NORMA TECNICA	**Criteri per la qualificazione e certificazione di addetti e responsabili di sicurezza informatica – Requisiti e guida per l'uso**	**NIS CERT 001**

MARZO 2025

Versione italiana

PREMESSA

La presente norma è stata elaborata da un Gruppo di lavoro composto da esperti di sicurezza informatica e professionisti del settore privato. Il Gruppo di lavoro ha dato la sua approvazione il 17/03/2025.

Le presente norma potrà essere soggetta ad aggiunte, modifiche, ampliamenti, nuovi criteri e nuove considerazioni. La norma sarà quindi revisionata, quando necessario, con la pubblicazione di nuove edizioni o di aggiornamenti. È importante, pertanto, che gli utilizzatori della stessa si accertino di essere in possesso dell'ultima edizione e degli eventuali aggiornamenti. Si invitano inoltre gli utilizzatori a verificare l'esistenza di altre norme ove citate nei riferimenti normativi.

INDICE

0 INTRODUZIONE

La Direttiva NIS 2, entrata in vigore il 16 gennaio 2023, rappresenta un significativo avanzamento nel quadro normativo europeo per la sicurezza informatica, sostituendo la precedente Direttiva NIS del 2016. Questo aggiornamento si è reso necessario a causa dell'evoluzione delle minacce cibernetiche e delle crescenti dipendenze digitali che hanno messo in luce vulnerabilità nelle infrastrutture digitali e una disomogeneità nelle misure di sicurezza tra gli Stati membri.

Tra le principali novità introdotte dalla NIS 2 vi è l'ampliamento del campo di applicazione: la direttiva ora copre un numero maggiore di settori, includendo non solo le infrastrutture critiche tradizionali come energia e trasporti, ma anche settori come la sanità, i servizi digitali e la gestione dei rifiuti. Inoltre, sono stati introdotti requisiti di sicurezza più stringenti, obblighi di notifica degli incidenti entro termini specifici e sanzioni più severe per il mancato rispetto delle disposizioni. Un altro cambiamento rilevante è l'eliminazione della distinzione tra Operatori di Servizi Essenziali (OSE) e Fornitori di Servizi Digitali (FSD), sostituita da una classificazione basata su "entità essenziali" e "entità importanti", con obblighi proporzionati alla criticità dei servizi offerti. Queste modifiche mirano a garantire un livello elevato e uniforme di sicurezza delle reti e dei sistemi informativi in tutta l'Unione Europea, promuovendo una maggiore cooperazione e resilienza cibernetica tra gli Stati membri.

In Italia, l'attuazione della NIS 2 è affidata all'Agenzia per la Cybersicurezza Nazionale (ACN), che ha il compito di coordinare le strategie nazionali per la sicurezza informatica e garantire la conformità alle direttive europee. L'ACN svolge un ruolo centrale nella definizione delle misure di sicurezza e nella gestione degli incidenti, assicurando che le entità regolamentate adottino standard adeguati a prevenire e mitigare gli attacchi informatici. L'agenzia opera anche per rafforzare la cooperazione tra settore pubblico e privato, promuovendo la formazione e la certificazione delle competenze in ambito cybersecurity.

Il Decreto Legislativo n. 138 del 4 settembre 2024, emanato a recepimento della Direttiva (UE) 2022/2555, impone ai soggetti interessati (c.d. "soggetti NIS") alcuni obblighi essenziali in materia di governo della cybersicurezza, individuando tre pilastri fondamentali: la formazione e la consapevolezza in tema di cybersecurity a tutti i livelli dell'organizzazione; la gestione e la segnalazione tempestiva degli incidenti di sicurezza; l'adozione di misure di sicurezza – tecniche, operative e organizzative – proporzionate ai rischi. Ulteriori specifiche per l'applicazione della norma sono fornite attraverso la legislazione secondaria formata da DPCM e Decreti del Direttore dell'ACN.

Uno scenario tecnologico in continua evoluzione, la natura mutevole delle minacce informatiche e l'emergere di nuovi rischi per la cybersicurezza impongono uno sviluppo puntuale e una regolamentazione accurata delle competenze richieste per poter indirizzare tali rischi: ciò si traduce nella necessità di definire standard formativi e professionali volti ad assicurare che le figure chiamate ad operare in questo settore dispongano tanto delle competenze tecniche fondamentali quanto della necessaria comprensione dei principi fondamentali sui quali si basa la disciplina NIS 2. L'istituzione di una certificazione professionale basata su requisiti uniformi rappresenta un passo essenziale per assicurare lo sviluppo responsabile e sostenibile della sicurezza informatica.

1 SCOPO E CAMPO DI APPLICAZIONE

La presente norma ha lo scopo di definire in modo chiaro e preciso i criteri e i requisiti necessari per alcune figure professionali operanti nel settore della sicurezza informatica. Essa descrive i percorsi formativi richiesti e i requisiti professionali che tali figure devono dimostrare di possedere per soddisfare gli standard specificati.
La presente norma può essere utilizzata come punto di riferimento dalle figure professionali che desiderano attestare le proprie competenze e qualifiche, rendendole visibili e riconosciute all'esterno. Inoltre, essa è destinata alle organizzazioni di qualsiasi tipo e dimensione, offrendo loro una guida per determinare e verificare le qualifiche del personale necessario a ricoprire specifiche posizioni nell'ambito della sicurezza informatica. L'adozione di questa norma permette di garantire un elevato livello di professionalità e competenza, promuovendo la crescita e lo sviluppo sostenibile del settore.

2 RIFERIMENTI NORMATIVI

Il presente documento contiene i seguenti riferimenti normativi:

- Norma UNI CEI EN ISO/IEC 17024:2012 "Requisiti generali per organismi che eseguono la certificazione di persone".
- Direttiva (UE) 2022/2555 (c.d. "NIS 2") relativa a misure per un livello comune elevato di cibersicurezza nell'Unione.
- Decreto Legislativo n. 138 del 4 settembre 2024, emanato a recepimento della Direttiva (UE) 2022/2555.
- Determinazioni del Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale.
- Regolamento NIS Cert per la certificazione di addetti e responsabili di sicurezza informatica.

3 TERMINI E DEFINIZIONI

Alla presente Norma si applicano i termini e le definizioni riportati dalla norma UNI CEI EN ISO/IEC 17024.
Processo di certificazione: Attività mediante le quali un organismo di certificazione stabilisce che una persona soddisfa i requisiti di certificazione, compresi la domanda, la valutazione, la decisione relativa alla certificazione, il rinnovo della certificazione e l'utilizzo di certificati e di loghi/marchi.
Schema di certificazione: Competenze e altri requisiti relativi a specifiche professioni o a categorie di persone specializzate aventi qualifiche o specifiche abilità.
Requisiti di certificazione: Insieme di requisiti specificati, comprendenti i requisiti dello schema da soddisfare al fine di rilasciare o mantenere la certificazione.
Proprietario dello schema: Organizzazione responsabile per l'elaborazione e il mantenimento di uno schema di certificazione.
Certificato: Documento emesso da un organismo secondo le disposizioni della norma internazionale sopra citata, indicante che la persona nominata ha soddisfatto i requisiti di certificazione.

Competenza: Capacità di applicare conoscenze e abilità al fine di conseguire i risultati prestabiliti.
Qualifica: Livello di istruzione, formazione ed esperienza di lavoro dimostrati, ove applicabile.
Valutazione: Processo che permette di valutare se una persona possiede i requisiti dello schema di certificazione.
Esame: Attività che fanno parte della valutazione, che permettono di misurare la competenza di un candidato mediante uno o più mezzi quali prove scritte, orali, pratiche o osservazione diretta, come definiti nello schema di certificazione.
Esaminatore: Persona che ha competenza per condurre un esame e, ove tale esame richieda un giudizio professionale, valutarne i risultati.
Sorvegliante: Persona autorizzata dall'organismo di certificazione che gestisce o sovrintende ad un esame, ma che non valuta la competenza del candidato.
Personale: Persone, interne o esterne all'organismo di certificazione, che eseguono attività per conto dell'organismo di certificazione.
Richiedente: Persona che ha presentato una domanda per essere ammessa al processo di certificazione.
Candidato: Richiedente che possiede i prerequisiti specificati ed è stato ammesso al processo di certificazione.
Imparzialità: Presenza di obiettività. L'obiettività implica l'assenza di conflitti di interessi, o che questi siano stati risolti in modo da non influenzare negativamente le successive attività dell'organismo di certificazione.
Equità: Uguale opportunità di successo garantita a ciascun candidato nel processo di certificazione.
Validità: Evidenza che la valutazione misuri ciò che si intende misurare, come definito dallo schema di certificazione.
Affidabilità: Indicatore della misura in cui i punteggi dell'esame sono coerenti nelle diverse sessioni d'esame, nelle differenti forme di esame e con differenti esaminatori.
Ricorso, appello: Richiesta da parte di un richiedente, candidato, o persona certificata, di riconsiderare qualsiasi decisione presa dall'organismo di certificazione relativa alla certificazione da lui/lei desiderata.
Reclamo: Espressione d'insoddisfazione, diversa dal ricorso, manifestata da una persona o da una organizzazione a un organismo di certificazione, relativa alle attività di tale organismo o di una persona certificata, per la quale è attesa una risposta.
Parte interessata: Persona, gruppo o organizzazione influenzati dalle prestazioni di una persona certificata o dell'organismo di certificazione.
Sorveglianza: Monitoraggio periodico, durante i periodi di validità della certificazione, delle prestazioni di una persona certificata per garantire che mantenga la conformità allo schema di certificazione.

4 PREREQUISITI

Ai fini dell'ammissione ai percorsi formativi di livello I (Addetto alla sicurezza NIS) e di livello II (Responsabile attuazione NIS), è richiesto il possesso di requisiti minimi di conoscenza.
I prerequisiti di carattere operativo, pur essendo riportati nel paragrafo dedicato al livello I, costituiscono requisito obbligatorio per l'accesso a entrambi i livelli.
I prerequisiti di carattere organizzativo, invece, sono specifici per il livello II e sono riportati esclusivamente nel relativo paragrafo.

4.1 Livello I (Addetto alla sicurezza NIS)

- Conoscenza dei principi della normativa NIS, inclusi gli elementi di novità introdotti con la NIS 2.
- Conoscenze fondamentali sui sistemi operativi (file system, utenti, permessi, comandi base).
- Nozioni di reti informatiche (modello TCP/IP, protocolli principali quali HTTP, DNS, DHCP, SMTP).
- Concetti di base della sicurezza informatica (riservatezza, integrità, disponibilità, autenticazione, non-ripudio).
- Conoscenze generali delle architetture IT (modelli distribuiti client server, concetti di virtualizzazione e cloud computing).
- Familiarità con i principali tipi di minacce informatiche (malware, phishing, ransomware, attacchi brute-force, attacchi DDoS, ecc.).

4.2 Livello II (Responsabile attuazione NIS)

- Tutti i requisiti richiesti per il livello I.
- Conoscenza degli obblighi imposti dalla normativa NIS, inclusi gli elementi di novità introdotti con la NIS 2.
- Conoscenza dei concetti fondamentali sulla governance e la sicurezza IT (policy, processi, procedure, matrici di ruoli e responsabilità, ecc.).
- Familiarità con i concetti di base sulla gestione del rischio (identificazione, valutazione e trattamento dei rischi informatici; terminologia).
- Familiarità con i principali riferimenti normativi ulteriori rispetto a NIS 2 (norme cogenti quali DORA e GDPR, standard volontari quali ISO/IEC 27001).
- Conoscenza dei concetti fondamentali delle verifiche di conformità (preparazione e conduzione di audit, raccolta e preservazione di evidenze, redazione di audit report, ecc.).

5 CONOSCENZE

Ogni livello di qualifica prevede un percorso formativo che integra e applica i principali concetti di governance della sicurezza informatica e gestione del rischio a contesti organizzativi concreti e infrastrutture digitali esistenti.
Gli argomenti trattati nei corsi di livello I, Addetto alla sicurezza NIS, e II, Responsabile attuazione NIS, sono di seguito riportati.

5.1 Livello I (Addetto alla sicurezza NIS)

- Basi della cybersecurity e le principali minacce informatiche.
- Misure di sicurezza operative per proteggere i sistemi informatici e le informazioni.
- Riconoscimento e gestione appropriata degli incidenti di sicurezza.
- Framework di sicurezza ACN e misure richieste per la conformità alla NIS2.

5.2 Livello II (Responsabile attuazione NIS)

- Definizione e implementazione di una strategia di cybersecurity aziendale.

- Basi della cybersecurity e le principali minacce informatiche.
- Valutazione e gestione dei rischi informatici attraverso metodologie strutturate.
- Supervisione della sicurezza delle infrastrutture IT e OT.
- Gestione efficace di incidenti e crisi di sicurezza, per garantire un'escalation e una risposta coordinate.

6 ESPERIENZA

Oltre al superamento del corso per la dimostrazione della conoscenza, come da capitolo 5, il candidato deve dimostrare di possedere almeno due dei requisiti di esperienza di seguito riportati.

6.1 Livello I (Addetto alla sicurezza NIS)

- Esperienza tecnica in ambito IT (operatore help desk, amministratore di sistema, amministratore di rete, operatore cybersecurity di primo livello).
- Partecipazione ad attività di monitoraggio della sicurezza informatica (controllo log firewall, verifica alert sistemi anti-malware, analisi eventi di sistema).
- Coinvolgimento in attività di gestione delle identità digitali e dei permessi di accesso alle risorse.
- Partecipazione a esercitazioni di risposta a incidenti o gestione eventi di sicurezza informatica.
- Familiarità con la gestione di strumenti e piattaforme di sicurezza (SIEM, IPS/IDS, EDR).

6.2 Livello II (Responsabile attuazione NIS)

- Ruoli di responsabilità nella conduzione di infrastrutture IT, nell'erogazione di servizi IT, o nella gestione di centri per la sicurezza operativa (SOC).
- Partecipazione ad audit o attività di preparazione alla conformità normativa (ISO/IEC 27001, GDPR, D.lgs. 138/2024).
- Coinvolgimento diretto nella definizione di strategie per la cybersicurezza o nella gestione del rischio IT.
- Esperienza nella gestione di crisi di sicurezza e di incidenti complessi (analisi, escalation, recovery).
- Coinvolgimento in progetti di sicurezza IT su infrastrutture critiche o servizi essenziali.

7 COMPETENZE

Al termine del processo di certificazione, i candidati saranno in grado di dimostrare una serie di competenze specifiche che li renderanno qualificati per operare nel campo della sicurezza informatica. Le competenze in uscita riflettono la capacità dei candidati di applicare le conoscenze apprese e l'esperienza professionale conseguita a situazioni reali e problemi complessi.

Sono di seguito elencate le competenze chiave che i candidati saranno in grado di dimostrare una volta completato con successo il processo di certificazione di livello I, Addetto alla sicurezza NIS, e II, Responsabile attuazione NIS.

7.1 Livello I (Addetto alla sicurezza NIS)

- Fondamenti di cybersecurity e minacce informatiche.
- Gestione della sicurezza operativa e protezione delle informazioni.
- Gestione degli incidenti di sicurezza secondo tassonomia ACN.
- Misure di sicurezza (Control Framework) promosse dalla ACN.

7.2 Livello II (Responsabile attuazione NIS)

- Strategia e governance della cybersecurity.
- Gestione del rischio e compliance normativa.
- Supervisione della sicurezza delle infrastrutture IT e OT.
- Gestione delle crisi e degli incidenti di sicurezza.