# Modello di Piano di Adeguamento alla Direttiva NIS2

Questo documento fornisce un modello operativo per pianificare l'adeguamento alla Direttiva NIS2, rivolto ad aziende classificate come soggetti essenziali o importanti. Il piano è suddiviso in fasi e azioni, con obiettivi chiari e responsabilità definite.

## Fase 1 – Valutazione Iniziale

- Verifica dell'applicabilità della direttiva all'organizzazione.

- Identificazione dello status (soggetto essenziale o importante).

- Gap analysis rispetto ai requisiti dell'Art. 21 (misure tecniche e organizzative).

- Identificazione dei sistemi, asset e processi critici.

## Fase 2 – Governance e Responsabilità

- Nomina del responsabile per la cybersecurity e del team di progetto.

- Definizione delle responsabilità dei dirigenti e della funzione IT.

- Creazione di un comitato di sicurezza o di continuità operativa.

## Fase 3 – Adozione delle Misure Richieste

- Implementazione di controlli di accesso, segmentazione di rete, backup.

- Monitoraggio della rete e uso di strumenti come SIEM/EDR.

- Piani di business continuity e disaster recovery aggiornati.

- Formazione periodica dei dipendenti in tema di sicurezza.

## Fase 4 – Incident Response e Notifica

- Redazione di un piano di risposta agli incidenti.

- Procedure di notifica alle autorità entro i termini previsti (24h, 72h, 1 mese).

- Collegamento con il CSIRT nazionale e strutture di supporto.

- Simulazioni di incidenti e aggiornamento continuo del piano.

## Fase 5 – Monitoraggio e Verifica

- Audit periodici interni e, se previsto, esterni.

- Revisione annuale del piano e delle politiche di sicurezza.

- Valutazione della supply chain e dei fornitori critici.

- Documentazione delle attività e preparazione alla supervisione.

## Fase 6 – Piano di Attuazione e Tempistiche

- Definizione delle priorità in base ai rischi e alla maturità aziendale.

- Piano GANTT con fasi, scadenze e responsabili.

- Tracciamento dell'avanzamento e aggiornamenti regolari.

## Conclusione

L'attuazione del piano di adeguamento alla NIS2 richiede il coinvolgimento trasversale di tutte le funzioni aziendali. È fondamentale garantire un approccio sistemico e documentato alla gestione della cybersecurity.

## Fase 1 – Valutazione Iniziale (Dettagliata)

1. Verifica dell'applicabilità della direttiva:

- Stabilire se l'organizzazione rientra tra i 'soggetti essenziali' o 'soggetti importanti' secondo l'Allegato I e II della direttiva.
- Considerare il numero di dipendenti (>50) e il fatturato (>10 milioni €) per la qualificazione automatica.
- Valutare se l'organizzazione fornisce servizi considerati critici per la società, l'economia o la sicurezza pubblica.

2. Classificazione dei servizi e degli asset:

- Identificare i servizi critici forniti (es. fornitura energetica, trasporti, sanità, finanza, servizi digitali, infrastrutture IT).
- Mappare i processi aziendali legati a questi servizi.
- Mappare asset hardware e software associati: server, applicativi, database, dispositivi IoT/OT, cloud, ecc.
- Identificare dipendenze interne ed esterne (es. fornitori, data center, connessioni internet, servizi cloud).

3. Gap analysis rispetto all'articolo 21 della NIS2:

- Valutare la presenza o meno delle 10 misure richieste (es. gestione rischio, incident response, business continuity, supply chain security, crittografia, logging).
- Utilizzare checklist o framework (ISO/IEC 27001, NIST CSF) per comparazione.
- Coinvolgere il responsabile IT/cybersecurity, l'ufficio legale e il management per una fotografia realistica della situazione attuale.

4. Valutazione della maturità cybersecurity:

- Usare uno strumento di autovalutazione (maturity model, questionari interni, servizi esterni).
- Stimare il rischio residuo attuale e la capacità di risposta ad attacchi informatici.
- Produrre un rapporto iniziale interno che documenti: rischi principali, punti deboli e priorità.

5. Documentazione iniziale:

- Redigere un documento di 'analisi di impatto' (Business Impact Analysis - BIA) per i servizi essenziali.
- Creare un registro degli asset critici.
- Predisporre una roadmap con obiettivi preliminari e scadenze a breve termine (3-6 mesi).

## Fase 2 – Governance e Responsabilità (Dettagliata)

1. Nomina delle figure responsabili:

- Designare un Responsabile della Sicurezza delle Informazioni (CISO o equivalente) con mandato chiaro.
- Se non presente, valutare la creazione di un team interno o l'esternalizzazione a un MSSP (Managed Security Service Provider).
- Individuare i referenti per: IT, legale, HR, operations e business continuity.

2. Definizione dei ruoli e delle responsabilità:

- Mappare ruoli e responsabilità connessi alla gestione della cybersecurity e conformità NIS2.
- Formalizzare le responsabilità tramite job description e atti di nomina.
- Coinvolgere attivamente il management e i dirigenti (obbligo diretto previsto dall'art. 20 e 30 della direttiva).

3. Strutturazione della governance della sicurezza:

- Costituire un Comitato per la Sicurezza o Cybersecurity Board, con riunioni periodiche (es. trimestrali).
- Definire un piano di incontri tra CISO e vertici aziendali per aggiornamento su rischi, incidenti e stato dei controlli.
- Introdurre un sistema di escalation in caso di violazioni, criticità o non conformità.

4. Integrazione della sicurezza nei processi aziendali:

- Integrare la gestione della sicurezza IT nei processi di acquisto, sviluppo, gestione risorse umane e compliance.
- Valutare l'adozione di un SGSI (Sistema di Gestione della Sicurezza delle Informazioni) secondo ISO/IEC 27001.
- Introdurre metriche e KPI per monitorare lo stato della sicurezza (incidenti, aggiornamenti, formazione, audit).

5. Coinvolgimento del top management:

- Il consiglio di amministrazione deve essere informato periodicamente sulla postura di sicurezza e sulle misure attuate.
- Inserire la cybersecurity nei report strategici e nelle valutazioni di rischio aziendale.
- Sensibilizzare i vertici sulla responsabilità diretta e le potenziali sanzioni per mancata conformità alla NIS2.

6. Documentazione e tracciabilità:

- Produrre un documento di governance della sicurezza (es. policy di sicurezza, assetto organizzativo).
- Archiviare verbali, atti di nomina e registri delle attività del comitato di sicurezza.
- Verificare che ogni ruolo abbia una formazione specifica documentata e aggiornata.

## Fase 3 – Adozione delle Misure Richieste (Dettagliata)

1. Misure tecniche:

- Configurare firewall, IDS/IPS, segmentazione di rete.
- Abilitare l'autenticazione multifattore (MFA) su tutti i servizi critici.
- Applicare patch regolarmente, usare strumenti di gestione vulnerabilità.
- Monitorare accessi e comportamenti anomali (UEBA, SIEM).

2. Misure organizzative:

- Creare e diffondere policy di sicurezza informatica.
- Definire piani di formazione periodici per i dipendenti.
- Introdurre procedure per il provisioning/deprovisioning degli account.
- Gestire il ciclo di vita dei dati e dei dispositivi.

3. Business Continuity e Disaster Recovery:

- Realizzare un piano BCP/DRP documentato, testato e aggiornato.
- Effettuare esercitazioni annuali e simulazioni di disastro.
- Integrare le risposte IT con quelle operative e logistiche.

4. Supply Chain Security:

- Valutare la sicurezza dei fornitori critici tramite audit o checklist.
- Introdurre obblighi di sicurezza nei contratti (es. SLA, gestione incidenti).
- Monitorare gli accessi e le integrazioni di terze parti nei sistemi interni.

## Fase 4 – Incident Response e Notifica (Dettagliata)

1. Definizione di incidente:

- Qualsiasi evento che compromette riservatezza, integrità o disponibilità dei sistemi.
- Es.: malware, accesso non autorizzato, perdita dati, ransomware.

2. Redazione di un Incident Response Plan (IRP):

- Descrivere fasi: preparazione, rilevamento, contenimento, recupero, lezione appresa.
- Identificare ruoli, responsabili e canali di comunicazione.
- Simulare scenari reali (es. phishing, attacco DDoS) almeno annualmente.

3. Obblighi di notifica secondo NIS2:

- Notifica iniziale entro 24h all'autorità competente (CSIRT nazionale).
- Notifica dettagliata entro 72h.
- Relazione finale entro un mese.
- Mantenere registro dettagliato degli incidenti e delle azioni intraprese.

4. Integrazione con strumenti di monitoraggio:

- Utilizzare SIEM per l’aggregazione e la correlazione dei log.
- Configurare alert e soglie automatiche per rilevare anomalie.
- Stabilire un contatto operativo diretto con il CSIRT nazionale o il SOC esterno.

## Fase 5 – Monitoraggio e Verifica (Dettagliata)

1. Audit periodici:

- Effettuare audit interni almeno annuali, su base documentale e tecnica.
- Valutare la conformità ai requisiti NIS2 e alle policy interne.
- Verificare l'adozione e l'efficacia delle misure implementate.

2. Supervisione e revisione:

- Pianificare revisioni formali da parte del management.
- Rivedere e aggiornare documentazione, policy e IRP.
- Introdurre un ciclo PDCA (Plan-Do-Check-Act) per la sicurezza.

3. Supply chain e fornitori:

- Riesaminare i contratti con i fornitori critici.
- Inserire clausole di auditabilità e obblighi di reporting incidenti.
- Valutare i fornitori rispetto a uno standard di sicurezza.

4. Tracciabilità e reportistica:

- Mantenere un registro aggiornato delle attività di sicurezza.
- Redigere report periodici per il comitato sicurezza e la direzione.
- Archiviare le evidenze utili per ispezioni e verifiche ispettive future.

## Fase 6 – Piano di Attuazione e Tempistiche (Dettagliata)

1. Definizione delle priorità:

- Classificare le azioni in: urgenti, importanti, strategiche.
- Valutare l'impatto sui servizi critici e il livello di rischio attuale.
- Coordinare l'allocazione delle risorse (budget, personale, strumenti).

2. Elaborazione di una roadmap:

- Creare una tabella con attività, responsabili, scadenze e stato.
- Utilizzare strumenti Gantt o project management.
- Collegare le attività ai controlli di sicurezza e agli obblighi normativi.

3. Monitoraggio dell'avanzamento:

- Tenere riunioni periodiche per aggiornare sullo stato del piano.
- Verificare il raggiungimento degli obiettivi intermedi.
- Ricalibrare il piano in base a cambiamenti tecnologici, normativi o di rischio.