Fare **chiarezza** sulle opportunità e diffondere buone pratiche, esperienze e cultura sulla cybersecurity, raggiungendo il più **ampio numero di persone** possibile

AGGIORNAMENTO

Mettere a disposizione il **know-how** unico e distintivo dell'Osservatorio tramite la produzione di output peculiari e modelli interpretativi originali

La storia dell'Osservatorio: 10 anni di attività



2024

Cyber Divide: rischio per tutti, protezione per pochi?

I 10 anni dell'Osservatorio!

Le aziende coinvolte nella Ricerca

- ***Più** di **1.000 aziende end-user coinvolte***
- ***Più di 1.300 membri attivi della community***
- ***Più** di **140 sostenitori della ricerca***

Le occasioni di confronto

- ***42 Workshop di Ricerca***
- ***9 Percorsi autorità** (dal 2020)*
- ***1** (per il momento) **Gran Galà dei CISO***
- ***9 Convegni***

Diffusione dei risultati della Ricerca

- *Articoli e citazioni su **quotidiani** e periodici cartacei e digitali (oltre **1.950 uscite stampa** su testate nazionali e specialistiche tra il 2016 e il 2024)*
- *Interviste su **Radio e Televisione***

Piano delle attività 2024

APR | MAG | GIU | ... | NOV | ... | GEN | FEB

WORKSHOP DI RICERCA

- **9 APR** — INCONTRO DI KICK-OFF DELLA RICERCA
- **28 MAG** — CLOUD SECURITY
- **24 GIU** — CISO e C-SUITE
- **27 NOV** — I RISCHI CYBER NEI MODELLI DI AI
- **21 GEN 25** — EXECUTIVE DINNER

PERCORSO AUTORITÀ

- **29 NOV** — CYBERSECURITY E NIS2: COME PREPARARSI AL NUOVO SCENARIO NORMATIVO

Online

- **27 FEB 25** — CONVEGNO FINALE

Ibrido (presenza + online)

La storia del percorso autorità

2020

Strategia Nazionale Cybersecurity e sviluppo delle tecnologie in ambito nazionale ed europeo

Con DIS, CERT-AGID e AIPSA

Tracciamento digitale e limitazione dei diritti in periodo di emergenza sanitaria

con Garante per la protezione dei Dati Personali e Commissione Europea

Scenari e aspetti programmatici della data protection in italia per presidiare al meglio il percorso della digitalizzazione

Con Garante per la protezione dei Dati Personali e Università Roma tre

2021

Il Data Protection Officer all'interno delle complessità organizzative pubbliche e private

Con associazioni di categoria in ambito data protection

GDPR e Cloud Provider: la compliance e la sicurezza dei dati

Con Garante per la protezione dei Dati Personali

2022

L'Agenzia per la Cybersicurezza Nazionale

Con Agenzia per la Cybersicurezza Nazionale

La Strategia Nazionale di Cybersicurezza

Con Agenzia per la Cybersicurezza Nazionale

2023

Il Regolamento DORA e le sfide relative alla cybersecurity nel settore finanziario: come strutturare un percorso di adeguamento efficace

Con EIOPA, UniCredit Bank Austria e Politecnico di Milano

2024

Cybersecurity e NIS2: come prepararsi al nuovo scenario normativo

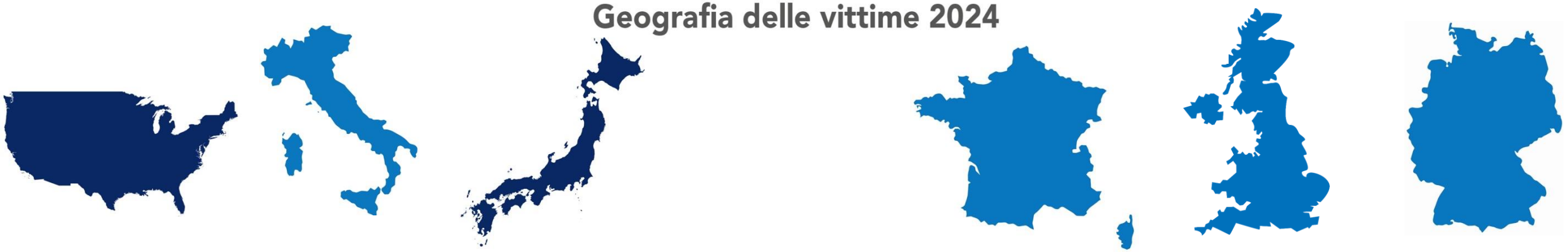
Con Agenzia per la Cybersicurezza Nazionale

Geografia delle vittime 2024

Continente Americano	USA		Italia	Continente Europeo
1.235	1.031	**Incidenti cyber**	357	1.075
29,8 miliardi US$	26,8 miliardi US$	**PIL/incidente**	6,4 miliardi US$	17,6 miliardi US$
810.000	291.000	**Popolazione/Incidenti**	140.000	650.000
0,24%	0,3%	**Spesa cyber/PIL**	0,12%	0,3%

Fonti: World Bank Group - Clusit - Osservatorio del Politecnico di Milano - Mordor Intelligence

Geografia delle vittime 2024



	USA	Italia	Giappone		Francia	UK	Germania
PIL	27.720 miliardi US$	2.300 miliardi US$	4.204 miliardi US$	PIL	3.051 miliardi US$	3.380 miliardi US$	4.525 miliardi US$
Popolazione	> 300.000.000	> 50.000.000	> 120.000.0000	Popolazione	> 65.000.000	> 65.000.000	> 80.000.000
Incidenti cyber	1.031	357	191	Incidenti cyber	128	106	98
PIL/incidente	26,8 miliardi US$	6,4 miliardi US$	22 miliardi US$	PIL/incidente	23,8 miliardi US$	31,8 miliardi US$	46,1 miliardi US$
Popolazione/Incidenti	291.000	140.000	640.000	Popolazione/Incidenti	500.000	640.000	800.000
Spesa cyber/PIL	0,3%	0,12%	0,24%	Spesa cyber/PIL	0,18%	0,31%	0,16%

Fonti: World Bank Group - Clusit - Osservatorio del Politecnico di Milano - Mordor Intelligence

L'agenda dell'incontro

09:20 Benvenuto e introduzione

Gabriele Faggioli, *Responsabile Scientifico, Osservatorio Cybersecurity & Data Protection – Presidente Onorario CLUSIT*

Giorgia Dragoni, *Ricercatrice Senior, Osservatorio Cybersecurity & Data Protection*

09:30 Interventi a cura di:

Milena Antonella Rizzi, *Capo Servizio Regolazione dell'Agenzia per la Cybersicurezza Nazionale*

Vincenzo Allia, *Vice Capo della Divisione Perimetro di Sicurezza Nazionale Cibernetica (PSNC) e discipline nazionali dell'Agenzia per la Cybersicurezza Nazionale*

10:30 Sessione di Q&A

Luca Bechelli, *Senior Advisor, Osservatorio Cybersecurity & Data Protection, CD Clusit*

Alessio Pennasilico, *Senior Advisor, Osservatorio Cybersecurity & Data Protection, CS Clusit*

11:45 Chiusura dei lavori e Cocktail

POLIMI SCHOOL OF MANAGEMENT | osservatori.net digital innovation

Clusit Associazione Italiana per la Sicurezza Informatica

Pref. Milena Antonella Rizzi

Capo Servizio Regolazione

Agenzia per la Cybersicurezza Nazionale

Vincenzo Allia

Vice Capo della Divisione Perimetro di Sicurezza Nazionale Cibernetica (PSNC) e discipline nazionali

Agenzia per la Cybersicurezza Nazionale

Nuova disciplina NIS

Specifiche di base: misure di sicurezza e incidenti.

12 maggio 2025

Modalità e specifiche di base

Art. 24

Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica

1. I soggetti essenziali e i soggetti importanti adottano misure tecniche, operative e organizzative adeguate e proporzionate, secondo le modalità e i termini di cui agli articoli 30, 31 e 32, alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi. Tali misure:

a) assicurano un livello di sicurezza dei sistemi informativi e di rete adeguato ai rischi esistenti, tenuto conto delle conoscenze più aggiornate e dello stato dell'arte in materia e, ove applicabile, delle pertinenti norme nazionali, europee e internazionali, nonché dei costi di attuazione;

b) sono proporzionate al grado di esposizione a rischi del soggetto, alle dimensioni del soggetto e alla probabilità che si verifichino incidenti, nonché alla loro gravità, compreso il loro impatto sociale ed economico.

Art. 25

Obblighi in materia di notifica di incidente

1. I soggetti essenziali e i soggetti importanti notificano, senza ingiustificato ritardo, al CSIRT Italia ogni incidente che, ai sensi del comma 4, ha un impatto significativo sulla fornitura dei loro servizi, secondo le modalità e i termini di cui agli articoli 30, 31 e 32.

Art. 31

Proporzionalità e gradualità degli obblighi

1. Ai fini di cui agli articoli 23, 24, 25, 27, 28 e 29 l'Autorità nazionale competente NIS stabilisce obblighi proporzionati tenuto debitamente conto del grado di esposizione dei soggetti ai rischi, delle dimensioni dei soggetti e della probabilità che si verifichino incidenti, nonché della loro gravità, compreso il loro impatto sociale ed economico.

Art. 40

Attuazione

5. Con una o più determinazioni dell'Agenzia per la cybersicurezza nazionale, sentito il Tavolo per l'attuazione della disciplina NIS:

l) sono stabiliti obblighi proporzionati e graduali, a valenza multisettoriale e, ove opportuno, settoriale, di cui all'articolo 31, le modalità di applicazione dei medesimi obblighi per i soggetti che svolgono attività in più settori o sottosettori e per i soggetti di cui all'articolo 32, commi 1 e 2;

Art. 42

Fase di prima applicazione

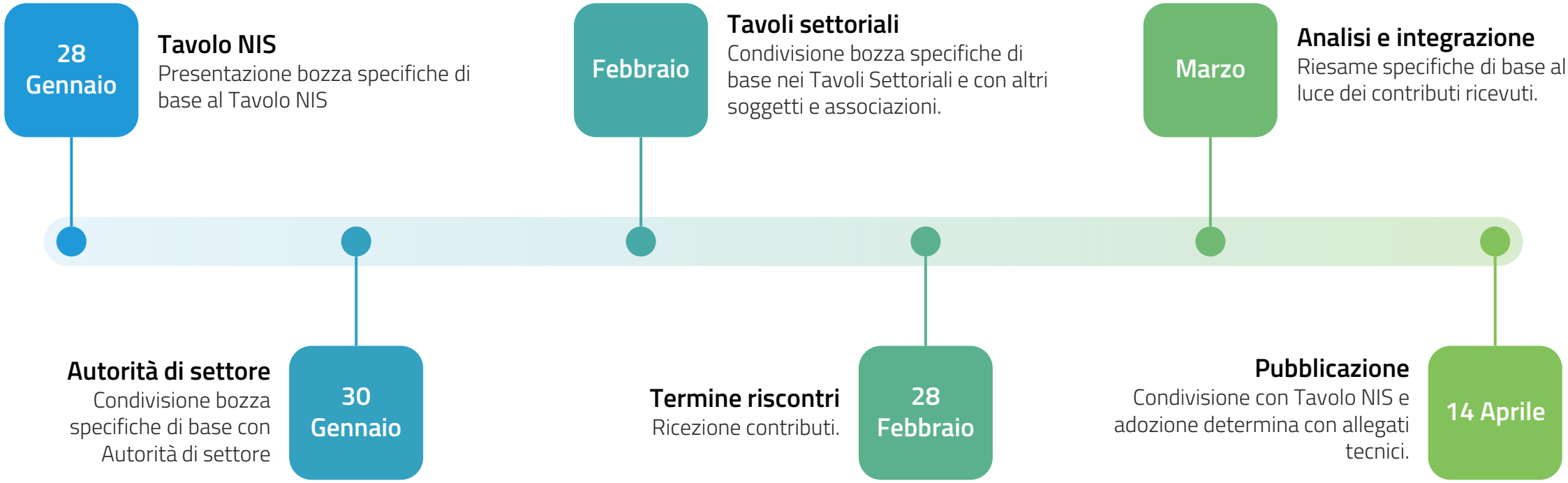
1. In fase di prima applicazione:

a) ai sensi dell'articolo 7, entro il 17 gennaio 2025, i fornitori di servizi di sistema dei nomi di dominio, i gestori di registri dei nomi di dominio di primo livello, i fornitori di servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, fornitori di servizi di data center, fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network che rientrano nell'ambito di applicazione del presente decreto, si registrano sulla piattaforma digitale di cui all'articolo 7, comma 1;

b) sino al 31 dicembre 2025, il Tavolo per l'attuazione della disciplina NIS di cui all'articolo 12 si riunisce almeno una volta ogni sessanta giorni;

c) sino al 31 dicembre 2025, il termine per l'adempimento degli obblighi di cui all'articolo 25 è fissato in nove mesi dalla ricezione della comunicazione di cui all'articolo 7, comma 3, lettere a) e b), e il termine per l'adempimento degli obblighi di cui agli articoli 23, 24 e 29 è fissato in diciotto mesi dalla medesima comunicazione. Ai fini di cui al primo periodo, l'Autorità nazionale competente NIS può stabilire modalità e specifiche di base per assicurare la conformità dei soggetti essenziali e dei soggetti importanti.

Processo di adozione



Gradualità degli obblighi

Specifiche di base

Specifiche degli obblighi, anche orizzontali, minimi per tutta l'infrastruttura con un orizzonte a breve termine.

Specifiche a lungo termine

Obblighi, anche settorializzati e potenzialmente ambiziosi, proporzionati in base alla categorizzazione e con scadenze a medio e lungo termine.

Misure di sicurezza

Elementi misure di sicurezza

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)

Processo di sviluppo

Framework Core

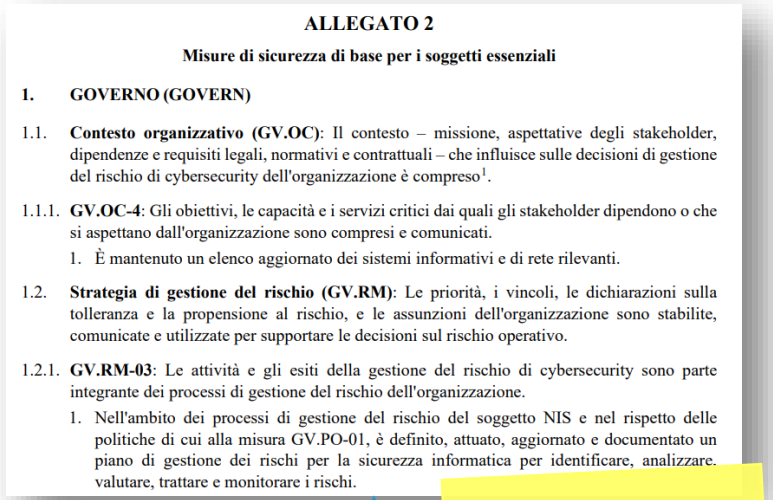
Funzioni	Categorie	Sottocategorie	Informative References
GOVERNO (GV)			
IDENTIFICAZIONE (ID)			
PROTEZIONE (PR)			
RILEVAMENTO (DE)			
RISPOSTA (RS)			
RIPRISTINO (RC)			

Framework contestualizzato

Funzioni	Categorie	Sottocategorie	Informative References
GOVERNO (GV)			
IDENTIFICAZIONE (ID)			
PROTEZIONE (PR)			
RILEVAMENTO (DE)			
RISPOSTA (RS)			
RIPRISTINO (RC)			

43 sottocategorie

Misure di sicurezza



ALLEGATO 2

Misure di sicurezza di base per i soggetti essenziali

1. GOVERNO (GOVERN)

1.1. **Contesto organizzativo (GV.OC)**: Il contesto – missione, aspettative degli stakeholder, dipendenze e requisiti legali, normativi e contrattuali – che influisce sulle decisioni di gestione del rischio di cybersecurity dell'organizzazione è compreso[1].

1.1.1. **GV.OC-4**: Gli obiettivi, le capacità e i servizi critici dai quali gli stakeholder dipendono o che si aspettano dall'organizzazione sono compresi e comunicati.

1. È mantenuto un elenco aggiornato dei sistemi informativi e di rete rilevanti.

1.2. **Strategia di gestione del rischio (GV.RM)**: Le priorità, i vincoli, le dichiarazioni sulla tolleranza e la propensione al rischio, e le assunzioni dell'organizzazione sono stabilite, comunicate e utilizzate per supportare le decisioni sul rischio operativo.

1.2.1. **GV.RM-03**: Le attività e gli esiti della gestione del rischio di cybersecurity sono parte integrante dei processi di gestione del rischio dell'organizzazione.

1. Nell'ambito dei processi di gestione del rischio del soggetto NIS e nel rispetto delle politiche di cui alla misura GV.PO-01, è definito, attuato, aggiornato e documentato un piano di gestione dei rischi per la sicurezza informatica per identificare, analizzare, valutare, trattare e monitorare i rischi.

116 requisiti

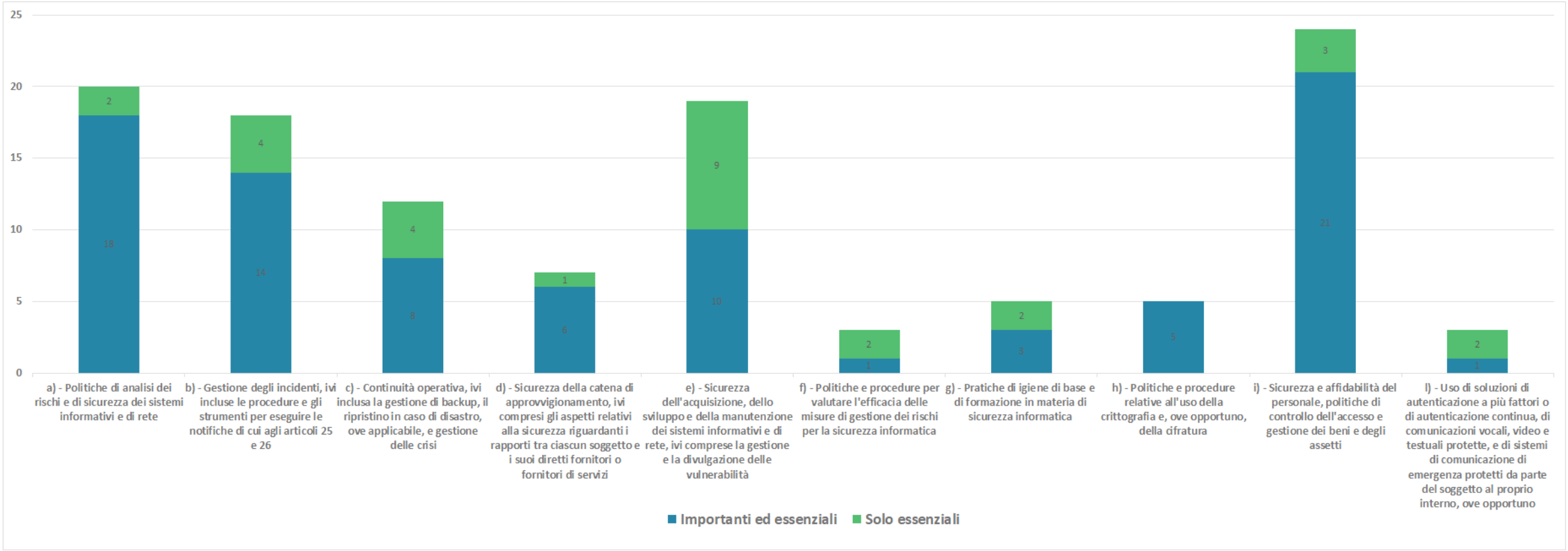
Selezione sottocategorie

Definizione requisiti

Previsioni D.Lgs. 138/2024

Best practices

Mappatura requisiti – elementi art. 24, co. 2, decreto NIS



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.

Declinazione 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

PR.DS-11

I backup dei dati sono creati, protetti, mantenuti e verificati.

PUNTO	REQUISITO	S_I	S_E
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.	●	●
3	Per almeno i sistemi informativi e di rete rilevanti, è assicurata la riservatezza e l'integrità delle informazioni contenute nei backup mediante adeguata protezione fisica dei supporti ovvero mediante cifratura.		●
4	Per almeno i sistemi informativi e di rete rilevanti, è verificata periodicamente l'utilizzabilità dei backup effettuati mediante test di ripristino.		●
5	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 3 e 4.		●

In accordo a esiti valutazione rischio

PR.AA-01

Le identità e le credenziali degli utenti, dei servizi e dell'hardware autorizzati sono gestite dall'organizzazione.

PUNTO	REQUISITO	S_I	S_E
1	Tutte le utenze, ivi incluse quelle con privilegi amministrativi e quelle utilizzate per l'accesso remoto, sono censite, approvate da attori interni al soggetto NIS e, fatte salve motivate e documentate ragioni tecniche, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono individuali per gli utenti.	●	●
2	Le credenziali (ad esempio nome utente e password) relative alle utenze sono robuste e aggiornate in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05.	●	●
3	Per almeno i sistemi informativi e di rete rilevanti, sono verificate periodicamente le utenze e le relative autorizzazioni, aggiornandole/revocandole in caso di variazioni (ad esempio trasferimento o cessazione di personale).	●	●
4	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1, 2 e 3.	●	●

PR.AA-03

Utenti, servizi e hardware sono autenticati

PUNTO	REQUISITO	S_I	S_E
1	Le modalità di autenticazione delle utenze per accedere ai sistemi informativi e di rete sono commisurate al rischio. A tal fine sono valutati almeno i rischi connessi: a) ai privilegi delle utenze; b) alla criticità dei sistemi informativi e di rete; c) alla tipologia di operazioni che le utenze possono effettuare sui sistemi informativi e di rete.	●	●
2	Per almeno i sistemi informativi e di rete rilevanti e in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono impiegate modalità di autenticazione multifattore.	●	●
3	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1 e 2.	●	●

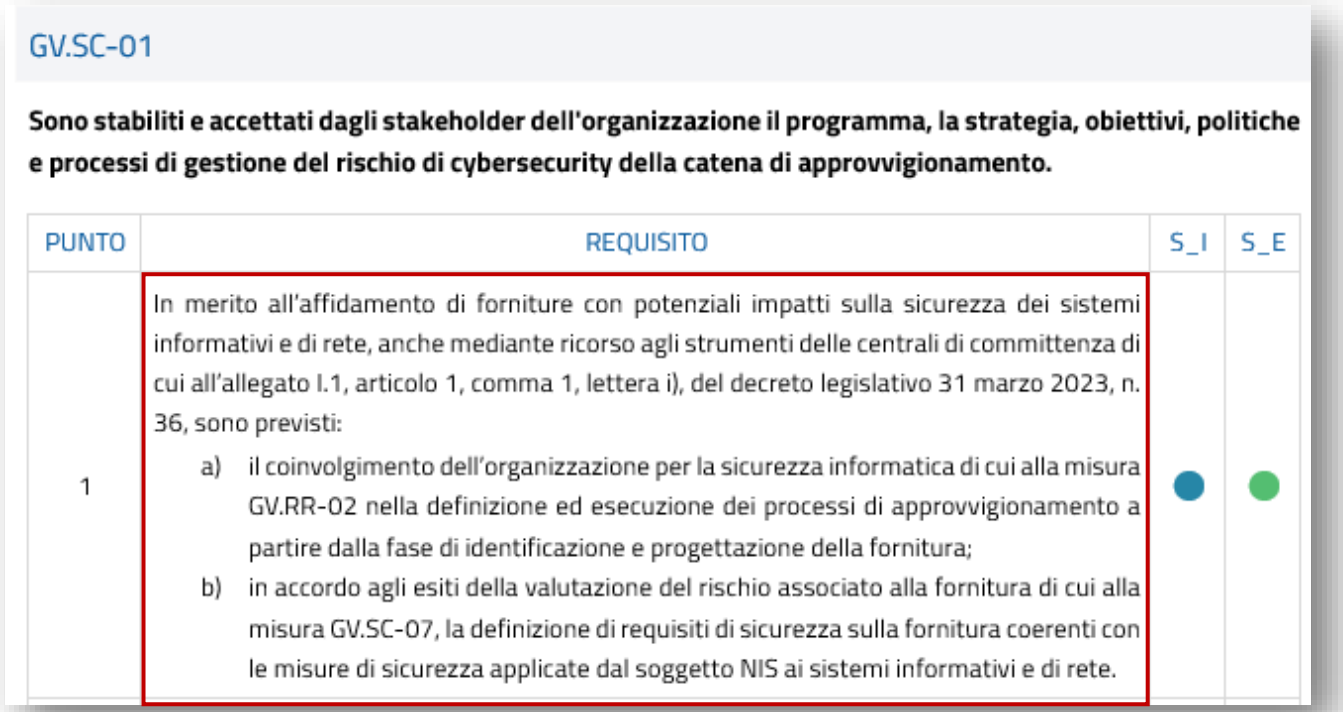
Fatte salve motivate e documentate ragioni

DE.CM-09

L'hardware e il software di elaborazione, gli ambienti di runtime e i loro dati sono monitorati per individuare eventi potenzialmente avversi.

PUNTO	REQUISITO	S_I	S_E
1	Fatte salve motivate e documentate ragioni normative o tecniche, sono presenti, aggiornati, mantenuti e configurati in modo adeguato, sistemi di protezione delle postazioni terminali per il rilevamento del codice malevolo.	●	●
2	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.	●	●

Forniture con potenziali impatti sulla sicurezza



GV.SC-01

Sono stabiliti e accettati dagli stakeholder dell'organizzazione il programma, la strategia, obiettivi, politiche e processi di gestione del rischio di cybersecurity della catena di approvvigionamento.

PUNTO	REQUISITO	S_I	S_E
1	In merito all'affidamento di forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete, anche mediante ricorso agli strumenti delle centrali di committenza di cui all'allegato I.1, articolo 1, comma 1, lettera i), del decreto legislativo 31 marzo 2023, n. 36, sono previsti: a) il coinvolgimento dell'organizzazione per la sicurezza informatica di cui alla misura GV.RR-02 nella definizione ed esecuzione dei processi di approvvigionamento a partire dalla fase di identificazione e progettazione della fornitura; b) in accordo agli esiti della valutazione del rischio associato alla fornitura di cui alla misura GV.SC-07, la definizione di requisiti di sicurezza sulla fornitura coerenti con le misure di sicurezza applicate dal soggetto NIS ai sistemi informativi e di rete.	●	●

Tipologia requisiti

Specifiche amministrative

Ad esempio:

- Adozione e approvazione politiche e procedure.
- Definizione di piani (ad es. risposta agli incidenti)
- Redazione documentazione.

Specifiche tecniche

Ad esempio:

- Cifratura dei dati.
- Aggiornamento del software.
- Modalità di autenticazione multifattore.

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*.

Politiche di sicurezza informatica

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.

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.

Incidenti significativi

Incidenti significativi di base (1/2)

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

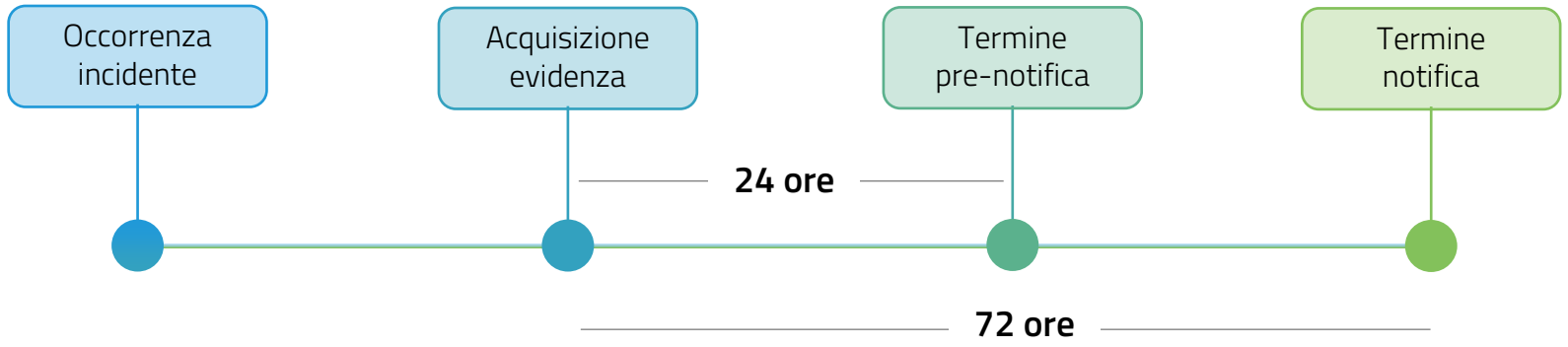
Solo soggetti essenziali
1 tipologia di incidente

Incidenti significativi di base (2/2)

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.



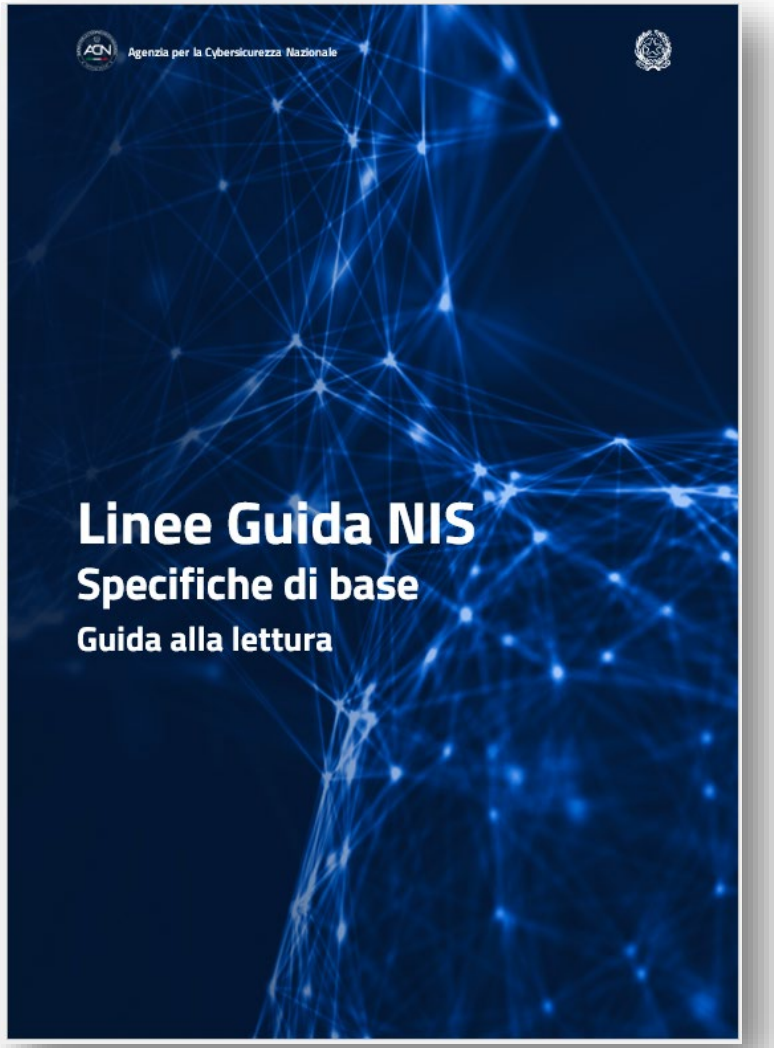
Abuso dei privilegi concessi

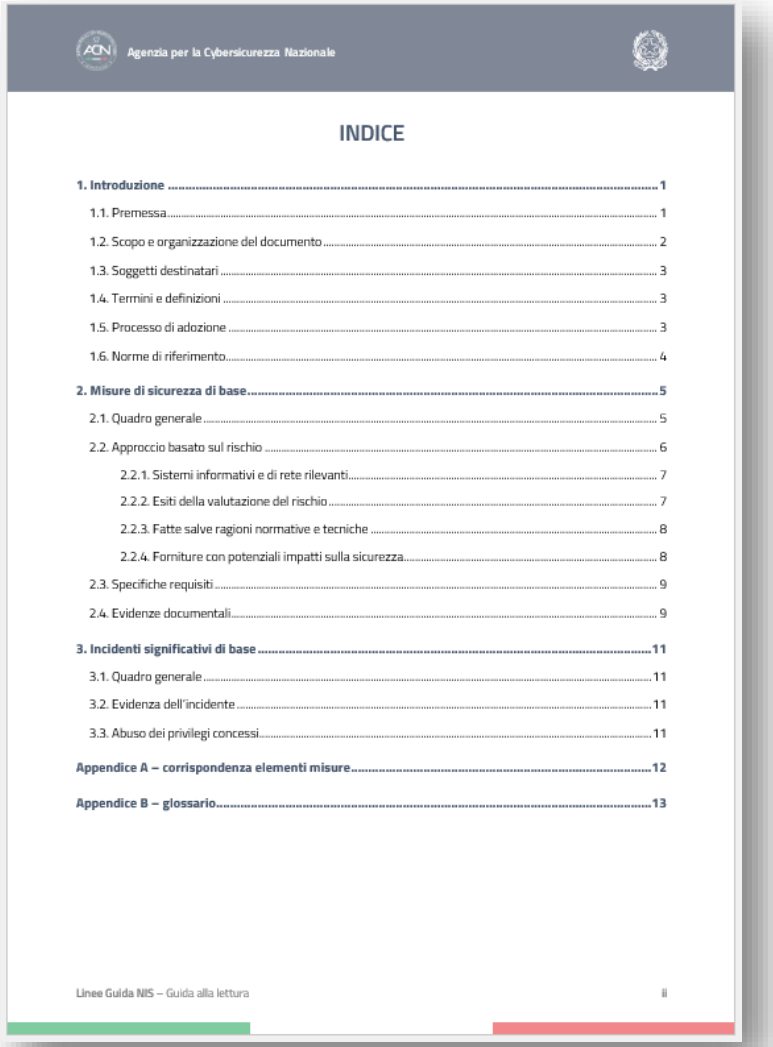
Fattispecie in cui un operatore abbia l'autorizzazione tecnica (ossia la disponibilità di credenziali che sono configurate per accedere ai dati) per accedere a determinati dati ma tale acceso sia effettivamente illecito in quanto, ad esempio, effettuato in violazione delle politiche del soggetto o risulti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

Strumenti di supporto

Strumenti di supporto

BOZZA




Agenzia per la Cybersicurezza Nazionale

INDICE


AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT

L'agenda dell'incontro

09:20 Benvenuto e introduzione

Gabriele Faggioli, *Responsabile Scientifico, Osservatorio Cybersecurity & Data Protection – Presidente Onorario CLUSIT*

Giorgia Dragoni, *Ricercatrice Senior, Osservatorio Cybersecurity & Data Protection*

09:30 Interventi a cura di:

Milena Antonella Rizzi, *Capo Servizio Regolazione dell'Agenzia per la Cybersicurezza Nazionale*

Vincenzo Allia, *Vice Capo della Divisione Perimetro di Sicurezza Nazionale Cibernetica (PSNC) e discipline nazionali dell'Agenzia per la Cybersicurezza Nazionale*

10:30 Sessione di Q&A

Luca Bechelli, *Senior Advisor Osservatorio Cybersecurity & Data Protection, CD Clusit*

Alessio Pennasilico, *Senior Advisor, Osservatorio Cybersecurity & Data Protection, CS Clusit*

11:45 Chiusura dei lavori e Cocktail

POLIMI SCHOOL OF MANAGEMENT | osservatori.net digital innovation

Clusit Associazione Italiana per la Sicurezza Informatica

Luca Bechelli

Senior Advisor Osservatorio
Cybersecurity & Data Protection

Comitato Direttivo Clusit

Alessio Pennasilico

Senior Advisor Osservatorio
Cybersecurity & Data Protection

Comitato Scientifico Clusit

POLIMI SCHOOL OF MANAGEMENT | osservatori.net digital innovation

Clusit Associazione Italiana per la Sicurezza Informatica

12.05.2025

Osservatorio Cybersecurity & Data Protection

NIS2, le istruzioni per l'uso: tutto quello che c'è da sapere

Sessione di Q&A

nis2@clusit.it

Nata nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, è la più numerosa ed autorevole associazione "no-profit" italiana nel campo della sicurezza informatica.
*Oggi rappresenta oltre **700 organizzazioni**, appartenenti a tutti i settori del Sistema-Paese.*

Obiettivi:

- Diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini.
- Partecipare alla elaborazione di leggi, norme e regolamenti che coinvolgono la sicurezza informatica, sia a livello nazionale che europeo.
- Contribuire alla definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza.
- Promuovere l'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

- **10.000+** partecipanti alle attività 2024
- **50+ eventi divulgativi** organizzati nel 2024
- **80+ webinar e seminari** tenuti nel 2024
- **300+ speaker e docenti** coinvolti
- **7.000 partecipanti** ai nostri eventi nel 2024
- **150+ documenti** prodotti (rapporti, quaderni, pillole di sicurezza, White Papers)
- **200+ contributori/autori** delle pubblicazioni
- **80.000 lettori** delle pubblicazioni (rapporti, quaderni, pillole di sicurezza)
- 800+ articoli e servizi su web, cartaceo, Radio e TV

Il Rapporto CLUSIT

Il Rapporto Clusit presenta un'analisi approfondita del cybercrime in Italia e nel mondo.

Giunto al XIII anno di pubblicazione, il Rapporto contiene inoltre una panoramica del mercato italiano dell'ICT security ed è completato da focus on specifici su temi caldi del momento.

Si tratta di un quadro estremamente aggiornato della situazione globale, con particolare attenzione a quella italiana, ed è ormai un fondamentale testo di riferimento per manager d'azienda, imprenditori, esperti, professionisti.

Ogni anno, distribuiamo oltre 2.500 copie cartacee, spedite anche a giornalisti, politici, vertici delle Istituzioni italiane, funzionari della PA legati al mondo ICT ed ai CIO, CSO e CISO di grandi aziende.

I Rapporti Clusit sono stati scaricati nel 2024 oltre 80.000 volte e sono stati oggetto nel 2024 di oltre 500 articoli e servizi su web, cartaceo, Radio e TV.

La prima edizione sarà presentata a Milano il giorno 11 marzo 2025 mentre l'edizione autunnale, totalmente inedita, nel novembre 2025.

Inoltre, in occasione degli appuntamenti verticali e della tappa di Roma, saranno prodotti degli approfondimenti sui settori Energy & Utilities, Healthcare, Manufacturing, P.A e Difesa e Finance.

POLIMI SCHOOL OF MANAGEMENT | osservatori.net digital innovation

Clusit Associazione Italiana per la Sicurezza Informatica

12.05.2025

Osservatorio Cybersecurity & Data Protection

NIS2, le istruzioni per l'uso:

tutto quello che c'è da sapere, e che volevate chiedere, sugli obblighi di base e le informazioni da fornire entro il 31 maggio.

nis2@clusit.it