

WEBINAR: NIS 2, Facciamo Chiarezza e Iniziamo ad Adeguarci

LINEE GUIDA PER L'IMPLEMENTAZIONE

STEP 1 (assessment):

- Verificare il perimetro della norma;
- Effettuare un assessment e una gap analysis;

STEP 2 (implementation):

- Pianificare le attività suggerite dalla fase di assessment;
- Implementare le attività pianificate;
- Verificare i risultati;
- Intraprendere eventuali azioni di miglioramento;

STEP 3 (improvement)

- Somministrare formazione continua;
- Aggiornare valutazione dei rischi, procedure, politiche;
- Osservare scadenze e comunicazioni obbligatorie ad ACN.



RELATORE: NICOLA COZZOLI - TECHMETIS

tech
metis



EVOLUUMIA
The cyber security company

MUSA
FORMAZIONE E LAVORO

WEBINAR: NIS 2, Facciamo Chiarezza e Iniziamo ad Adeguarci

STEP 1: ASSESSMENT

- ✓ Verificare il perimetro della norma:
Se si rientra nelle categorie dei soggetti essenziali o importanti, in base alla dimensione aziendale ed al settore di appartenenza, ovvero nelle **categorie individuate dal D. Lgs.134/2024** (vedi **art. 6 e allegati I, II, III, IV**). L'output di questa attività indica se procedere alle fasi di analisi e adeguamento.

- ✓ Effettuare un assessment e una gap analysis:
Verificare, con opportune competenze e strumenti, il livello di maturità e di copertura in riferimento alle **misure di sicurezza** minime previste dalla norma.
L'output di questa attività concorre a predisporre (STEP 2) un piano di azioni di adeguamento.



RELATORE:

tech
metis



EVOLUUMIA
The cyber security company

MUSA
FORMAZIONE E LAVORO

WEBINAR: NIS 2, Facciamo Chiarezza e Iniziamo ad Adeguarci

STEP 1: ASSESSMENT

Misure di sicurezza minime:

1. Analisi dei rischi e sicurezza dei sistemi informativi
2. Gestione degli incidenti
3. Continuità operativa
4. Sicurezza della catena di approvvigionamento
5. Sicurezza delle reti e dei sistemi informativi
6. Misure di gestione del rischio di sicurezza informatica
7. Formazione in materia di igiene e sicurezza informatica
8. Crittografia
9. Sicurezza delle risorse umane
- 10. Autenticazione**



RELATORE:

tech
metis



EVOLUIMIA
The cyber security company

MUSA
FORMAZIONE E LAVORO

WEBINAR: NIS 2, Facciamo Chiarezza e Iniziamo ad Adeguarci

STEP 2: IMPLEMENTATION

- ✓ Pianificare le attività suggerite dalla fase di assessment:
Stabilire processi e risorse necessarie per l'**implementazione delle misure di sicurezza minime previste**, e identificare e affrontare i rischi e le opportunità. Questa fase consiste nella redazione di un piano che contenga, a titolo esemplificativo, un elenco di azioni correttive proposte, azioni di risoluzione transitorie (se previste), il nome del responsabile dell'attuazione, la data di attuazione.

ESEMPIO: Azione: Implementazione della autenticazione multifattoriale obbligatoria per l'accesso alla casella di posta aziendale / Responsabile: ing. Bianchi – Area IT / Data: Dicembre 2024.

- ✓ Implementare le attività pianificate:
Attuare tutte le azioni pianificate, con le risorse previste.

ESEMPIO: Configurazione dei sistemi per rendere obbligatoria l'autenticazione MFA per l'accesso alla casella di posta.



RELATORE:

tech
metis



EVOLUMIA
The cyber security company

MUSA
FORMAZIONE E LAVORO

WEBINAR: NIS 2, Facciamo Chiarezza e Iniziamo ad Adeguarci

STEP 2: IMPLEMENTATION

- ✓ **Verificare i risultati:**
Monitorare e, se possibile, misurare i processi/prodotti/servizi implementati rispetto ai requisiti di sicurezza.

ESEMPIO: Misurare l'adozione dell'autenticazione a più fattori, nell'intervallo di tempo definito.

- ✓ **Intraprendere eventuali azioni di miglioramento;**
Dove previsto, avviare attività di ottimizzazione dei processi/prodotti/servizi implementati.

ESEMPIO: Diffondere guide, ad uso personale, per la corretta configurazione della autenticazione a più fattori.



RELATORE:

tech
metis



EVOLUUMIA
The cyber security company

MUSA
FORMAZIONE E LAVORO

WEBINAR: NIS 2, Facciamo Chiarezza e Iniziamo ad Adeguarci

STEP 3: IMPROVEMENT

- ✓ Somministrare formazione continua;
Redigere ed aggiornare il piano di formazione su temi specifici di cybersecurity, includendo anche gli organi decisionali.
- ✓ Aggiornare valutazione dei rischi, procedure, politiche:
Verificare la validità dell'ultima valutazione ed aggiornarla includendo nuovi rischi o eliminandone di obsoleti.
- ✓ Osservare scadenze e comunicazioni obbligatorie ad ACN:
Adempiere agli obblighi previsti dalla norma, rispettando le scadenze temporali.



RELATORE:

tech
metis



EVOLUIMIA
The cyber security company

MUSA
FORMAZIONE E LAVORO

WEBINAR: NIS 2, Facciamo Chiarezza e Iniziamo ad Adeguarci

STEP 3: IMPROVEMENT

SCADENZE E ADEMPIMENTI:

✔ **Entro il 31 dicembre 2024:**
le aziende e le pubbliche amministrazioni devono effettuare un assessment per determinare se rientrano sotto l'ambito di applicazione della Direttiva NIS 2.

✔ **Tra il 1° gennaio e il 28 febbraio 2025:**
le entità che, a seguito dell'assessment, si considerano soggette agli obblighi del decreto dovranno registrarsi sulla piattaforma digitale fornita dall'ACN, fornendo le informazioni richieste dalla normativa.

✔ **Entro il 17 gennaio 2025:**
è previsto che si registrino sulla piattaforma i fornitori di servizi relativi ai nomi di dominio, i gestori di registri dei nomi di dominio di primo livello, i fornitori di servizi di cloud computing, i fornitori di data center, i fornitori di reti di distribuzione dei contenuti, e altre categorie di servizi online.

✔ **Entro il 31 marzo 2025:**
l'ACN dovrà stilare l'elenco dei soggetti essenziali e importanti, basato sulle registrazioni ricevute



RELATORE:

tech
metis



EVOLUUMIA
The cyber security company

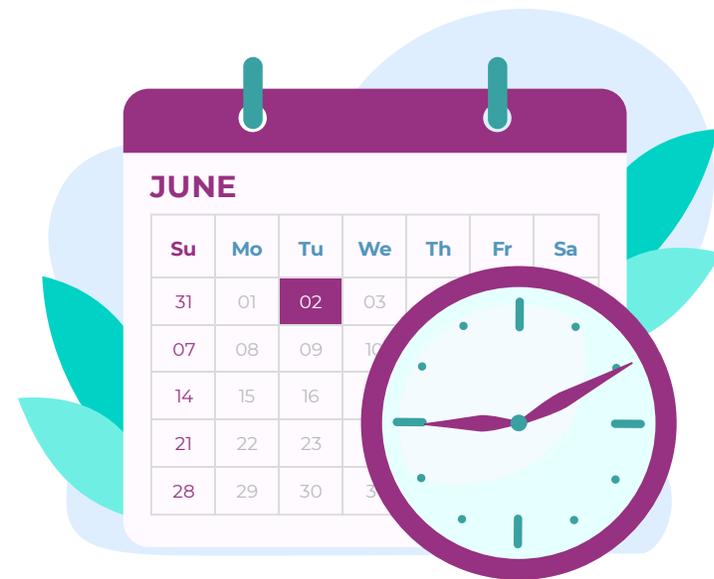
MUSA
FORMAZIONE E LAVORO

WEBINAR: NIS 2, Facciamo Chiarezza e Iniziamo ad Adeguarci

STEP 3: IMPROVEMENT

SCADENZE E ADEMPIMENTI:

- ✓ **Tra il 1° e il 15 aprile 2025:**
l'ACN comunicherà ai soggetti registrati l'inclusione nell'elenco dei soggetti essenziali o importanti.
- ✓ **Entro il 15 aprile 2025:**
le entità che riceveranno tale comunicazione dovranno nominare un responsabile per l'adempimento degli obblighi previsti dal decreto.
- ✓ **Tra il 15 aprile e il 31 maggio 2025:**
le entità dovranno fornire ulteriori informazioni richieste dalla normativa.
- ✓ **A partire dal 1° gennaio 2026:**
dovranno essere rispettati gli obblighi di notifica degli incidenti.
- ✓ **Entro il 1° ottobre 2026:**
si dovranno adempiere agli obblighi per gli organi di amministrazione e per quelli direttivi, adottare misure di sicurezza adeguate, e mantenere una banca dati per la registrazione dei nomi di dominio, se applicabile.



RELATORE:

WEBINAR: NIS 2, Facciamo Chiarezza e Iniziamo ad Adeguarci

CONCLUSIONI

Il percorso di adeguamento alla NIS2 richiede obiettivi specifici, risorse adeguate e tempi di implementazione non sempre prevedibili: sono, infatti, spesso necessari interventi invasivi nelle procedure e nelle infrastrutture del perimetro di sicurezza.

E' importante perciò affiancarsi a professionisti e aziende con esperienze trasversali in temi di governance, cybersecurity e formazione, adottando un approccio analogo a quello dei sistemi di gestione più noti (qualità – 9001, sicurezza delle informazioni – 27001) che preveda – tra tanti aspetti – l'analisi dei rischi ed il miglioramento continuo.



RELATORE:

tech
metis



EVOLUIMIA
The cyber security company

MUSA
FORMAZIONE E LAVORO