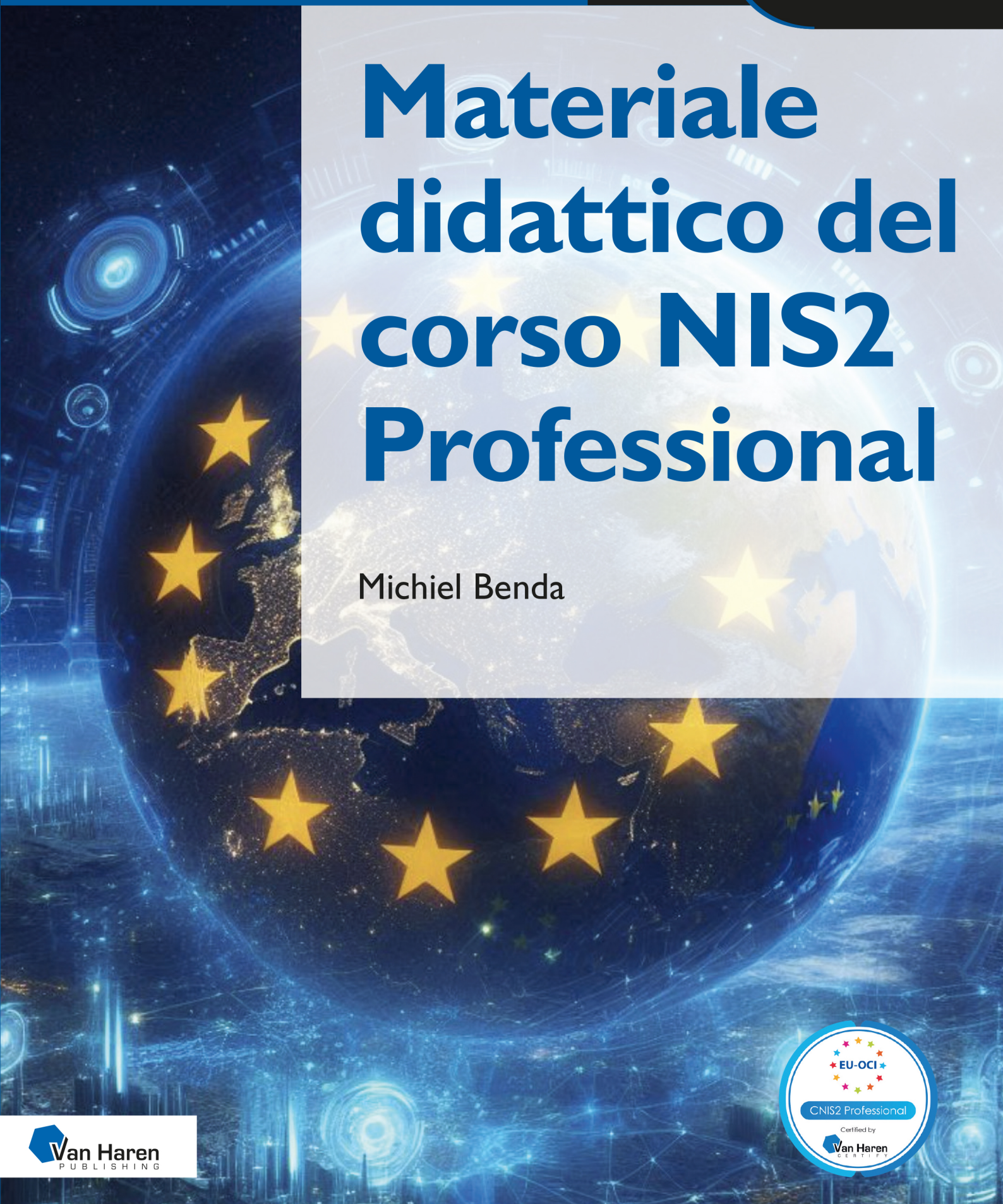
COURSEWARE

Materiale didattico del corso NIS2 Professional

Michiel Benda



Van Haren PUBLISHING

EU-OCI
CNIS2 Professional
Certified by
Van Haren CERTIFY

Materiale didattico del corso

NIS2 Professional

v1.0

Colophon

Titolo:	Materiale didattico del corso NIS2 Professional
Autore:	Michiel Benda
Tradutorre:	Nicolò Reale
Editore:	Van Haren Publishing, ‘s-Hertogenbosch
ISBN copia cartacea:	978 94 018 1306 8
Edizione:	Prima edizione, prima stampa, Marzo 2025
Progetto:	Van Haren Publishing, ‘s-Hertogenbosch
Copyright:	© Van Haren Publishing 2025
	Per ulteriori informazioni su Van Haren Publishing potete scrivere all’indirizzo: info@vanharen.net o visitare il sito: www.vanharen.ne

Note dell’Editore sul materiale del corso

Il materiale del corso è stato creato da esperti del settore che hanno contribuito come autore/i a questa pubblicazione. Il contenuto si basa su pubblicazioni esistenti e sull'esperienza e competenza dell’autore/i. Il materiale è stato revisionato da formatori con esperienza nell’utilizzo del materiale stesso. È stata prestata particolare attenzione ai punti chiave di apprendimento per garantire la comprensione degli elementi da padroneggiare.

L'obiettivo del materiale del corso è fornire il massimo supporto al formatore e allo studente durante il percorso formativo. La struttura modulare del materiale, secondo l'autore/i, offre le migliori possibilità di successo per gli studenti che scelgono di sostenere l'esame.

Per questo motivo il materiale è accreditato, ove applicabile. Per soddisfare i requisiti di accreditamento il materiale deve rispettare determinati standard di qualità. La struttura, l’uso di determinati termini, i diagrammi e i riferimenti fanno tutti parte dell’accreditamento. Inoltre il materiale deve essere reso disponibile a ciascuno studente per ottenere l’accreditamento completo. Per supportare al meglio il formatore e il partecipante il materiale include esercitazioni, esami di prova e risultati.

Riferimenti diretti alla letteratura consigliata sono spesso presenti nelle slide per consentire agli studenti di trovare ulteriori informazioni su un argomento specifico. La scelta di escludere pagine di note dal materiale è stata presa per incoraggiare gli studenti a prendere appunti lungo il percorso.

Anche se il materiale è completo esiste la possibilità che il formatore si discosti dalla struttura delle slide o scelga di non fare riferimento a tutte le slide o istruzioni. Lo studente ha sempre la possibilità di esplorare autonomamente tali argomenti. Si raccomanda di seguire la struttura del materiale e delle pubblicazioni per una preparazione ottimale all'esame.

Il materiale del corso e la letteratura consigliata rappresentano la combinazione ideale per apprendere e comprendere la teoria.

-- Van Haren Publishing

Altre pubblicazioni di Van Haren Publishing

Van Haren Publishing (VHP) è specializzata in titoli relativi a Best Practice, metodi e standard in quattro ambiti:

- IT e gestione IT
- Architettura (Enterprise e IT)
- Gestione aziendale
- Gestione dei progetti

Van Haren Publishing pubblica anche per conto di organizzazioni e aziende leader: ASLBiSL Foundation, BRMI, CA, Centre Henri Tudor, Gaming Works, IACCM, IAOP, IFDC, Innovation Value Institute, IPMA-NL, ITSqc, NAF, KNVI, PMI-NL, PON, The Open Group, The SOX Institute.

Argomenti trattati (per ambito):

IT e Gestione IT

ABC of ICT
ASL®
CATS CM®
CMMI®
COBIT®
e-CF
ISO/IEC 20000
ISO/IEC 27001/27002
ISPL
IT4IT®
IT-CMF™
IT Service CMM
ITIL®
MOF
MSF
SABSA
SAF
SIAM™
TRIM
VeriSM™

Enterprise Architecture

ArchiMate®
GEA®
Novius Architectuur Methode
TOGAF®

Gestione Aziendale

BABOK ®Guide
BiSL® and BiSL® Next
BRMBOK™
BTF
EFQM
eSCM
IACCM
ISA-95
ISO 9000/9001
OPBOK
SixSigma
SOX
SqEME®

Gestione dei Progetti

A4-Projectmanagement
DSDM/Atern
ICB / NCB
ISO 21500
MINCE®
M_o_R®
MSP®
P3O®
PMBOK ® Guide
Praxis®
PRINCE2®

Per le informazioni più aggiornate sulle pubblicazioni di VHP visita il nostro sito web: www.vanharen.net

Prefazione

Quando la Direttiva Network and Information Systems (NIS2) è stata pubblicata a dicembre 2022, era chiaro che avrebbe avuto un impatto significativo in Europa. Per molte aziende è stata uno stimolo:

A. A comprendere che avrebbero dovuto migliorare la propria gestione della sicurezza delle informazioni;

B. A preparare una nuova linea di servizi per aiutare le organizzazioni a conformarsi alla Direttiva;

C. A iniziare a informare persone e organizzazioni sui contenuti della NIS2 e su cosa avrebbe significato per loro.

Il punto C ha portato a una vasta gamma di corsi, webinar, seminari, tavole rotonde e altro ancora. Il materiale formativo che state leggendo si distingue dagli altri per una combinazione di diversi fattori:

1. Spiega i requisiti elencati nella Direttiva tracciandone il significato e l'intento attraverso i numerosi Considerando presenti nella Direttiva e riferimenti ad altre pubblicazioni legali dell'UE. Ad esempio invece di limitarsi a dichiarare che è necessario implementare la sicurezza delle risorse umane come specificato nell'Articolo 21(2i), questo corso spiega cosa intende la NIS2 per questo requisito, tracciandone le specifiche fino al Considerando 79 e alla Direttiva UE 2022/2557.

2. Illustra i requisiti della NIS2 in termini semplici, evitando il gergo tecnico a meno che la Direttiva non si riferisca esplicitamente al termine stesso. In questi casi il termine sarà spiegato in modi quanto più lontani possibile dalla tecnologia. Questo corso è rivolto a coloro che svolgono un ruolo nella governance della sicurezza delle informazioni e nella conformità alla Direttiva e non richiede una conoscenza tecnica approfondita.

3. Fornisce i mezzi per valutare la propria organizzazione rispetto ai requisiti della NIS2. Man mano che si affrontano i requisiti si annoterà il proprio stato (stimato) di conformità sul modulo di valutazione GAP. Al termine del corso si avrà una valutazione ad alto livello del proprio stato di conformità, insieme a un punteggio complessivo dell'organizzazione. La valutazione GAP suggerirà inoltre un chiaro insieme di azioni da intraprendere per raggiungere la piena conformità.

4. Combina questo materiale formativo con un corso di due giorni erogato da formatori certificati che hanno una conoscenza approfondita della sicurezza delle informazioni e della Direttiva NIS2. Il corso consente di sostenere un esame per ottenere l'ambita certificazione CNIS2 che attesterà la comprensione dei requisiti della Direttiva e la preparazione a supportare l'organizzazione nell'ottenere la conformità.

5. Fornisce approfondimenti sulla Direttiva da una prospettiva europea piuttosto che statunitense. L'intero corso e l'esame sono scritti e revisionati da esperti europei del settore della sicurezza delle informazioni. La certificazione CNIS2 è rilasciata e controllata da un'organizzazione di accreditamento interamente europea.

Informazioni sull’autore

Michiel Benda è un professionista affermato con oltre 30 anni di esperienza in privacy, IT e sicurezza delle informazioni. Il suo percorso è iniziato nella gestione alberghiera, per poi spostarsi rapidamente verso l'automazione dei processi e i servizi IT. Nei servizi IT, Michiel ha rapidamente scalato i ruoli di ingegneria e gestione IT fino a diventare Direttore IT per una grande azienda multinazionale.

Riconoscendo l'importanza crescente della protezione delle informazioni, Michiel ha orientato la sua carriera verso la sicurezza delle informazioni. Ha progettato e implementato robuste misure di sicurezza per aziende in tutto il mondo, da piccole imprese a grandi aziende con migliaia di dipendenti, senza mai compromettere le priorità e l'operatività aziendali.

Nel 2017, spinto dal desiderio di aiutare più organizzazioni, Michiel ha fondato Omni-U. La sua visione è quella di permettere a qualsiasi organizzazione, indipendentemente dalle dimensioni o dalla conoscenza e competenza in sicurezza delle informazioni, di proteggere le proprie operazioni e obiettivi aziendali dalle minacce alla sicurezza informatica. Michiel è un esperto di governance della sicurezza delle informazioni e gestione del rischio.

Il corso di formazione e il materiale didattico CNIS2 Professional riflettono l'impegno di Michiel verso la visione di Omni-U. Attingendo alla sua vasta esperienza, il corso offre approfondimenti pratici, strategie e consigli per orientarsi nella complessità della Direttiva NIS2. Che tu sia un professionista del settore, un legislatore o un appassionato di cybersicurezza, l’esperienza di Michiel evidenzierà il percorso verso un ambiente digitale più sicuro.

Michiel vive nella tranquilla zona boschiva della Veluwe nei Paesi Bassi, dove bilancia il suo impegno per un mondo migliore e più sicuro con una vita personale arricchita da una famiglia amorevole, amici e una passione per catturare il mondo attraverso l’obiettivo della sua macchina fotografica.

Michiel Benda: Fondatore di Omni-U e 0-Effort Solutions, Esperto di Sicurezza delle Informazioni e Autore.

Avvertenza

Le informazioni contenute in questo manuale forniscono una spiegazione della Direttiva NIS2 e delle sue aspettative. Non dovreste agire, implementare cambiamenti o eseguire idee, suggerimenti o concetti presenti in questo manuale o nel corso senza una dovuta considerazione e valutazione delle circostanze specifiche dell'organizzazione in cui intendete applicarli.

Sia il corso che questo manuale sono destinati esclusivamente ad aiutare a valutare la propria organizzazione rispetto ai requisiti della Direttiva e a fornire una comprensione su come raggiungere la conformità. Né il corso né il materiale formativo sono intesi a fornire un'interpretazione legale della Direttiva. Eventuali dubbi in merito a tali interpretazioni dovrebbero essere sottoposti a un consulente legale interno o esterno.

Note di chiarimento

Per motivi di leggibilità questo manuale si riferirà alla Direttiva 2022/2555 come “NIS2” o semplicemente “Direttiva”.

Il manuale spesso si riferisce direttamente a “voi”, a cosa “voi” dovreste fare o a cosa significa qualcosa per “voi”. In questi casi, “voi” si riferisce a voi come rappresentanti della vostra organizzazione piuttosto che a voi come individui. Una “organizzazione” è qualsiasi entità giuridica che deve rispettare i requisiti della NIS2. Può essere un ente governativo, un istituto nazionale, una società, una fondazione, un lavoratore autonomo, un'azienda privata o qualsiasi altra entità che potrebbe dover applicare le regole stabilite in questa Direttiva.

Scopo

…i membri degli organi direttivi dei soggetti essenziali e importanti siano tenuti a seguire una formazione…per far sì che questi acquisiscano conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi di cybersicurezza e il loro impatto sui servizi offerti dal soggetto.

NIS2, Articolo 20, paragrafo 2

In qualità di dirigenti di organizzazioni che rientrano nell'ambito della Direttiva NIS2, siete tenuti a seguire una formazione adeguata per prendere decisioni informate sulle pratiche di cybersicurezza della vostra organizzazione. Questo corso è progettato per soddisfare tale requisito.

Come dirigenti il vostro tempo è prezioso. Sebbene la formazione sia importante, ciò che probabilmente volete davvero sapere è se siete conformi ai requisiti della Direttiva. Questo corso è concepito per rispondere a entrambe le esigenze.

Questo manuale supporta il corso di certificazione CNIS2. Sia il corso che il manuale hanno l'obiettivo di aiutarvi a prepararvi alla conformità con la Direttiva NIS2.

La Direttiva NIS2 è un'istruzione agli Stati membri dell'UE per creare una legge nazionale. Le direttive includono gran parte di ciò che conterranno le leggi nazionali definitive, ma lasciano spazio per interpretazioni locali/nazionali. Per conformarsi alle leggi nazionali che verranno redatte potrebbe essere necessario rispettare requisiti aggiuntivi inseriti da ciascun singolo Stato membro nella legislazione derivata dalla NIS2.

Questo manuale si concentra sulle implicazioni pratiche della Direttiva e su cosa devono fare per soddisfarne l'intento le organizzazioni che devono conformarsi alla Direttiva. È scritto per i membri degli organi direttivi, inclusi il responsabile della sicurezza delle informazioni e il responsabile della protezione dei dati, per fornire una guida pratica sui requisiti della Direttiva. Il manuale vi aiuterà a valutare e prepararvi alla conformità di base alla Direttiva in modo strutturato e facilmente comprensibile.

La formazione associata a questo manuale è inoltre supportata dal libro "The NIS2 Navigator’s Handbook: Bridging the cybersecurity GAP". Il libro approfondisce molti dei temi trattati nel corso per offrire a coloro che perseguiranno attivamente la conformità alla NIS2 una visione più dettagliata della legge e della sua interpretazione. Il libro include anche un'analisi GAP più dettagliata per una comprensione ancora più chiara di ciò che deve essere fatto nella vostra organizzazione per ottenere la conformità.

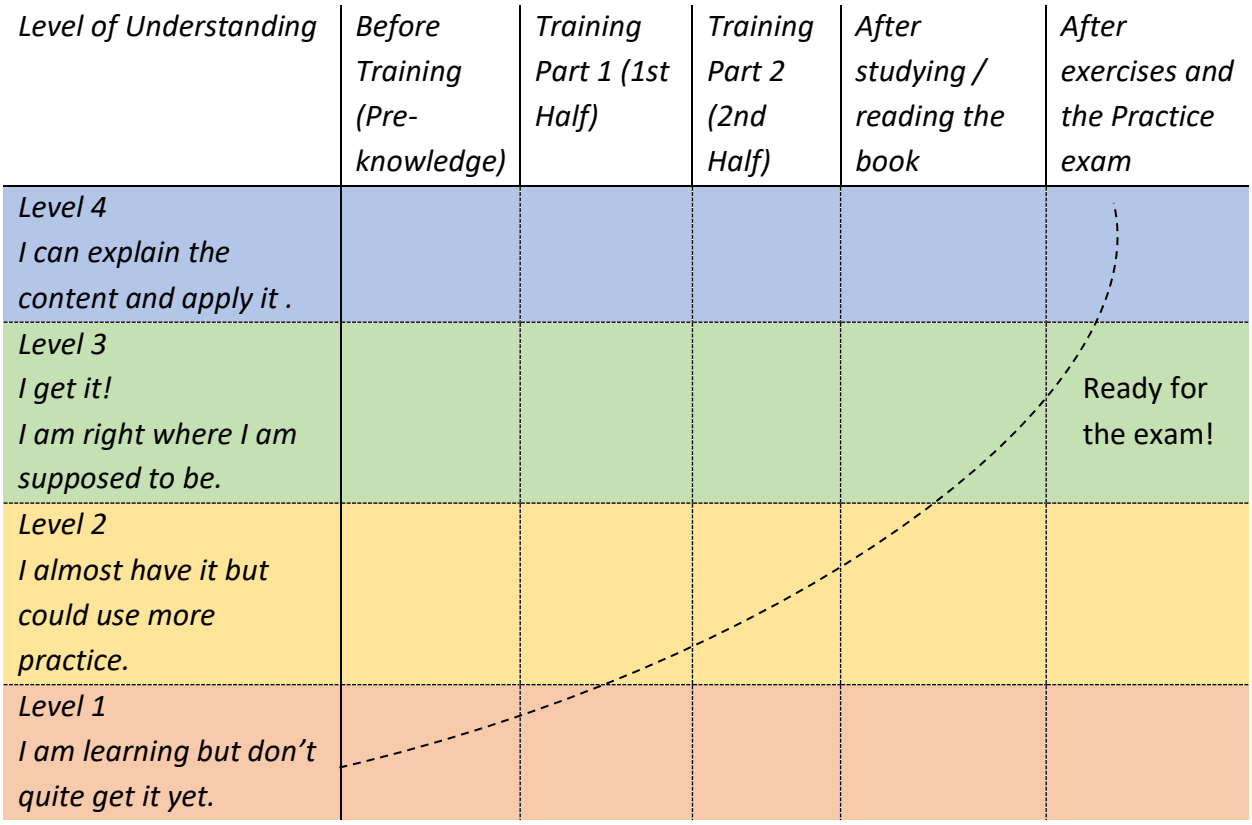
Indice dei contenuti

Self-Reflection of understanding Diagram

‘*What you do not measure, you cannot control*.’’ – Tom Peters

Fill in this diagram to self-evaluate your understanding of the material. This is an evaluation of how well you know the material and how well you understand it. In order to pass the exam successfully you should be aiming to reach the higher end of Level 3. If you really want to become a pro, then you should be aiming for Level 4. Your overall level of understanding will naturally follow the learning curve. So, it’s important to keep track of where you are at each point of the training and address any areas of difficulty.

Based on where you are within the Self-Reflection of Understanding diagram you can evaluate the progress of your own training.



(Self-Reflection of Understanding Diagram)

Write down the problem areas that you are still having difficulty with so that you can consolidate them yourself, or with your trainer. After you have had a look at these, then you should evaluate to see if you now have a better understanding of where you actually are on the learning curve.

Troubleshooting

Problem areas:	*Topic:*
Part 1	
Part 2	
You have gone through the book and studied.	
You have answered the questions and done the practice exam.	

Agenda

Giorno 1: Le basi della Direttiva NIS2

- Contesto dei programmi della UE
- Panoramica della Direttiva NIS2
- Concetti di sicurezza nella NIS2
- Enti e istituzioni pubbliche
- Obblighi dei soggetti
- Supervisione e imposizione
- Ruoli e responsabilità

Giorno 2: Valutazione del GAP

- Spiegazione della valutazione del GAP
- Programma di cybersicurezza
- Formazione sulla sicurezza informatica
- Gestione del rischio
- Politiche
- Pianificazione della resilienza
- Controlli organizzativi
- Controlli tecnici

Syllabus

Certified NIS2 Professional (CNIS2)

Versione 1.0

Questo materiale contiene diagrammi e informazioni testuali basate su:

The NIS2 Navigator’s Handbook: Bridging the Cybersecurity Gap ©Van Haren Publishing

Informazioni sul Certified NIS2 Professional (CNIS2)

Con l'aumento della rilevanza dei rischi informatici nei profili di rischio delle organizzazioni è richiesto che i membri dei vertici aziendali comprendano tali rischi e prendano decisioni informate che considerino l'impatto non solo sull'organizzazione stessa, ma anche sui destinatari finali dei loro prodotti e servizi.

Proprietà Intellettuale:	EU Organisational Compliance Institute
Istituto di Accreditamento:	Van Haren Certify
Istituto Esaminatore:	certN

La direttiva Network and Information Systems del 2022 (NIS2 Directive) sottolinea l'importanza di questa consapevolezza e coinvolgimento da parte dei vertici aziendali, richiedendo che si impegnino attivamente nella gestione del rischio informatico e nell'implementazione delle misure per rendere questi rischi accettabili.

Il corso Certified NIS2 Professional offre una panoramica della Direttiva NIS2 per i membri del management aziendale, siano essi Chief Information Security Officers, Chief Risk Officers, Chief Executive Officers o altri membri del team gestionale. Il corso è unico in quanto è strutturato appositamente per queste figure, per le quali il tempo è un bene prezioso. Il primo giorno fornisce una panoramica generale della Direttiva, mentre il secondo giorno guida i partecipanti in una valutazione NIS2 della propria organizzazione. Al termine del corso i partecipanti avranno non solo compreso il significato della NIS2, ma anche cosa implica per loro e quali azioni intraprendere per conformarsi alla normativa.

Definizione della Certificazione

La certificazione CNIS2 attesta la comprensione della Direttiva, incluse le misure prescritte, e verifica la conoscenza dei concetti base della sicurezza delle informazioni, consentendo al candidato di discutere le misure di gestione del rischio informatico con coloro che sono incaricati della loro implementazione e manutenzione.

Come ottenere la certificazione

I candidati possono ottenere la certificazione superando l'esame Certified NIS2 Professional.

I voucher per l'esame di certificazione sono disponibili tramite formatori accreditati e il gruppo Van Haren.

Rinnovo della certificazione

La certificazione CNIS2 Professional è valida a tempo indeterminato.

Il certificato rilasciato dopo il superamento dell'esame riporta la data di emissione e indica anche la durata della validità della certificazione.

Formato dell'esame

A questo esame si applicano le regole generali sugli esami.

Tentativi per ogni voucher:	1
Numero di domande:	40
Punteggio minimo per superare l'esame:	60%
Punteggio minimo per superare l'esame per i docenti:	75%
Tempo a disposizione:	60 min.
Esame a libro aperto:	No
Lingua:	Italiano
Supervisione:	Si
Tipo di domande:	A scelta multipla

Syllabus dell'esame

Questa tabella riepiloga gli argomenti trattati nell'esame di certificazione.

Modulo	Requisito d'esame	Specifica d'esame	Livello Bloom	Peso %	Libro	Courseware
1	Contesto			10%		
1.1		Cybersicurezza nell'Unione	1		Cap. 2.1-2.4	Cap. 1.1
1.2		Strategie e programmi di cybersicurezza nella UE			Cap. 2.2	Cap. 1.2-1.5
1.3		Il quadro normativo dell'UE			Cap. 2.4.2	Cap. 1.6
2	Struttura della Direttiva			15%		
2.1		La Direttiva NIS	1		Cap. 2.2.3, 2.5	Cap. 2.1
2.2		Ambito della NIS2	1		Cap. 3.6-3.7	Cap. 2.2-2.3
2.3		Struttura della NIS2			Cap. 3.1, 3.3	Cap. 2.4
2.4		Enti e istituzioni pubbliche NIS2			Cap. 3.5	Cap. 4
3	Ruoli, responsabilità e obblighi delle entità			15%		
3.1		Ruoli e responsabilità	1 + 2		Cap. 3.10	Cap. 6
3.2		Obblighi delle entità	1		Cap. 3.8	Cap. 5.1-5.4
3.3		Supervisione e applicazione			Cap. 3.9	Cap. 5.5
4	Concetti di sicurezza			10%		
4.1		Concetti di sicurezza di base	2		Cap. 3.4	Cap. 3
5	Misure di gestione del rischio di sicurezza informatica			30%		
5.1		Programma di sicurezza informatica	1		Cap. 4.1	Cap. 7.1
5.2		Gestione del rischio	1		Cap. 4.3	Cap. 7.2
6	Implementazione			20%		
6.1		Misure di implementazione			Cap. 4.2, 4.4-4.8	Cap. 7.3-7.15
6.2		Report alla direzione			Cap. 3.8.2, 3.10.1, 3.10.2	

* Per ulteriori informazioni sui livelli di apprendimento Bloom cliccare qui.

Materiale di riferimento

Il materiale di riferimento per l'esame Certified NIS2 Professional è:

- The NIS2 Navigator's Handbook: Bridging the Cybersecurity Gap
- Autore: Michiel Benda
- Pubblicato da: Van Haren Publishing

Accreditamento dei docenti

Van Haren Learning Solutions organizza l'accreditamento dei docenti per questo programma di certificazione. Maggiori informazioni sul processo di accreditamento sono disponibili sul loro sito web.

1 Contesto

Il 27 dicembre 2022 l'Unione Europea ha pubblicato quattro nuove direttive e regolamenti. Queste quattro pubblicazioni sono strettamente correlate tra loro poiché ciascuna di esse affronta la resilienza organizzativa per i soggetti europei che sono critici per il funzionamento dell'economia dell'Unione Europea e della sua società. Le pubblicazioni sono elencate di seguito.

- **DORA (2022/2554)**
  DORA sta per Digital Operational Resilience Act. È un regolamento introdotto per il settore finanziario. Si concentra sulla resilienza da una prospettiva ICT ampia. I soggetti che devono seguire DORA probabilmente dovranno seguire anche NIS2.
- **Emendamenti basati su DORA (2022/2556)**
  Questa direttiva fornisce aggiornamenti ad altre direttive esistenti per allinearle al regolamento DORA. Modificando queste direttive, l'UE istruisce gli Stati membri ad aggiornare le legislazioni che hanno redatto basandosi sulle direttive menzionate.
- **Direttiva NIS2 (2022/2555)**
  La Direttiva NIS2 sta per Network and Information Systems Directive versione 2. È una direttiva focalizzata sulla resilienza informatica dei soggetti nell'Unione Europea da cui i cittadini dell'UE dipendono maggiormente per la loro sicurezza, protezione e benessere. Succede alla Direttiva NIS del 2016.
- **Direttiva CER (2022/2557)**
  La Direttiva CER sta per Critical Entities Resilience Directive. Affronta la resilienza delle Entità Critiche rispetto a tutti i pericoli, siano essi naturali o causati dall'uomo, accidentali o intenzionali. Affronta la resilienza di un'organizzazione oltre la resilienza informatica e si estende alle minacce fisiche come reati terroristici, sabotaggi e disastri naturali. I soggetti identificati come critici ai sensi della CER sono considerati essenziali ai sensi della NIS2. I requisiti specificati nella NIS2 prevalgono su eventuali requisiti contrastanti nella CER.

Delle quattro pubblicazioni, tre affrontano la resilienza nelle operazioni digitali dell'organizzazione. La sicurezza informatica è al centro di ciascuna di esse.

1.1 Sicurezza informatica nell'Unione Europea

Le tecnologie digitali sono essenziali per la maggior parte dei cittadini e delle imprese dell'UE. Le interruzioni operative potrebbero avere un effetto significativo sul ruolo dell'UE nella società mondiale. La dipendenza dell'Unione da sistemi e soluzioni provenienti da altre regioni del mondo crea una preoccupazione ulteriore che l'UE sia mal equipaggiata per controllare tali interruzioni. Le attività informatiche dannose possono minacciare direttamente la sua economia e i suoi cittadini. In alcuni casi, queste attività dannose possono persino cercare di minare la coesione e il funzionamento della democrazia in Europa.

La sicurezza informatica è stata nell'agenda dell'UE dall'inizio del secolo. È considerata fondamentale per la resilienza, la sicurezza e l'affidabilità dell'infrastruttura digitale, dei servizi e dell'economia dell'Europa.

La sicurezza informatica è cruciale per il futuro dell'UE per diversi motivi:

- **Le infrastrutture critiche devono essere protette.**
  Le infrastrutture critiche, come energia, trasporti, sanità e sistemi finanziari, dipendono dalle tecnologie digitali. Il loro funzionamento continuo è essenziale per il benessere dei cittadini dell'UE e per l'economia, nonché per sostenere il funzionamento della società.

- **La competitività economica deve essere mantenuta.**
  Un ambiente digitale sicuro e affidabile è essenziale per mantenere la competitività economica globale. Una buona sicurezza informatica fornisce fiducia e sicurezza nei servizi digitali, che a loro volta alimenteranno l'innovazione, consentiranno la crescita economica e manterranno la competitività.
- **I dati personali e la privacy devono essere protetti.**
  La privacy è una priorità nell'agenda dell'UE. I dati personali devono essere protetti nell'ambiente digitale utilizzando misure di sicurezza informatica robuste per sostenere i diritti e le libertà dei cittadini dell'UE.
- **L'economia dell'UE deve essere difesa dalle minacce informatiche.**
  La sicurezza informatica è una parte critica delle difese dell'UE contro le minacce informatiche come il crimine informatico, gli attacchi sponsorizzati da stati esteri e lo spionaggio informatico. Man mano che queste minacce evolvono i meccanismi di difesa informatica dell'UE devono evolversi con esse per proteggere la sicurezza nazionale e mantenere l'integrità delle istituzioni e dei processi dell'UE.
- **I cittadini dell'UE dovrebbero potersi fidare dei servizi digitali ed essere in grado di utilizzarli con sicurezza.**
  Tutti dovrebbero potersi fidare delle tecnologie digitali e sentirsi sicuri nelle loro interazioni digitali. Le misure di sicurezza informatica proteggono gli individui dai rischi informatici, dalle frodi e dagli abusi online, permettendo loro di partecipare pienamente alla società digitale.

1.2 La Strategia di Sicurezza Informatica del 2013

Nel 2013 l'UE ha adottato una strategia di sicurezza informatica che si concentrava sulla costruzione di un ambiente digitale sicuro e affidabile all'interno dell'Unione Europea. La strategia ha delineato cinque priorità.

1. **Rendere le reti e i sistemi informativi resilienti agli attacchi informatici.**
   La strategia raggiunge la resilienza attraverso:
   - Promozione delle pratiche di gestione del rischio;
   - Istituzione di un team di risposta alle emergenze per le istituzioni, gli organismi e le agenzie dell'Unione Europea (il CERT-EU);
   - Coinvolgimento in partenariati tra istituzioni pubbliche e private.
2. **Ridurre la criminalità informatica.**
   La riduzione del crimine informatico viene affrontata attraverso quadri giuridici e leggi, comprese le capacità di farle rispettare.
3. **Definire un quadro politico per la difesa informatica europea.**
   Stabilire un quadro di politica di difesa informatica europea comporta:
   - Miglioramento della cooperazione e della condivisione delle informazioni tra gli Stati membri;
   - Conduzione di esercitazioni di difesa informatica;
   - Supporto alla ricerca e allo sviluppo nel campo della sicurezza informatica.
4. **Potenziare le tecnologie di cybersicurezza dell'UE.**
   Il miglioramento delle risorse industriali e tecnologiche per la sicurezza informatica viene realizzato attraverso:
   - Incoraggiamento della ricerca e dell'innovazione;
   - Promozione dello sviluppo di standard di sicurezza informatica;
   - Supporto alla certificazione di prodotti e servizi.

5. **Creare e mantenere cooperazioni internazionali nel cyberspazio.**
   Le cooperazioni dovrebbero mirare a facilitare un cyberspazio aperto, sicuro e stabile. Le cooperazioni potrebbero essere tra Stati membri e altri Paesi, nonché tra enti pubblici e partner internazionali. Queste cooperazioni contribuirebbero allo sviluppo e alla pubblicazione di norme e standard internazionali per la sicurezza informatica.

Il GDPR è uno dei molti risultati della strategia.

1.3 La Strategia di Sicurezza Informatica per il Decennio Digitale

La Commissione Europea ha deciso di fare degli anni '20 il "Decennio Digitale" dell'Europa. In questo periodo l'Europa deve rafforzare la sua sovranità digitale e stabilire standard, piuttosto che seguire quelli di altre sovranità come gli Stati Uniti, con un chiaro focus su dati, tecnologia e infrastrutture.

Nel dicembre 2020 la Commissione Europea ha presentato la Strategia di Sicurezza Informatica dell'UE per il Decennio Digitale come una revisione della Strategia di Sicurezza Informatica del 2013. La Strategia di Sicurezza Informatica per il Decennio Digitale mira a:

- Sviluppare la sovranità tecnologica dell'UE in materia di sicurezza informatica;
- Costruire capacità per proteggere infrastrutture sensibili come le reti 5G;
- Ridurre la dipendenza da altre parti del mondo per tecnologie cruciali;
- Rafforzare la resilienza dell'Europa contro le minacce informatiche;
- Promuovere la fiducia nell'economia digitale.

Per garantire l'esecuzione efficace della strategia sono indispensabili politiche e investimenti nella sicurezza informatica dell'Unione.

La Strategia di Sicurezza Informatica per il Decennio Digitale ha tre obiettivi principali:

1. Rafforzare la resilienza collettiva dell'UE contro le minacce informatiche;
2. Promuovere un cyberspazio globale e aperto;
3. Far progredire una diplomazia informatica coerente dell'UE.

Essa delinea diverse azioni chiave per raggiungere i suoi obiettivi, tra cui:

- Sviluppare un organismo che rafforzi la risposta dell'UE agli incidenti informatici su larga scala;
- Rafforzare la sicurezza informatica dei settori critici, come energia, trasporti e finanza;
- Migliorare il quadro giuridico per la sicurezza informatica, inclusa la sostituzione della Direttiva NIS;
- Stabilire un quadro globale per il comportamento responsabile degli Stati nel cyberspazio.

1.4 Un'Europa pronta per l'era digitale (Europe Fit for the Digital Age)

Il Programma "Un'Europa pronta per l'era digitale" è stato lanciato dalla Commissione Europea nel dicembre 2019. Il programma può essere visto come un quadro strategico attraverso il quale l'UE riconosce l'importanza della trasformazione digitale e la necessità di adattare e preparare l'Europa e la sua popolazione per le opportunità e le sfide presentate dall'era digitale.

Il quadro comprende varie iniziative, politiche e obiettivi mirati a preparare l'Europa alla trasformazione digitale e a sfruttare il potenziale delle tecnologie digitali a beneficio dei cittadini e dell'economia dell'UE.

Il programma si concentra sulle seguenti priorità chiave:

- **Competenze digitali**: Promuovere l'alfabetizzazione digitale e garantire che gli europei abbiano le competenze necessarie per prosperare nell'era digitale;
- **Infrastrutture digitali**: Espandere la connettività ad alta velocità, comprese le reti 5/6G e l'accesso diffuso alla banda larga, per garantire servizi digitali affidabili e veloci;
- **Economia e società digitali**: Sostenere la crescita dell'economia digitale, promuovere l'innovazione e creare un ambiente favorevole e sicuro per le imprese che adottano tecnologie digitali;
- **Governance digitale**: Stabilire regole e quadri di riferimento chiari per affrontare le sfide digitali emergenti, inclusa la protezione dei dati, la sicurezza informatica e l'uso etico dell'intelligenza artificiale.

1.5 Il Programma Europa Digitale (DIGITAL)

Il Programma Europa Digitale (DIGITAL) è un programma di finanziamento da 7,5 miliardi di euro che mira a raggiungere l'obiettivo di un'Europa climaticamente neutra portando la tecnologia digitale alle imprese, ai cittadini dell'UE e alle amministrazioni pubbliche, ma in particolare alle piccole e medie imprese. Supporta progetti in cinque aree chiave:

1. Supercalcolo;
2. Intelligenza artificiale;
3. Cybersecurity e fiducia;
4. Competenze digitali avanzate;
5. Centri di innovazione digitale.

DIGITAL fornisce supporto finanziario per misure di sicurezza informatica e aggiornamenti tecnologici necessari per la conformità alla NIS2.

1.6 Il quadro normativo dell'UE

Il programma Un'Europa pronta per l'era digitale, il Programma Europa Digitale e la Strategia di Sicurezza Informatica dell'UE richiedono tutti un quadro normativo per migliorare la resilienza e rafforzare la capacità dell'UE di operare indipendentemente da altre nazioni. Il quadro è costituito da diverse direttive e leggi.

1.6.1 Il Regolamento sui mercati digitali (The Digital Markets Act - 2022)

L'Atto promuove mercati digitali più equi. Identifica le grandi piattaforme digitali, come motori di ricerca, app store e servizi di messaggistica, come "intermediari" ("gatekeeper"). Questi intermediari sono soggetti a requisiti specifici, come l'accesso e l'interoperabilità, per garantire una concorrenza leale, il divieto di autopreferenza, la trasparenza e il ranking equo divulgando gli algoritmi di ranking, e il divieto di pratiche che danneggiano la concorrenza.

1.6.2 Regolamento sui servizi digitali (The Digital Services Act - 2022)

L'Atto regola gli intermediari e le piattaforme online, come i marketplace, i social network, le piattaforme di condivisione di contenuti, gli app store e le piattaforme di viaggio online. Mira a prevenire attività illegali e dannose online, ridurre la diffusione della disinformazione e creare un ambiente online equo e aperto.

1.6.3 Direttiva sulle reti e sui sistemi informativi (NIS2: Network and Information Systems Directive - 2023)

Definisce misure per un alto livello comune di sicurezza informatica in tutta l'Unione. La versione rivista (NIS2) è entrata in vigore il 16 gennaio 2023.

1.6.4 Direttiva sulla Resilienza delle Entità Critiche (The Critical Entities Resilience Directive - 2023) - CER

La Direttiva migliora la resilienza dei soggetti che forniscono servizi vitali per le funzioni sociali e le attività economiche. La direttiva garantisce che queste entità possano prevenire, resistere, assorbire e riprendersi dalle interruzioni, come pericoli naturali, terrorismo, minacce interne, sabotaggi ed emergenze sanitarie.

1.6.5 Il Regolamento sulla Resilienza Operativa Digitale (DORA: Digital Operational Resilience Act - 2023)

L'Atto rafforza la sicurezza IT per i soggetti finanziari come banche, assicurazioni e società di investimento. Armonizza le regole per 20 tipi di entità finanziarie e fornitori di servizi ICT di terze parti, garantendo la loro resilienza durante gravi interruzioni operative.

1.6.6 Portafoglio europeo di identità digitale (The European Digital Identity Wallet - 2023)

Il Portafoglio europeo di Identità Digitale consente ai cittadini di dimostrare la propria identità in tutta l'UE quando accedono ai servizi online, condividono documenti digitali o verificano attributi personali specifici (come l'età) senza rivelare dettagli completi dell'identità. Migliora la sicurezza e i vantaggi sia per gli utenti che per le imprese.

1.6.7 Regolamento sui semiconduttori (The European Chips Act - 2023)

L'Atto mira a rafforzare la leadership tecnologica dell'Europa nelle tecnologie e applicazioni dei semiconduttori. Affronta le carenze globali di semiconduttori e le sfide della catena di approvvigionamento supportando la produzione su larga scala, l'innovazione, la ricerca e le competenze nel settore dei chip.

1.6.8 Regolamento sull'intelligenza artificiale (The Artificial Intelligence Act - 2024)

L'Atto mira a stabilire regole armonizzate per l'intelligenza artificiale (AI) all'interno dell'Unione Europea. Affronta sia i benefici che i rischi associati all'AI, garantendo che il suo sviluppo sia in linea con i valori, i diritti fondamentali e i principi dell'UE. L'atto copre definizioni, classificazione dei rischi, divieti, protezione dei diritti, governance e applicazione.

1.6.9 Regolamento europeo sui dati (The European Data Act - 2024)

L'Atto è stato progettato per migliorare l'economia dei dati dell'UE e promuovere un mercato dei dati competitivo. L'Atto rende i dati (ad esempio i dati industriali) più accessibili e utilizzabili, incoraggiando l'innovazione basata sui dati e aumentando la disponibilità dei dati. Uno dei modi in cui l'Atto mira a raggiungere questo obiettivo è chiarendo chi può creare valore dai dati e a quali condizioni. In questo modo contribuisce ad avanzare la trasformazione digitale e a stabilire un mercato unico dei dati nell'UE. Incoraggia la condivisione sicura dei dati tra i settori, a beneficio sia dell'economia europea che della società nel suo complesso.

1.6.10 Il Regolamento sulla resilienza informatica (Cyber Resilience Act - 2024)

L'Atto mira a migliorare la sicurezza informatica per i prodotti e i software con componenti digitali. Impone requisiti di sicurezza informatica per i produttori e i rivenditori, garantendo prodotti più sicuri durante tutto il loro ciclo di vita. Consumatori e imprese beneficiano di una maggiore sicurezza e di scelte informate quando acquistano prodotti con marchio CE.

Panoramica della Direttiva NIS2

2 Basi e struttura della Direttiva NIS2

2.1 La Direttiva NIS del 2016

Nel 2016 è entrata in vigore la Direttiva Network and Information Systems (NIS). Nella maggior parte degli Stati membri la Direttiva è stata adottata nella legislazione locale nel 2018.

L'intenzione della NIS era di stabilire capacità di sicurezza informatica uniformi in tutta l'Unione. Il suo ambito era rivolto ai sistemi informativi e di rete dei soggetti che fornivano servizi essenziali in settori chiave. I servizi essenziali erano considerati quelli che, se interrotti, avrebbero influito significativamente sul funzionamento dell'economia e della società dell'Unione.

La NIS si è dimostrata molto efficace poiché la resilienza informatica dei soggetti coinvolti, sia enti privati che pubblici, è migliorata significativamente. Alcuni dei risultati della NIS sono:

- Il completamento di quadri di riferimento e strategie nazionali sulla sicurezza dei sistemi informativi e di rete;
- L'istituzione di capacità nazionali di sicurezza informatica;
- L'implementazione di misure regolamentari che coprono le infrastrutture essenziali e le entità identificate da ciascuno Stato membro;
- Una migliore cooperazione tra gli Stati membri attraverso l'istituzione del Gruppo di Cooperazione e della rete di team nazionali di risposta agli incidenti di sicurezza informatica.

Dall'adozione della NIS ci sono stati cambiamenti significativi nel mondo e, nonostante i risultati sopra menzionati, le revisioni hanno rivelato carenze intrinseche che impediscono alla NIS di affrontare efficacemente le sfide attuali ed emergenti della sicurezza informatica. Di conseguenza la Strategia di Sicurezza Informatica per il Decennio Digitale ha incluso l'iniziativa di aggiornare la Direttiva NIS.

2.1.1 Carenze della Direttiva NIS

I sistemi informativi e di rete giocano un ruolo sempre più centrale nella vita quotidiana. Le trasformazioni digitali, gli scambi transfrontalieri e le interazioni sociali digitali senza confini sono diventati gli elementi sociali più comuni e attesi. Questa crescita delle opportunità informatiche porta con sé allo stesso tempo una crescita delle minacce informatiche. L'espansione del panorama informatico introduce nuove sfide che richiedono risposte meglio coordinate e innovative.

Dall'adozione della Direttiva NIS, il numero, la magnitudine, la sofisticazione, la frequenza e l'impatto degli incidenti legati alla sicurezza informatica sono cresciuti, spesso in modo esponenziale. Queste minacce informatiche rappresentano una preoccupazione importante per il funzionamento dell'Unione e dei singoli Stati membri. Possono ostacolare le attività economiche, generare perdite finanziarie, minare la fiducia degli utenti e causare danni significativi al funzionamento dell'economia e della società dell'UE. Un programma di sicurezza informatica efficace e la preparazione dei soggetti che contribuiscono al funzionamento dell'economia e della società sono quindi diventati più essenziali che mai per il corretto funzionamento del mercato interno europeo. Questi cambiamenti nel panorama sono insufficientemente affrontati nella Direttiva NIS in diverse aree, inclusa la definizione dei soggetti, dove l'impatto della catena di approvvigionamento è stato sottovalutato, così come gli approcci per affrontare le minacce.

L'insufficienza è causata in parte dalle variazioni nell'implementazione della NIS nei vari Stati membri. Esistono grandi differenze sia nei requisiti che nella supervisione. In alcuni casi le interpretazioni dei

requisiti sono in conflitto tra le implementazioni della NIS dei vari Paesi, il che grava in modo sproporzionato sulle aziende che offrono servizi e prodotti transfrontalieri.

2.1.2 Come la NIS2 migliora la Direttiva NIS

La Direttiva NIS2 è stata introdotta per affrontare le carenze della NIS e per preparare l'Unione a un panorama informatico più dinamico, in modo che la maggior parte dei soggetti operanti nell'Unione possano affidarsi e dipendere ancora di più da tale panorama. Introduce nuovi requisiti per migliorare ulteriormente la resilienza informatica dell'UE e per affrontare l'aumento significativo dell'uso di servizi di terze parti e ambienti di cloud computing.

La Direttiva NIS2 ora migliora la NIS originale attraverso i seguenti punti:

- Sono stati aggiunti nuovi requisiti per affrontare la sicurezza della catena di approvvigionamento;
- Sono stati inclusi requisiti più concreti per affrontare la supervisione da parte degli Stati membri, inclusa una maggiore diligenza nell'imporre sanzioni ai soggetti che non rispettano la Direttiva;
- La classificazione di "Operatore di servizi essenziali" è stata sostituita da due nuove classificazioni di "essenziale" e "importante";
- Molti nuovi tipi di soggetti sono stati aggiunti all'ambito per migliorare la sicurezza e la resilienza dell'UE, tra cui molti dei subappaltatori e fornitori di servizi con accesso a infrastrutture critiche.

Il mandato di applicazione per le autorità è stato esteso significativamente. È stato anche aggiunto un requisito di segnalazione rigoroso in cui i soggetti devono segnalare qualsiasi incidente entro 72 ore, con un avviso preliminare entro 24 ore. Questo consente alle autorità di reagire rapidamente e migliorare la possibilità di contenere la minaccia informatica e limitare il suo impatto sul funzionamento dell'economia e della società il più possibile. In caso di incidente di sicurezza e di rifiuto di cooperare con le autorità, la NIS2 fornisce agli Stati membri il diritto di ingiunzione (essenzialmente costringendo le organizzazioni ad aderire alle istruzioni) o di bypassare la gestione dell'organizzazione per far rispettare le istruzioni. A seconda della classificazione del soggetto che viola le normative, le autorità possono anche emettere multe fino al 2% del fatturato.

2.2 Ambito della NIS2

La NIS2 si applica sia ai soggetti pubblici che privati. La Direttiva ha un elenco di settori e tipi di soggetti (definiti nei suoi Allegati I e II) che sono inclusi nell'ambito se sono almeno medie imprese come descritto nella figura 2.1.

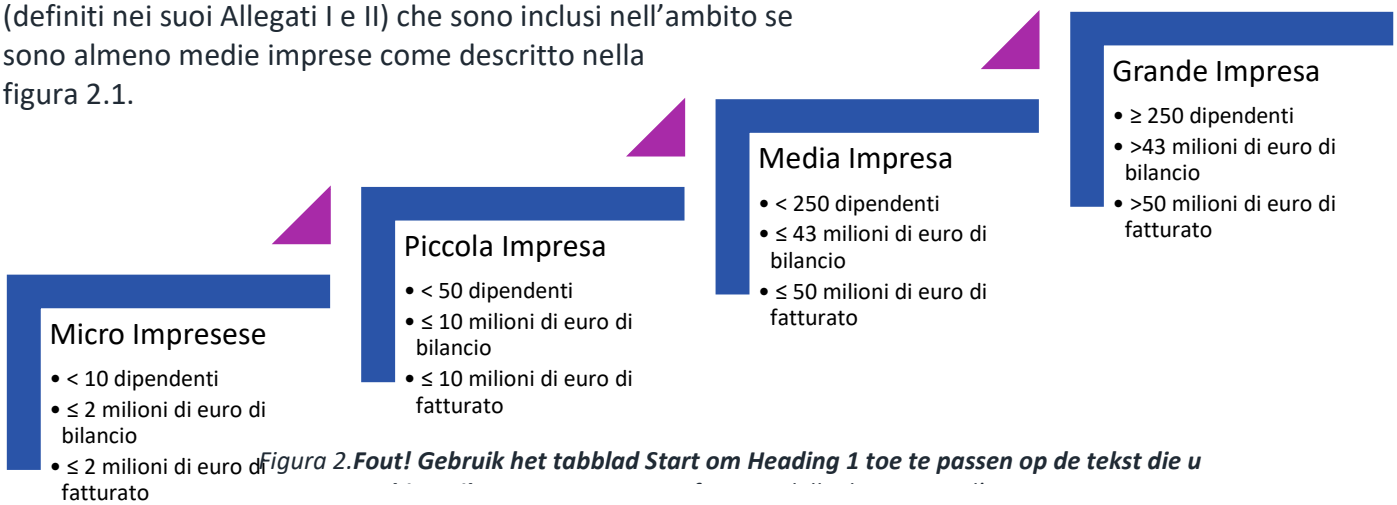


*Figura 2.**Fout! Gebruik het tabblad Start om Heading 1 toe te passen op de tekst die u***

Quando si calcola la dimensione dell'impresa il numero di dipendenti è calcolato in base all'occupazione a tempo pieno e include i contrattisti di terze parti, sebbene escluda i tirocinanti. Chiunque lavori part-time è calcolato in base alla quantità relativa di tempo che lavora. Ci sono ulteriori considerazioni basate sul fatto che l'organizzazione sia un'impresa partner o collegata. Queste considerazioni dovrebbero essere viste in linea con le definizioni fornite nell'Allegato alla Raccomandazione della Commissione 2003/361.

Ci sono alcune eccezioni alle restrizioni di dimensione. La NIS2 si applica a tutte i soggetti, indipendentemente dalla loro dimensione, che sono:

- Fornitori di reti di comunicazione elettronica pubbliche o di servizi di comunicazione elettronica accessibili al pubblico;
- Fornitori di servizi fiduciari;
- Registri dei nomi di dominio di primo livello e fornitori di servizi del sistema dei nomi di dominio;
- L'unico fornitore in uno Stato membro di un servizio essenziale per il mantenimento di attività critiche sociali o economiche;
- Fornitori di servizi che, se interrotti, potrebbero avere un impatto significativo sulla sicurezza pubblica, sulla incolumità o sulla salute pubblica;
- Fornitori di servizi che, se interrotti, potrebbero indurre un rischio sistemico significativo, in particolare per i settori in cui tale interruzione potrebbe avere un impatto transfrontaliero;
- Critici a causa della loro importanza specifica a livello nazionale o regionale per il particolare settore o tipo di servizio, o per altri settori interdipendenti nello Stato membro;
- Entità di amministrazione pubblica del governo centrale;
- Entità di amministrazione pubblica a livello regionale che, a seguito di una valutazione basata sul rischio, forniscono servizi la cui interruzione potrebbe avere un impatto significativo su attività critiche sociali o economiche;
- Designate come Soggetti Critici ai sensi della CER;
- Entità che forniscono servizi di registrazione di nomi di dominio.

Gli Stati membri possono scegliere di applicare la NIS2 alle entità di amministrazione pubblica a livello locale e alle istituzioni educative, in particolare dove svolgono attività di ricerca critiche.

<table>
<tr><th>Non definito</th><th>Non tipizzato</th><th colspan="3">Essenziale</th><th>Deciso dallo Stato membro</th><th>Importante</th><th>Escluso</th></tr>
<tr><td rowspan="2"></td><td rowspan="2"></td><td colspan="2"></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2"></td><td>Grandi soggetti elencati nell'Allegato I</td><td>Fornitori unici di attività economiche o sociali essenziali in settori dell'Allegato I o II</td><td>Medi soggetti elencati nell'Allegato I</td><td>Esclusioni dal campo di applicazione del DORA</td></tr>
<tr><td colspan="2"></td><td>Servizi fiduciari provenienti da enti nazionali o pubblici di sicurezza, difesa o forze dell'ordine</td><td>Fornitori di servizi di nomi di dominio</td><td>Registri di nomi a dominio di primo livello</td><td>Soggetti con impatto significativo sulla sicurezza pubblica, sulla incolumità o sulla salute in settori dell'Allegato I o II</td><td>Medi o Grandi soggetti elencati nell'Allegato II</td><td>Soggetti che servono esclusivamente la sicurezza nazionale, la sicurezza pubblica, la difesa e l'applicazione della legge</td></tr>
</table>

	Istituzioni educative, in particolare dove svolgono attività di ricerca critiche	Soggetti identificati ai sensi del CER	Governo centrale	Fornitori di servizi DNS	Soggetti che possono causare un rischio sistemico con potenziale impatto transfrontaliero in settori dell'Allegato I o II	Governo regionale non grande	Soggetti che svolgono attività nella sicurezza nazionale, nella sicurezza pubblica, nella difesa e nell'applicazione della legge
Soggetti nell'ambito NIS	Governo locale	Soggetti di comunicazione elettronica di grandi/medie dimensioni	Grande governo regionale	Fornitori di servizi fiduciari	Soggetti critici per settori a livello nazionale o regionale o per un tipo di servizio in settori dell'Allegato I o II	Soggetti di comunicazione elettronica piccoli o micro	Sicurezza nazionale, sicurezza pubblica, difesa e applicazione della legge

*Figura 2**Fout! Gebruik het tabblad Start om Heading 1 toe te passen op de tekst die u hier wilt weergeven.**.2 – Panoramica dell'ambito e del tipo dei soggetti*

2.3 Tipi di soggetti

Combinati, la Direttiva sulla Resilienza delle Entità Critiche (CER) e la NIS2 hanno introdotto tre classificazioni di soggetti, ovvero Soggetti Critici, Essenziali e Importanti.

- **Soggetti Critici**: Questo è un tipo identificato nella CER. I Soggetti Critici forniscono servizi cruciali per il funzionamento dell'economia, della società, della salute pubblica e della sicurezza o dell'ambiente.
- **Soggetti Essenziali:** Come i Soggetti Critici, queste entità forniscono servizi cruciali per il funzionamento dell'economia, della società, della salute pubblica e della sicurezza o dell'ambiente. Tali soggetti sono classificati come Soggetti Essenziali nella NIS2 in quanto fornitori di servizi cruciali che si basano su tecnologie digitali per fornire tali servizi.
- **Soggetti Importanti:** Le entità che forniscono servizi in aree cruciali ma sono state escluse dall'elenco dei Soggetti Essenziali possono essere classificate come Soggetti Importanti. Allo stesso modo i Soggetti Importanti possono essere fornitori di servizi che sono critici per i servizi cruciali forniti dai Soggetti Essenziali.

I soggetti nell'ambito della NIS2 sono classificati come Soggetti Essenziali e Importanti.

La NIS2 include due Allegati che specificano i tipi di soggetti che possono essere considerati essenziali e importanti. L'ambito è ulteriormente definito da un insieme di regole, in cui la dimensione è il fattore principale, escludendo la maggior parte delle micro e piccole imprese. Tutte le entità che la CER considera Soggetti Critici sono considerate Soggetti Essenziali, indipendentemente dal fatto che siano specificate negli allegati della NIS2 come soggetti inclusi nell'ambito della Direttiva.

La NIS2 specifica la classificazione di molti tipi di entità ma consente agli Stati membri di ampliare l'elenco secondo necessità. Gli Stati membri dovranno aver stabilito un elenco di Soggetti Essenziali e Importanti entro il 17 aprile 2025. Una panoramica grafica dei diversi tipi di soggetti in relazione alle entità nell'ambito può essere trovata nella figura 2Fout**! Gebruik het tabblad Start om Heading 1 toe te passen op de tekst die u hier wilt weergeven.**.2, pagina 20.

2.3.1 Soggetti Critici

La Direttiva sulla Resilienza delle Entità Critiche (CER - Critical Entities Resilience Directive) affronta la resilienza delle entità che forniscono servizi critici nell'Unione la cui interruzione può avere un impatto significativo sul funzionamento dell'economia e della società.

La Direttiva affronta la resilienza da un ampio spettro, concentrandosi su tutto ciò che è necessario affinché i soggetti nell'ambito siano resilienti contro i disastri. Per le interruzioni basate su minacce informatiche, la CER si riferisce alla NIS2.

Il termine Soggetti Critici è utilizzato nella CER. Da una prospettiva NIS2, qualsiasi entità identificata come critica dalla CER deve essere un Soggetto Essenziale ai sensi della NIS2 (Articolo 3(1f)). I Soggetti Critici sono entità pubbliche o private che:

- Forniscono uno o più servizi essenziali;
- Operano nell'Unione Europea;
- Hanno la loro infrastruttura critica situata nell'UE;
- Potrebbero causare una significativa interruzione se colpite da un incidente.

2.3.2 Soggetti Essenziali

I Soggetti Essenziali sono entità la cui interruzione avrà un impatto significativo sull'UE e sulla sua economia, sicurezza pubblica, incolumità o salute pubblica. La NIS2 ha identificato un insieme di regole che determinano quali entità devono essere classificate come essenziali. I soggetti sono considerati essenziali quando:

- Sono elencati nell'Allegato I della Direttiva e sono più grandi delle medie imprese;
- Sono fornitori di servizi fiduciari qualificati, registri di nomi di dominio di primo livello o fornitori di servizi DNS, indipendentemente dalle dimensioni;
- Sono almeno medie imprese che forniscono reti di comunicazione elettronica pubbliche o servizi di comunicazione elettronica accessibili al pubblico;
- Sono entità di amministrazione pubblica del governo centrale, escludendo le entità nei settori della sicurezza nazionale, sicurezza pubblica, difesa o applicazione della legge;
- Sono entità di amministrazione pubblica a livello regionale che forniscono servizi che, se interrotti, influiscono significativamente su attività critiche sociali o economiche;
- Sono gli unici fornitori di un servizio essenziale in uno Stato membro per il mantenimento di attività critiche sociali o economiche;
- L'interruzione del loro servizio potrebbe avere un impatto significativo sulla sicurezza pubblica, incolumità o salute pubblica;
- L'interruzione del loro servizio potrebbe indurre un rischio sistemico significativo (il rischio di un collasso di un intero sistema piuttosto che semplicemente il fallimento di singole parti), in particolare per i settori in cui tale interruzione potrebbe avere un impatto transfrontaliero;
- Sono critici a causa della loro importanza specifica a livello nazionale o regionale per il settore o tipo di servizio, o per altri settori interdipendenti nello Stato membro;
- Sono stati identificati come soggetti critici ai sensi della CER.

Se uno Stato membro ha ampliato l'elenco degli operatori di servizi essenziali prima del momento in cui la NIS2 è entrata in vigore, questi operatori possono essere inclusi come Soggetti Essenziali ai sensi della NIS2.

2.3.3 Soggetti Importanti

I soggetti di un tipo menzionato nell'Allegato I o II che non si qualificano come Soggetti Essenziali, sono Soggetti Importanti. Questo include le entità identificate dagli Stati membri come Soggetti Importanti perché:

- Il soggetto è l'unico fornitore di un servizio essenziale per il mantenimento di attività critiche;
- Le interruzioni del servizio fornito dal soggetto possono avere un impatto significativo sulla sicurezza pubblica, incolumità o salute pubblica;
- L'interruzione del servizio fornito dal soggetto potrebbe causare una cascata di eventi dirompenti, possibilmente anche transfrontalieri (rischio sistemico);
- Ha un'importanza specifica a livello nazionale o regionale per un particolare settore o tipo di servizio, o per altri settori interdipendenti.

2.3.4 Differenze tra Soggetti Essenziali e Importanti

Il Considerando 15 della NIS2 afferma che i soggetti rientranti nell'ambito della NIS2 dovrebbero essere classificati in Soggetti Essenziali e Importanti. La classificazione dovrebbe riflettere la misura in cui sono critici in relazione al settore in cui operano o al tipo di servizio che forniscono, nonché alle loro dimensioni.

I regimi di supervisione e applicazione per queste due categorie di soggetti sono differenziati per garantire un equilibrio equo tra requisiti basati sul rischio e obblighi da un lato, e il carico amministrativo derivante dalla supervisione della conformità dall'altro.

La NIS2 ha creato un insieme di requisiti molto più rigorosi per la supervisione dei Soggetti Essenziali rispetto ai Soggetti Importanti.

2.4 Struttura della NIS2

2.4.1 Direttiva o regolamento

La NIS2 è una Direttiva. Dovrebbe essere vista come un'istruzione agli Stati membri per creare una legge nazionale basata sui requisiti stabiliti nella Direttiva. Le direttive hanno diversi tipi di requisiti. Gli Stati membri saranno tenuti a:

- Incorporare alcuni dei requisiti nella legge nazionale senza alcun cambiamento strutturale nel testo rispetto al testo della Direttiva;
- Interpretare i requisiti e allinearli a ciò che si adatta meglio in relazione alle loro leggi nazionali;
- Scegliere di includere i requisiti nella legge o lasciarli fuori completamente.

La NIS2 è entrata in vigore il 16 gennaio 2023. Gli Stati membri hanno avuto 21 mesi per tradurre la Direttiva in legge nazionale. Pertanto entro il 17 ottobre 2024 gli Stati membri devono adottare e pubblicare la legge nazionale che rispetta la Direttiva NIS2. La legge nazionale si applicherà immediatamente, il che significa che a partire dal 18 ottobre 2024 (al più tardi) i soggetti devono conformarsi alla legislazione nazionale derivata dalla NIS2.

Fino a quando uno Stato membro non trascrive la Direttiva in legge nazionale, i soggetti nell'ambito di tale Stato membro sono esenti da qualsiasi obbligo della Direttiva.

2.4.2 Considerando e Disposizioni

La NIS2 è composta da Considerando e Disposizioni. I Considerando sono il testo all'inizio della NIS2 che descrive il contesto della Direttiva e dà un'idea di come interpretare le Disposizioni. Sono introdotti dalla parola "Considerando" e sono numerati da 1 a 144.

I Considerando di per sé non hanno conseguenze giuridicamente vincolanti mentre invece le Disposizioni le hanno.

Le Disposizioni sono concise ma spesso lasciano spazio all'interpretazione. Se una Disposizione può essere interpretata in modi diversi, i Considerando forniscono il contesto su come le Disposizioni dovrebbero essere lette. La Corte di Giustizia dell'UE (CGUE) adotta un'interpretazione "finalistica" (teleologica) della NIS2. Se il testo di una Disposizione è poco chiaro, piuttosto che affrontarlo letteralmente la CGUE lo interpreterà in base allo scopo o allo spirito della legislazione come contestualizzato nei Considerando. Tuttavia il contenuto delle Disposizioni operative prevale sempre sul contenuto di eventuali Considerando associati: se i Considerando sono incoerenti con una Disposizione, allora il testo della Disposizione avrà la precedenza.

Le Disposizioni stabiliscono i requisiti giuridicamente vincolanti. Sono divise in capitoli, articoli e, dove appropriato, paragrafi, ciascuno numerato separatamente. Ci sono nove capitoli nella NIS2 e quarantasei articoli. Gli articoli sono numerati unicamente come Disposizioni individuali in tutta la NIS2. La numerazione degli articoli è continua e non influenzata dalle divisioni dei capitoli.

Molti articoli sono estesi e affrontano i requisiti che vengono descritti per diverse situazioni e tipi di soggetti. Dove questo è il caso, gli articoli sono divisi in paragrafi. Alcuni paragrafi sono estesi e possono avere una ulteriore divisione in commi. Il numero degli articoli è rappresentato in questo manuale come segue:

Articolo 21(2g) = Articolo 21, Paragrafo 2, Comma g

2.4.3 I nove capitoli della NIS2

La NIS2 è divisa in nove capitoli e tre allegati. Ciascuno è brevemente descritto di seguito:

- **Capitolo I: Disposizioni generali**
  Una panoramica generale della NIS2, inclusa una descrizione dell'oggetto, dell'ambito, dell'allineamento ad altre leggi e delle definizioni dei termini.
- **Capitolo II: Framework coordinati in materia di cybersicurezza**
  Requisiti nazionali per ciascuno Stato membro, inclusi lo sviluppo di una strategia nazionale di sicurezza informatica e la designazione o la creazione di varie istituzioni e autorità.
- **Capitolo III: Cooperazione a livello dell'Unione e internazionale**
  I requisiti a livello dell'Unione e la formalizzazione del desiderio di cooperare a livello internazionale.
- **Capitolo IV: Misure di gestione del rischio informatico e obblighi di segnalazione**
  I requisiti che ciascun soggetto deve rispettare.
- **Capitolo V: Giurisdizione e registrazione**
  Chiarimenti giurisdizionali su dove i soggetti sono rappresentati in più Stati membri.
- **Capitolo VI: Condivisione delle informazioni**
  Le possibilità di condividere i risultati su base volontaria.
- **Capitolo VII: Supervisione e applicazione**
  I diritti delle autorità e le conseguenze della violazione della NIS2.
- **Capitolo VIII: Atti delegati e di esecuzione**
  Atti delegati che possono introdurre specifiche giuridicamente vincolanti sulla legge e gli atti di esecuzione che facilitano l'implementazione della legge nel quadro legislativo di uno Stato membro.
- **Capitolo IX: Disposizioni finali**
  Manutenzione e implementazione della NIS2.

- **Allegato I e II: Settori, sotto settori e tipi di soggetti nell'ambito della NIS2**
- **Allegato III: Tabella di correlazione con la NIS originale**