WORKSHOP GARR 2025

NET MAKERS

NIS2: indicazioni operative per la comunità

Alessandro Inzerilli

GARR

Disclaimer

Le informazioni contenute in questa presentazione hanno scopo esclusivamente informativo e divulgativo. I contenuti riguardano anche il Decreto Legislativo 21 settembre 2024, n. 138, di recepimento della Direttiva (UE) 2022/2555 – NIS2, le determinazioni del Direttore generale dell'Agenzia per la cybersicurezza nazionale 333017/2025 e 136118/2025 e sono basate su fonti ufficiali e documenti normativi pubblici disponibili al momento della redazione.

Pur essendo stata prestata la massima attenzione all'accuratezza e all'aggiornamento delle informazioni, non si garantisce l'assenza di errori, omissioni o modifiche normative successive.

La presentazione non costituisce consulenza legale, tecnica o di conformità normativa, e l'autore non si assume alcuna responsabilità per decisioni o azioni intraprese sulla base dei contenuti esposti.

Per le domande: wooclap.com e codice WSGARR25

Normativa NIS

Direttiva (UE) 2022/2555 (NIS2)

- Aggiorna la normativa comunitaria in materia di **cybersicurezza**, abrogando la precedente direttiva (NIS1)
- Mira a **uniformare il quadro giuridico** in tutti gli Stati membri dell'UE, garantendo un **livello comune elevato** di sicurezza informatica
- Estende il **campo di applicazione** ad un numero maggiore di settori
- Rafforza la **cooperazione** tra gli Stati membri e le autorità di sicurezza.

Decreto legislativo 138/2024

- Recepisce la direttiva UE a livello nazionale
- Definisce obblighi in materia di **misure di sicurezza** e di **notifica di incidente**
- Individua **18 settori** in ambito di cui **11 altamente critici** e **7 critici** (allegati I - IV decreto)
- Definisce i **criteri oggettivi** per l'individuazione dei soggetti NIS, distinti tra **soggetti essenziali** ed **importanti** in base al livello di criticità dei settori
- Attribuisce ad **ACN** (Autorità nazionale competente NIS) poteri di **vigilanza** e **sanzione**

Provvedimenti attuativi

- Determinazioni ACN stabiliscono **termini**, **modalità**, **specifiche** e **tempi graduali** di **implementazione** degli obblighi
- Costituiscono le **norme attuative** in tema di misure di sicurezza e di notifica degli incidenti
- Regolano **adempimenti annuali** da effettuarsi tramite il portale ACN
- Definiscono le modalità di **designazione** referenti NIS e **censimento** organi di amministrazione e direttivi

Comunità GARR e NIS

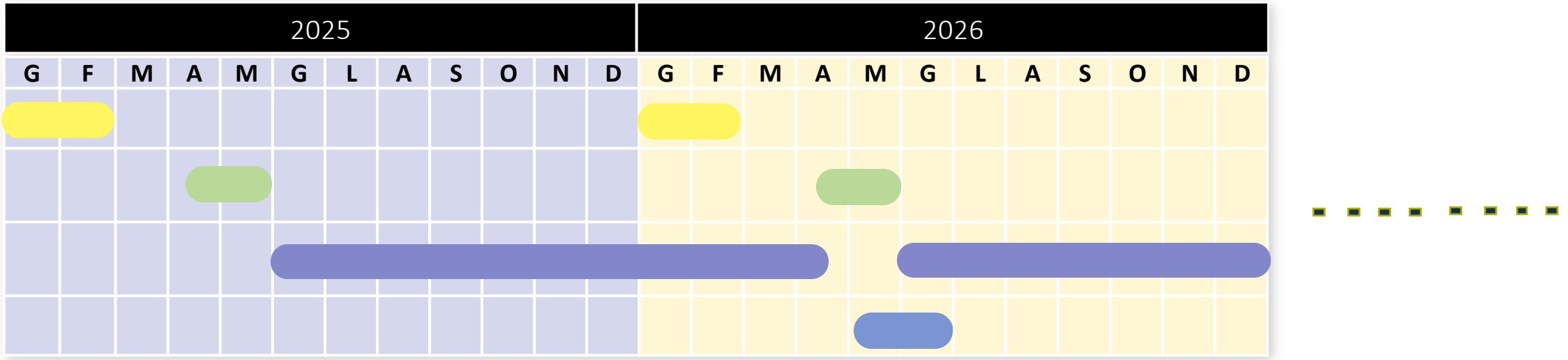
Enti GARR appartenenti alla comunità dell'**istruzione**, della **ricerca** e della **cultura**

Le loro attività rientrano prevalentemente in settori definiti **critici** e pertanto identificati prevalentemente come **soggetti importanti** con qualche eccezione*

Settore	Allegato Decreto	Autorità di settore
Infrastrutture digitali*	I - numero 8	MIMIT
Settore sanitario*	I - numero 5	MS
Fornitori di servizi digitali	II - numero 6	MIMIT
Organizzazioni di ricerca	II - numero 7	MUR
Enti e le Istituzioni di ricerca	III - lettera d) - numero 5	PCM (ACN)
Istituti zooprofilattici sperimentali	III - lettera d) - numero 6	PCM (ACN)
Istituti di istruzione che svolgono attività di ricerca	IV - numero 2	MUR
Soggetti che svolgono attività di interesse culturale	IV - numero 3	MiC

Adempimenti annuali

Adempimenti Annuali	Rif. D.Lgs.138/2024	Norme attuative	Termini
Registrazione (annuale)	Art. 7 - comma 1	Det. ACN 333017/2025 art. 11	1 gennaio - 28 febbraio
Aggiornamento annuale	Art. 7 - commi 4 e 5	Det. ACN 333017/2025 artt. 16 e 17	15 aprile - 31 maggio
Aggiornamento continuo	Art. 7 - comma 7	Det. ACN 333017/2025 art. 18	1 giugno - 14 aprile anno successivo
Elencazione, caratterizzazione e categorizzazione attività e servizi	Art. 30	Non adottate	1 maggio - 30 giugno (a partire dal 2026)



WORKSHOP GARR 2025

NET MAKERS

Attuazione Decreto NIS: specifiche di base

Alessandro Inzerilli

GARR

Adozione delle specifiche di base

Con la determinazione ACN 164179 del 14 aprile 2025 sono adottate le **specifiche di base**

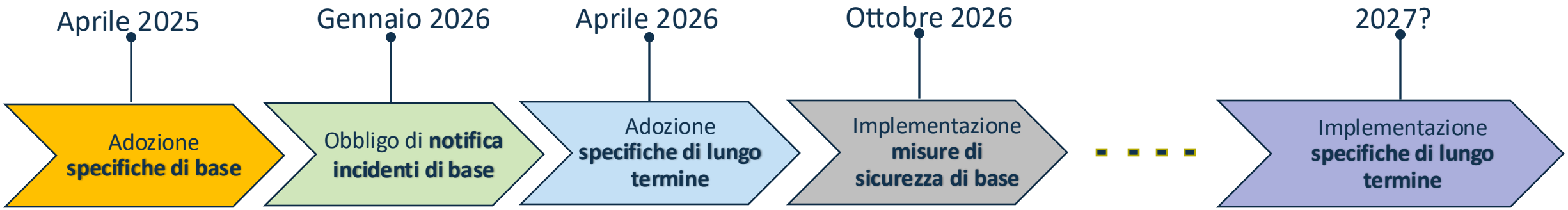
Norme attuative degli obblighi degli artt. 23 (organi di amministrazione e direttivi), 24 (misure di sicurezza), 25 (notifica degli incidenti)

Obblighi da adottare **a breve termine** per **tutta l'infrastruttura ICT**

Misure di sicurezza di base (allegati 1 e 2)

Incidenti significativi di base (allegati 3 e 4)

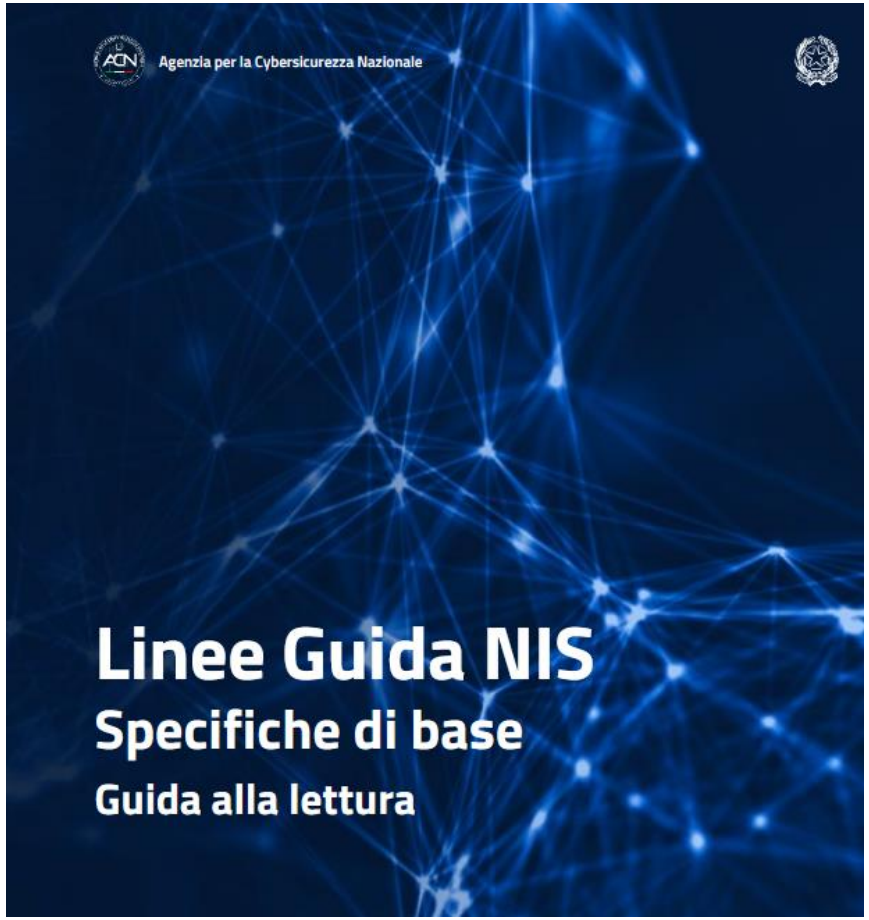
Entro Aprile 2026 verranno adottate le **specifiche a lungo termine**



Linee Guida NIS

Linee guida NIS – Specifiche di base – Guida alla lettura pubblicate da ACN il 4 settembre 2025

A supporto dei soggetti NIS nella comprensione, interpretazione e attuazione della specifiche di base



Misure di sicurezza

Decreto NIS (art. 24) richiede l'adozione di misure **tecniche**, **operative** e **organizzative** secondo un principio di **proporzionalità** e **gradualità.**

Devono essere **proporzionate** al grado di esposizione ai rischi e alla dimensione dei soggetti, **adeguate** alla probabilità degli incidenti e alla loro gravità

In fase di prima applicazione le misure di sicurezza di base sono **differenziate** a seconda dell'individuazione del soggetto quale essenziale o importante

Le misure a lungo termine saranno differenziate sulla base della **caratterizzazione** delle attività e servizi

Modello di categorizzazione verrà adottato entro aprile 2026

Adottato approccio **multi-rischio** (non solo rischio cyber)

Comprendono 10 elementi

Elementi Decreto NIS
a) Politiche di **analisi dei rischi** e di **sicurezza** dei sistemi informativi e di rete
b) Gestione degli **incidenti**, ivi incluse le procedure e gli strumenti per eseguire le notifiche di cui agli articoli 25 e 26
c) **Continuità operativa**, ivi inclusa la gestione di **backup**, il **ripristino in caso di disastro**, ove applicabile, e **gestione delle crisi**
d) Sicurezza della **catena di approvvigionamento**, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi
e) Sicurezza dell'**acquisizione**, dello **sviluppo** e della **manutenzione** dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle **vulnerabilità**
f) Politiche e procedure per valutare l'**efficacia** delle misure di **gestione dei rischi** per la sicurezza informatica
g) Pratiche di **igiene di base** e di **formazione** in materia di sicurezza informatica
h) Politiche e procedure relative all'uso della **crittografia** e, ove opportuno, della cifratura
i) Sicurezza e **affidabilità** del **personale**, politiche di **controllo** dell'**accesso** e **gestione** dei beni e degli **assetti**
l) 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, ove opportuno

Mappatura Elementi -Ambiti delle misure di sicurezza

Elemento NIS - D.Lgs. 138/2024 (Nr. 10)	Ambiti Politiche - Specifiche di Base (Nr. 16)
a) Politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete	a) Gestione del rischio b) Ruoli e responsabilità d) Conformità e audit di sicurezza
b) Gestione degli incidenti, ivi incluse le procedure e gli strumenti per eseguire le notifiche di cui agli articoli 25 e 26	m) Sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete o) Monitoraggio degli eventi di sicurezza. p) Risposta agli incidenti e ripristino
c) Continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove applicabile, e gestione delle crisi	h) Continuità operativa, ripristino in caso di disastro e gestione delle crisi l) Sicurezza dei dati p) Risposta agli incidenti e ripristino
d) Sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi	e) Gestione dei rischi per la sicurezza informatica della catena di approvvigionamento
e) Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità	e) Gestione dei rischi per la sicurezza informatica della catena di approvvigionamento g) Gestione delle vulnerabilità m) Sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete
f) Politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica	d) Conformità e audit di sicurezza
g) Pratiche di igiene di base e di formazione in materia di sicurezza informatica	k) Formazione del personale e consapevolezza
h) Politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura	l) Sicurezza dei dati
i) Sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli assetti	c) Affidabilità delle risorse umane f) Gestione degli asset i) Gestione dell'autenticazione, delle identità digitali e del controllo accessi j) Sicurezza fisica n) Protezione delle reti e delle comunicazioni
l) 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, ove opportuno	i) Gestione dell'autenticazione, delle identità digitali e del controllo accessi l) Sicurezza dei dati n) Protezione delle reti e delle comunicazioni

Misure di sicurezza di base

Sviluppate in accordo con il **Framework Nazionale per la Cybersecurity e la Data Protection** (FNCS v2.1) https://www.cybersecurityframework.it/ , allineato nel 2025 con la versione 2.0 del core del Cybersecurity Framwork (CSF) NIST

Ogni misura di sicurezza è caratterizzata da un codice identificativo, una descrizione e da uno o più requisiti. Il codice e la descrizione fanno riferimento alle funzioni, categorie e sottocategorie del framework (es. GV.RR-01)

I requisiti specificano ciò che è richiesto ai fini dell'implementazione della misura

Per i soggetti essenziali sono state individuate **43** sotto-categorie e **116** requisiti (**37** e **87** rispettivamente per soggetti importanti)

Requisiti possono essere generalmente suddivisi in due tipologie:

- **organizzativi** (es. governance, policy, piani, processi, procedure)
- **tecnici** (es. uso di strumenti e tecnologici, cifratura, MFA)

Nelle misure di base prevalgono quelle organizzative.

Specifiche di base: documentazione

Elaborazione di documenti ai fini

- dell'**attuazione**
- dell'**attestazione**

dell'effettiva implementazione delle misure di sicurezza (*evidenze documentali*)

Piani (Nr. 10)	Requisito
gestione dei rischio	GV.RM-03 punto 1
trattamento del rischio	ID.RA-06 punto 1
gestione vulnerabilità	ID.RA-08 punto 1
adeguamento	ID.IM-01 punto 1
valutazione dell'efficacia*	ID.IM-01 punto 3
continuità operativa	ID.IM-04 punto 1
ripristino in caso di disastro	ID.IM-04 punto 2
per la gestione delle crisi	ID.IM-04 punto 3
formazione tutti i dipendenti	PR.AT-01 punto 1
gestione degli incidenti	RS.MA-01 punto 1

* Richiesti solo ai soggetti essenziali

ELENCHI (Nr. 5)	Requisito
sistemi informativi e di rete rilevanti	GV.OC-04 punto 1
personale dell'organizzazione di sicurezza informatica	GV.RR-02 punto 2
personale dell'organizzazione di sicurezza informatica fornitori	GV.SC-02 punto 2
configurazioni di riferimento sicure*	PR.PS-01 punto 1
sistemi informativi e di rete accessibili da remoto	PR.IR-01 punto 2

REGISTRI (Nr.5)	Requisito
esiti del riesame politiche di sicurezza	GV.PO-02 punto 3
formazione tutti i dipendenti	PR.AT-01 punto 3
formazione amministratori*	PR.AT-02 punto 2
manutenzioni effettuate sull'hardware*	PR.PS-03 punto 2
accessi eseguiti da remoto e quelli privilegiati	PR.PS-04 punto 1

INVENTARI (Nr.5)	Requisito
Inventario fornitori	GV.SC-04 punto 1
apparati fisici (hardware)	ID.AM-01 punto 1
Servizi, sistemi e applicazioni software	ID.AM-02 punto 1
flussi di rete tra i sistemi informativi e di rete*	ID.AM-03 punto 1
servizi informatici erogati dai fornitori (inclusi i servizi cloud)	ID.AM-04 punto 1

Specifiche di base: documentazione (cont.)

Adozione e **documentazione** di **procedure** relative a **33** requisiti di **19** misure di sicurezza, prevalentemente di natura tecnica (di cui **7** richieste solo ai soggetti essenziali *)

La normativa impone un **aggiornamento continuo** della documentazione

Necessario per le organizzazione dotarsi di un **sistema documentale** in grado di tracciare le revisioni e l'iter di approvazione

Requisiti	Oggetto Procedura
GV.RR-04 - punto 1	Affidabilità personale autorizzato ad accedere ai sistemi informativi e di rete rilevanti
GV.RR-04 - punto 2	Affidabilità amministratori di sistemi e di rete
GV.RR-04 - punto 4	Obblighi contrattuali in materia di sicurezza informatica *
PR.AA-01 - punto 1	Approvazione utenze individuali
PR.AA-01 - punto 2	Robustezza credenziali
PR.AA-01 - punto 3	Audit utenze per sistemi informativi e di rete rilevanti
PR.AA-03 - punto 1	Modalità autenticazione
PR.AA-03 - punto 2	MFA per sistemi informativi e di rete rilevanti
PR.AA-05 - punto 1	Criterio minimo privilegio e separazione funzioni
PR.AA-05 - punto 2	Distinzione tra utenze privilegiate e no
PR.AA-06 - punto 1	Accesso fisico protetto ai sistemi informativi e di rete rilevante
PR.DS-01 - punto 1	Cifratura dati per sistemi informativi e di rete rilevanti
PR.DS-01 - punto 2	Sicurezza dei supporti rimovibili
PR.DS-02 - punto 1	Trasmissione cifrata dei dati per sistemi informativi e di rete rilevanti
PR.DS-11 - punto 1	Backup periodici offline per i sistemi informativi e di rete rilevanti
PR.DS-11 - punto 3	Cifratura backup per i sistemi informativi e di rete rilevanti *
PR.DS-11 - punto 4	Verifica ripristino dati da backup per i sistemi informativi e di rete rilevanti *
PR.PS-01 - punto 1	Elenco configurazioni di riferimento sicure per i sistemi informativi e di rete rilevanti *
PR.PS-02 - punto 1	Granzia disponibilità aggiornamenti software di sicurezza
PR.PS-02 - punto 2	Installazione aggiornamenti software di sicurezza
PR.PS-02 - punto 4	Aggiornamento critici in ambiente di test
PR.PS-04 - punto 1	Tracciamento accessi remoti e accessi privileggiati
PR.PS-04 - punto 2	Tracciamento log eventi cyber e accessi per i sistemi informativi e di rete rilevanti
PR.IR-01 - punto 1	Attività consentite da remoto per i sistemi informativi e di rete rilevanti
PR.IR-01 - punto 2	Elenco sistemi accessibili da remoto
PR.IR-01 - punto 3	Presenza sistemi perimetriali
PR.IR-03 - punto 1	Utilizzo di sistemi di comunicazione di emergenza protetti *
DE.CM-01 - punto 1	Monitoraggio incidenti per i sistemi informativi e di rete rilevanti
DE.CM-01 - punto 2	Livelli di servizio attesi
DE.CM-01 - punto 4	Filtraggio e analisi del traffico per i sistemi informativi e di rete rilevanti
DE.CM-01 - punto 5	Monitoraggio accessi da remoto, attività, eventi, accessi eseguiti o falliti per i sistemi informativi e di rete rilevanti *
DE.CM-01 - punto 6	Parametri quali-quantitativi per rilevare accessi non autorizzati o abusivi per i sistemi informativi e di rete rilevanti *
DE.CM-09 - punto 1	Anti-malware endpoint

Ruolo degli Organi di Amministrazione e Direttivi

Gli organi di amministrazione e direttivi dei soggetti NIS hanno una **responsabilità diretta e specifica in materia di cybersicurezza** (art. 23)

Obblighi degli organi di amministrazione e direttivi:

devono approvare le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica (**Responsibility**)
devono sovrintendere all'implementazione delle misure di sicurezza con risultati verificabili e documentabili (**Accountability**)
sono responsabili per eventuali violazioni (**Liability**)

promuovono una formazione specifica in materia di cybersicurezza per i tutti dipendenti (inclusi loro stessi)

delegano al proprio interno l'attuazione degli obblighi rimanendone responsabili (es. punto di contatto e sostituto, etc.)

coincidono tipicamente con i componenti del **Consiglio di amministrazione dell'organizzazione** (non comprendono altre figure apicali se sotto ordinate ai CdA)

Specifiche di base: organi di amministrazione e direttivi

Le specifiche di base delineano gli obblighi degli organi di amministrazione e direttivi

13 requisiti di **9** misure citano esplicitamente gli organi di amministrazione e direttivi (**CdA**)

sono responsabili dell'approvazione dei **11** documenti che definiscono complessivamente la governance in materia di sicurezza informatica delle organizzazioni GV.RR-02 punto 1, GV.PO-01 punto 1, ID.RA-05 punto 3, ID.RA-06 punto 3, ID.RA-08 punto 4, ID.IM-01 punto 1, ID.IM-04 punto 1, PR.AT-01 punto 1, RS.MA-01 punto 2

sono informati sullo stato di avanzamento (**miglioramento continua**) del piano di adeguamento ID.IM-01 punto 2 e di quello di valutazione dell'efficacia delle misure di gestione del rischio ID.IM-01 punto 4

sono informati sugli incidenti significativi RS.MA-01 punto 1

Documenti approvati dagli Organi di Amministrazione e Direttivi

Documenti	Periodicità aggiornamento *	Requisito
Organizzazione per la sicurezza informatica con definizione ruoli e responsabilità	Almeno ogni 2 anni	GV.RR-02 punto 1
Politiche di sicurezza informatica	Almeno ogni anno	GV.PO-01 punto 1
Valutazione del rischio	Almeno ogni 2 anni	ID.RA-05 punto 3
Piano di trattamento del rischio	Almeno ogni 2 anni	ID.RA-06 punto 3
Piano di gestione delle vulnerabilità	Non specificato (annuale)	ID.RA-08 punto 4
Piani di adeguamento	Almeno ogni anno	ID.IM-01 punto 1
Piani di continuità operativa, ripristino in caso di disastro e gestione delle crisi per servizi e attività NIS	Almeno ogni 2 anni	ID.IM-04 punto 1
Piano di formazione	Non specificato (annuale)	PR.AT-01 punto 1
Piano per la gestione e notifica degli incidenti di sicurezza informatica	Almeno ogni 2 anni	RS.MA-01 punto 2

* Documenti da aggiornare prima in caso di evoluzioni del contesto normativo, incidenti significativi, variazioni organizzative, mutamenti dell'esposizione alle minacce e ai relativi rischi

Politiche di sicurezza

Le organizzazione devono definire, adottare e documentare le **politiche di sicurezza** nei **16** ambiti previsti dalla normativa GV.PO-01 punto 1

Per ogni ambito sono indicati puntualmente (tabella 1 degli allegati 1 e 2 della det.) i requisiti per cui vanno specificate le politiche (**94** su 116, di cui **23** specifici per i soggetti essenziali) GV.PO-01 punto 2

Le politiche di sicurezza vanno approvate dal **CdA** GV.PO-01 punto 3

Le politiche vanno **riesaminate** almeno con cadenza **annuale** o prima in caso di variazione del contesto (normativo, organizzativo, di rischio) GV.PO-02 punto 1

Va verificata almeno la compliance rispetto al quadro normativo GV.PO-02 punto 2

Le variazioni vanno tracciate in un apposito **registro** GV.PO-02 punto 3

In base agli esiti del riesame è definito e attuato un **piano di adeguamento** con gli interventi correttivi necessari, che è approvato dal CdA ID.IM-01 punto 1

Ambiti Politiche
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

Organizzazione di Cybersicurezza

Ogni soggetto NIS deve definire in maniera formale (approvazione del CdA richiesta) e rendere nota al proprio interno, l'**organizzazione per la sicurezza informatica** stabilendo **ruoli** e **responsabilità** GV.RR-02 punto 1

Va mantenuto un elenco aggiornato dei componenti GV.RR-02 punto 2

Dell'organizzazione per la sicurezza informatica fanno parte il punto di contatto, sostituto GV.RR-02 punto 3 (e il referente CSIRT appena introdotto)

I ruoli e le responsabilità dei componenti vanno **riesaminati** e, eventualmente, aggiornati almeno ogni **due anni** GV.RR-02 punto 4

Politiche di sicurezza e ruoli

Analogie e differenze tra l'attuazione di una normativa come la NIS2 e la certificazione ISO/IEC 27001

Aver adottato il framework per l'istituzione di Sistema di Gestione della Sicurezza delle Informazioni (ISMS) costituisce una buon punto di partenza per soddisfare i requisiti della NIS2

La cybersicurezza è una questione strategica che coinvolge in modo trasversale tutte le organizzazioni (CdA, CEO/CIO/CFO/CISO, referenti NIS, aree compliance/RM/legale, DPO, amministrazione, HR, comunicazione, formazione, gruppi IT, CSIRT/SOC)

Necessario anche sviluppare competenze **specifiche**

Ruoli e responsabilità della cybersicurezza - Elementi chiave per l'assegnazione (fonte ACN)

European Cybersecurity Skills Framework (ECSF) (Fonte ENISA)

Cybersecurity roles and skills for NIS2 Essential and Important Entities (Fonte ENISA)

Gestione del rischio

Ogni organizzazione deve dotarsi di un **piano di gestione del rischio** per la sicurezza informatica allo scopo di identificare, analizzare, valutare, trattare e monitorare i rischi GV.RM-03 punto 1

Il piano deve prevedere
- **una valutazione dei rischi** (Risk Assessment - RA) ID.RA-05 punto 1
- **piano di trattamento del rischio** ID.RA-06 punto 1

Il RA (e il conseguente piano di trattamento) vanno ripetuti almeno **ogni due anni** o in occasione di incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi ID.RA-05 punto 2 e devono essere approvati dal **CdA** ID.RA-05 punto 3 e ID.RA-06 punto 3

Ogni organizzazione può adottare la **metodologia** che preferisce. Il RA deve prendere in considerazione i rischi a cui sono esposti i sistemi informativi e di rete, inclusi quelli legati alla supply chain, e comprendere almeno **identificazione**, **analisi** e **ponderazione** del rischio.

Solo nel caso dei soggetti essenziali è specificato che vanno considerate almeno le **minacce** interne ed esterne, le **vulnerabilità** non risolte e gli **impatti** conseguenti ad eventuali incidenti ID.RA-05 punto 4

Il piano di trattamento del rischio deve comprendere per ogni rischio opzioni di trattamento (es. evitare, modificare, condividere, accettare), misure di mitigazione, priorità, risk owner, tempistiche, motivazioni di accettazione dei rischi residui

L'**efficacia** delle misure di gestione del rischio va monitorata e valutate continuamente ID.IM-01 punto 3

Sistemi informativi e di rete rilevanti

Sistemi la cui **compromissione** in termini di RID avrebbe **impatto significativo** su **attività e servizi** per cui si è rientrati in ambito NIS

Di tali sistemi va mantenuto un elenco aggiornato GV.OC-04 punto 1

L'**ambito di applicazione** di **22** requisiti (13 per i soggetti importanti) può essere limitato a tali sistemi

Requisito	Descrizione (Nr. 22)
GV.RR-04 punto 1	Affidabilità personale autorizzato ad accedere ai sistemi informativi e di rete rilevanti
ID.RA-01 punto 2	Vulnerability assessment e penetration test per i sistemi informativi e di rete rilevanti*
ID.IM-04 punto 1	Piano continuità operativa per i sistemi informativi e di rete rilevanti
ID.IM-04 punto 2	Piano di ripristino per i sistemi informativi e di rete rilevanti
ID.IM-04 punto 3	Piano per la gestione delle crisi per i sistemi informativi e di rete rilevanti
PR.AA-01 punto 3	Audit utenze per sistemi informativi e di rete rilevanti
PR.AA-03 punto 2	MFA per sistemi informativi e di rete rilevanti
PR.AA-06 punto 1	Accesso fisico protetto ai sistemi informativi e di rete rilevante
PR.DS-01 punto 1	Cifratura dati per sistemi informativi e di rete rilevanti
PR.DS-02 punto 1	Trasmissione cifrata dei dati per sistemi informativi e di rete rilevanti
PR.DS-11 punto 1	Backup periodici offline per i sistemi informativi e di rete rilevanti
PR.DS-11 punto 3	Cifratura backup per i sistemi informativi e di rete rilevanti*
PR.DS-11 punto 4	Verifica ripristino dati da backup per i sistemi informativi e di rete rilevanti*
PR.PS-01 punto 1	Elenco configurazioni di riferimento sicure per i sistemi informativi e di rete rilevanti*
PR.PS-03 punto 1	Trasferimento e dismissione dispositivi memorizzazione per i sistemi informativi e di rete rilevanti*
PR.PS-03 punto 2	Registro manutenzioni hardware per i sistemi informativi e di rete rilevanti*
PR.PS-04 punto 2	Tracciamento log eventi cyber e accessi per i sistemi informativi e di rete rilevanti
PR.IR-01 punto 1	Attività consentite da remoto per i sistemi informativi e di rete rilevanti
DE.CM-01 punto 1	Monitoraggio incidenti per i sistemi informativi e di rete rilevanti
DE.CM-01 punto 4	Filtraggio e analisi del traffico per i sistemi informativi e di rete rilevanti*
DE.CM-01 punto 5	Monitoraggio accessi da remoto, attività, eventi per i sistemi informativi e di rete rilevanti*
DE.CM-01 punto 6	Parametri quali-quantitativi per accessi non autorizzati per i sistemi informativi e di rete rilevanti*

* Richiesti solo ai soggetti essenziali

Altre misure di sicurezza dipendenti dal RA

10 requisiti per cui vanno previste **misure di mitigazione compensative** nel piano di trattamento, se non implementate per motivi normativi o tecnici ID.RA-06 punto 3 (*..fatte salve motivate e documentate ragioni normative o tecniche..*)

3 requisiti applicabili alle sole **forniture con potenziale impatto sulle sicurezza** dei sistemi informativi e di rete (in caso di compromissione in termini di RID) (*forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete …*)

9 requisiti la cui **modalità** e **ambito** di **attuazione** dipendono dall'esito della valutazione del rischio (*..in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05 …*)

Requisito	Descrizione (Nr. 10)
GV.SC-05 punto 1	Requisiti sicurezza in contratti, gare, convenzioni
ID.RA-01 punto 2	VA e PT per i sistemi informativi e di rete rilevanti*
PR.AA-01 punto 1	Approvazione utenze individuali
PR.DS-01 punto 1	Cifratura dati per sistemi informativi e di rete rilevanti
PR.DS-01 punto 2	Sicurezza dei supporti rimovibili
PR.DS-02 punto 1	Trasmissione cifrata dei dati per sistemi informativi e di rete rilevanti
PR.PS-02 punto 1	Garanzia disponibilità aggiornamenti software di sicurezza
PR.PS-02 punto 2	Installazione aggiornamenti software di sicurezza
PR.PS-02 punto 4	Aggiornamento critici in ambiente di test*
DE.CM-09 punto 1	Anti-malware endpoint

Requisito	Descrizione (Nr. 3)
GV.SC-01 punto 1	Coinvolgimento org. cybersecurity e requisiti sicurezza nelle forniture
GV.SC-04 punto 1	Inventario fornitori
GV.SC-05 punto 1	requisiti sicurezza in contratti, gare, convenzioni

Requisito	Descrizione (Nr. 9)
GV.RR-04 punto 4	Obblighi contrattuali in materia di sicurezza informatica*
PR.AA-01 punto 1	Approvazione utenze individuali
PR.AA-01 punto 2	Robustezza credenziali
PR.AA-03 punto 2	MFA per sistemi informativi e di rete rilevanti
PR.DS-01 punto 1	Cifratura dati per sistemi informativi e di rete rilevanti
PR.DS-02 punto 1	Trasmissione cifrata dei dati per sistemi informativi e di rete rilevanti
PR.PS-02 punto 4	Aggiornamento critici in ambiente di test*
PR.PS-04 punto 3	tempo conservazione log
PR.IR-03 punto 1	Utilizzo di sistemi di comunicazione di emergenza protetti*

* Richiesti solo ai soggetti essenziali

Gestione del rischio

L’analisi del rischio è «al centro» della normativa NIS.

E’ fondamentale rendere il risk management un processo strategico all’interno delle organizzazioni, a protezione degli asset, ma anche come stimolo al miglioramento.

Serve definire policy, processi, procedure, criteri di valutazione, adeguanti al proprio contesto; individuare competenze e ruoli; dotarsi di strumenti a supporto dei processi.

Normativa stabilisce dei criteri generali, ma non detta metodologie.

Partire dagli standard di riferimento: ISO/IEC 27005, NIST SP 800-30 Rev. 1

Obbligo di notifica degli incidenti significativi

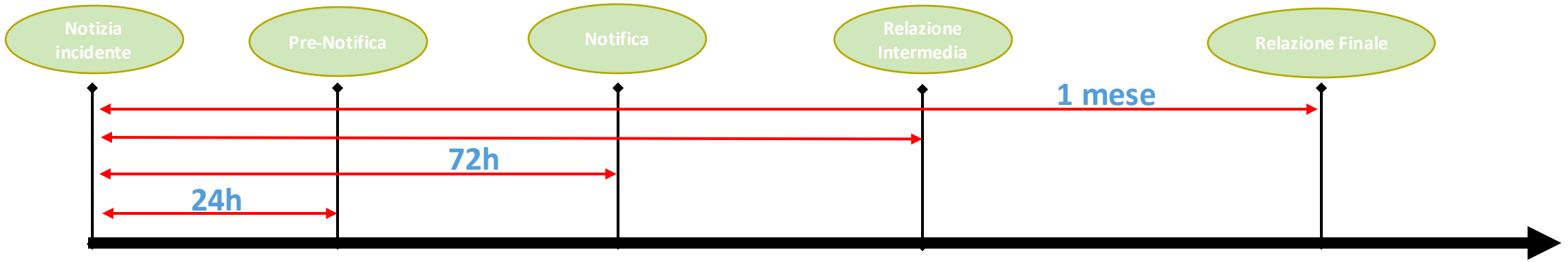
Decreto NIS richiede l'obbligo per i soggetti NIS di notifica allo **CSIRT Italia** di ogni **incidente** che ha un **impatto significativo** sulla fornitura dei loro servizi (art. 25)

Definisci un Incidente significativo se causa:

- una **grave perturbazione operativa** dei servizi
- **perdite finanziarie** per il soggetto interessato
- **ripercussioni** su altre **persone fisiche** o **giuridiche**
- **perdite materiali** o **immateriali** considerevoli

Regolamento di esecuzione (UE) 2024/2690 (17 ottobre 2024 – art. 3) individua **criteri quantitativi** per valutare l'impatto degli incidenti

Le specifiche di base «semplificano» l'interpretazione definendo gli **incidenti significativi di base**



Referente CSIRT

La determinazione ACN Det. ACN 333017/2025 (art. 7) ha introdotto la figura del **referente CSIRT,** non prevista da Direttiva e Decreto NIS, ma in linea con altre normative in ambito cyber security (es. PSNC).

Ha il compito di interloquire con lo CSIRT Italia e di effettuare le notifiche degli incidenti

Deve possedere **competenze di base** in materia di **sicurezza informatica** e di **gestione di incidenti** informatici, nonché una **conoscenza approfondita** dei sistemi informativi e di rete dell'organizzazione

Andrà designato tra il 20 novembre e il 31 dicembre 2025, insieme ad eventuali sostituti e può essere esterno (solo se diverso da punto di contatto)

Gestione degli incidenti

Ogni organizzazione deve definire, attuare e documentare un piano per la **gestione e notifica degli incidenti** RS.MA-01 punto 1

Il piano è approvato dal **CdA** RS.MA-01 punto 2 e riesaminato/aggiornato almeno ogni **due anni** RS.MA-01 punto 3

Il piano comprende

- procedure di gestione delle fasi dell'incidente e di notifica allo **CSIRT Italia**, inclusa la trasmissione delle relazioni previste (iniziale, intermedia, finale)
- personale coinvolto con ruoli e delle responsabilità
- modalità di comunicazione interna ed esterna (incluso **CdA**)

Sono previste anche le procedure per informare

- i propri utenti degli incidenti con impatto sui loro servizi, delle potenziali minacce e possibili azioni di mitigazione
- il pubblico RS.CO-02 punto 1 e 2

Vanno adottate e documentate procedure di **ripristino post-incidente** RC.RP-01 punto 1

Incidenti significativi di base

Le specifiche di base prevedono l'obbligo di notifica solo per **4** tipologie di incidenti definiti **incidenti significativi di base** (**3** per i soggetti importanti)

Tassonomia degli Incidenti semplificata mira a rendere gli incidenti facili da riconoscere

Incidenti che compromettono le proprietà **RID** dei dati digitali (IS-1, IS-2, IS-3)

Gli incidenti per perdita di **riservatezza** e **integrità non** prevedono **soglie minime**

Quelli per perdita di **disponibilità** vanno notificati in caso di **violazione di livelli di servizio attesi**, definiti dai soggetti stessi

La quarta tipologia (IS-4) di incidenti notificati solo dai soggetti essenziali

Codice	Descrizione
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 dei 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. (solo essenziali)

* Obbligo di notifica solo per i soggetti essenziali

Gestione degli incidenti

Partire dai framework noti: NIST SP 800-61 Rev. 3, ISO/IEC 27035 (part. 1-4), CISA Cybersecurity Incident & Vulnerability Response Playbooks

Importante sviluppare o dotarsi di procedure e strumenti efficaci per il rilevamento tempestivo degli eventi cyber e degli incidenti (misure DE-CM-01 e DE.CM-09)

Altri ambiti delle politiche di sicurezza informatica

Le specifiche di base definiscono requisiti in molti altri ambiti delle politiche di sicurezza, che non sono oggetto di questa presentazione:

- Continuità operativa, Disaster Recovery e gestione delle crisi
- Sicurezza della catena di approvvigionamento
- Formazione e Awareness
- Gestione vulnerabilità
- Gestione degli asset
- Affidabilità delle risorse umane
- Gestione dell'autenticazione, delle identità digitali e del controllo accessi
- Sicurezza fisica
- Sicurezza dei dati
- Sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete
- Protezione delle reti e delle comunicazioni
- Monitoraggio degli eventi di sicurezza

… **ci vediamo al webinar (4 dicembre 10:30 – 12:00)**

LEARNING GARR

Conclusioni

Sfida dell'implementazione della NIS impegnativa

Le organizzazioni dovranno investire ingenti risorse umane e finanziarie

Il forte commitment del management voluto dalla normativa è utile in questo senso

Fondamentale sviluppare competenze/strumenti al proprio interno

Non è sempre necessario affidarsi completamente a soluzioni commerciali

Esistono infinite fonti di informazioni (ACN, ENISA, ISO/IEC, NIST) e strumenti open (GRC, RA, CTI, VA, PT, etc.)

Fare comunità per condividere e sviluppare insieme best practices, baseline/framework, strumenti, documentazione …

NIS2: indicazioni operative per la comunità

Per le domande: wooclap.com e codice WSGARR25

WORKSHOP GARR 2025

NET MAKERS

Continuità operativa, Disaster Recovery e gestione delle crisi

Per almeno **i sistemi informativi e di rete rilevanti** sono definiti, attuati e documentati:

- **un piano di continuità operativa** ID.IM-04 punto 1
- **un piano di ripristino in caso di disastro** ID.IM-04 punto 2
- **un piano per la gestione delle crisi** ID.IM-04 punto 3

I piani vanno approvati dal **CdA** ID.IM-04 punto 4 e aggiornati almeno **ogni due anni** ID.IM-04 punto 5

Per tutti i piani vanno chiaramente definiti una serie di aspetti prettamente organizzativi quali:

- finalità e ambito
- ruoli e responsabilità
- canali e procedure di comunicazione (interni ed esterni)
- condizioni di attivazione/disattivazione
- procedure di ripristino post-disaster/crisi
- le risorse necessarie (backup, ridondanze)

Unici requisiti tecnici previsti dalla normativa sono quelli relativi alla corretta gestione dei backup (offline, cifratura, verifica) PR.DS-11 punti 1, 2 e 4 , sempre limitatamente ai sistemi informativi e di rete rilevanti

Sicurezza della catena di approvvigionamento

Le specifiche di base prevedono **5** misure di sicurezza articolate in **8** requisiti (**7** per i soggetti importanti) dedicate alla gestione del rischio della supply chain

Sono circoscritte alla forniture che hanno un potenziale impatto sulla sicurezza dei sistemi informativi e di rete

Introducono una serie di best practice per mitigare i rischi della supply chain, quali:

coinvolgimento dell'organizzazione di cybersecurity nell'affidamento delle forniture e nella definizione di **requisiti di sicurezza** coerenti con le misure di sicurezza delle organizzazioni GV.SC-01 punto 1

mantenimento di un **inventario fornitori** GV.SC-04 punto 1

inclusione del requisiti di sicurezza in rdo, contratti, gare, convenzioni, accordi GV.SC-05 punto 1

esplicita inclusione dei **rischi legati alla supply chain** (impatto interruzione forniture, tempi e costi di ripristino, accesso a sistemi IT, dati e proprietà intellettuale, etc.) nella valutazione del rischio GV.SC-07 punto 1

verifica periodica della **compliance delle forniture** rispetto ai requisiti di sicurezza GV.SC-07 punto 2

per i soli soggetti essenziali sono esplicitati i requisiti di sicurezza da includere nell'affidamento delle forniture (16 ambiti politiche, affidabilità/qualità fornitore, capacità tecnico-economica, sub-appalti, etc.) GV.SC-01 punto 2

Gestione delle vulnerabilità

Le specifiche di base prevedono in tema vulnerabilità **2** misure di sicurezza strutturate in **8** requisiti (di cui **3** specifici per i soli soggetti essenziali)

Le organizzazioni devono definire, attuare e documentare **un piano di gestione delle vulnerabilità** che deve essere approvato dal **CdA** ID.RA-08 punto 4

Il piano deve ID.RA-08 punto 3

- includere le modalità per identificare, monitorare, ricevere, analizzare e rispondere alle vulnerabilità
- definire procedure, ruoli e responsabilità

Allo scopo di identificare le vulnerabilità vanno monitorati almeno i canali di CSIRT Italia, altri CERT e Information Sharing & Analysis Centre (ISAC) ID.RA-01 punto 1 ID.RA-08 punto 1

Le vulnerabilità vanno prontamente risolte tramite aggiornamenti di sicurezza o misure di mitigazione (da documentare nel piano di trattamento del rischio) ID.RA-08 punto 2

Per i soggetti essenziali sono previsti due requisiti aggiuntivi

- esecuzione e documentazione di attività di **VA** e/o **PT** almeno limitatamente ai sistemi informativi e di rete rilevanti prima della loro messa in produzione ID.RA-01 punto 2
- monitoraggio dei canali dei fornitori del software ritenuto critico ID.RA-08 punto 2

Gestione delle vulnerabilità

Il GARR ha sviluppato e messo a disposizione dello comunità uno strumento (**SCARR**) per condurre scansioni di vulnerabilità remote in modo sicuro e flessibile.

SCARR fornisce informazioni dettagliate sulle criticità negli asset della propria rete, offrendo indicazioni e suggerimenti sui possibili rimedi https://scarr.garr.it/

Formazione

Sul tema formazione del personale e consapevolezza, sono previste **2** misure di cui una specifica per i soggetti essenziali.

La prima prevede definizione e attuazione di un **piano di formazione in materia di sicurezza informatica** per **tutti i dipendenti**, incluso il CdA con l'indicazione del calendario dei corsi, i contenuti della formazione e le modalità di verifica dell'apprendimento PR.AT-01 punto 1

Deve essere previsto un **registro** con riportati beneficiari della formazione, contenuti e verifichi finali PR.AT-01 punto 3

Il piano di formazione di cui al punto 1 è approvato dal **Cda** PR.AT-01 punto 2

La seconda misura prevede che i soggetti essenziali eroghino con le stesse modalità una **formazione dedicata al personale specialistico** (es. amministratori di sistemi e di rete) PR.AT-02 punto 1

Anche in questo caso deve essere mantenuto un apposito registro PR.AT-02 punto 1

Sono definiti anche i contenuti di tale formazione specialistica (configurazione/funzionamento sicuri dei sistemi informativi e di rete, minacce informatiche, le istruzioni sulla gestione degli incidenti)

Formazione e Awareness

Curare il «fattore umano» anche in ambito cybersecurity è fondamentale per tutte le organizzazioni

GARR contribuisce con le sue attività di formazione (https://learning.garr.it/) e partecipando ad iniziative come The European Cybersecurity Month (https://cybersecuritymonth.eu/, https://connect.geant.org/2025/09/24/geant-cybersecurity-campaign-2025-cyber-mindfulness-in-the-age-of-ai)