SECURITY SUMMIT

Security Summit

Milano 17-18-19 marzo 2026

Clusit

ASTREA

Ruolo delle Società In-house nella conformità pratica alla Direttiva NIS2: confronto di esperienze e best practices

Maurizio Pastore | GDPR e NIS Competence Center – Liguria Digitale

Maurizio Pastore
GDPR e NIS Competence Center – Liguria Digitale

La **Direttiva NIS2**, recepita in Italia con il **Decreto Legislativo 138/2024** dispone che un'organizzazione deve:

- **identificare i servizi critici**
- **classificare dati e sistemi**
- **valutare l'impatto** in caso di incidente cyber

Tutto ciò al fine di gestire e ridurre i rischi, migliorare la prevenzione, rilevazione e risposta agli incidenti, e garantire la continuità dei servizi essenziali.

Implementazione articolo 30

L'agenzia stabilisce processo, modalità e criteri per elencazione, caratterizzazione e categorizzazione attività e servizi dei soggetti.

Definizione modello categorizzazione

Settembre 25 - Gennaio 26

L'agenzia può avvalersi dei tavoli settoriali ai fini di quanto previsto dall'articolo 30 del decreto NIS

Revisione modello categorizzazione

Febbraio 26

I soggetti comunicano e aggiornano elenco attività e servizi comprensivi di caratterizzazione e categoria di rilevanza.

Funzionalità su piattaforma online

Maggio 26- Giugno 26

Modello di categorizzazione

Elenco attività e servizi

- Norma la predisposizione e la compilazione dell'elenco delle attività e dei servizi dei soggetti NIS.

Categorie di rilevanza

- Definisce le categorie di rilevanza delle attività e dei servizi dei soggetti NIS e le modalità di attribuzione delle stesse.

Soggetti privati e pubblici

- Differenziato a seconda che il soggetto NIS sia un soggetto privato o sia un soggetto della Pubblica Amministrazione.

Modello di categorizzazione per soggetti privati

Elementi del modello

- ✓ Definita una struttura delle attività e i servizi organizzata in **12 macro-aree** ognuna caratterizzata da denominazione, descrizione, elenco di esempi, categoria di rilevanza preassegnata.
- ✓ Ogni macro-area rappresenta un insieme astratto di attività e servizi di un'organizzazione caratterizzati da elementi in comune quali, ad esempio, utenti, finalità o tipologia di prestazione.
- ✓ Per le macro aree **Produzione di beni e servizi** e **Monitoraggio e controllo** gli esempi sono stati declinati sulla base della tipologia di soggetto (*esempi specifici*).

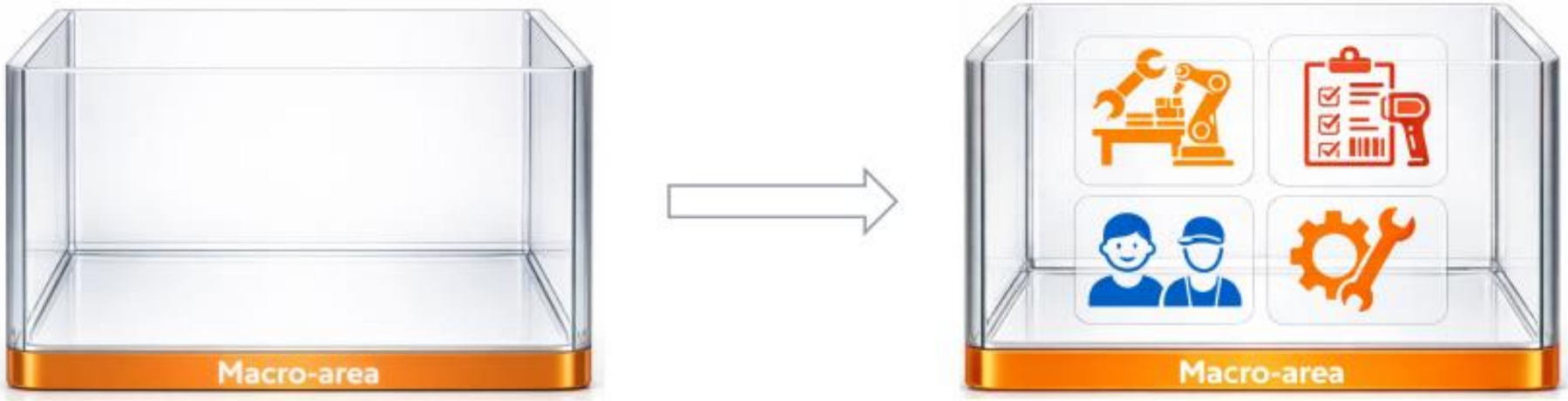
Categorie di rilevanza

- ✓ 4 categorie sulla base dell'impatto di una compromissione sulle capacità dell'organizzazione di erogare le attività e i servizi per i quali rientra nell'ambito dell'applicazione del decreto NIS (*attività e servizi NIS*):
  - impatto minimo
  - impatto basso
  - impatto medio
  - impatto alto
- ✓ Ai fini della valutazione dell'impatto sono considerati 3 scenari (economico, operativo e reputazionale).

Macro-area

Ogni macro-area rappresenta un **contenitore** di attività e servizi ed è caratterizzata da denominazione, descrizione, elenco di esempi (*per 2 macro-aree, gli esempi forniti sono specifici sulla base della tipologia di soggetto*) e categoria di rilevanza pre-assegnata.

Ogni soggetto **inserisce** proprie attività e propri servizi che rientrano nella macro area, eventualmente **modificando** la categoria di rilevanza anche a livello di singola attività o servizio. Se non dovesse avere alcuna attività o servizio, **rimuove** la macro-area.



Elenco macro aree

Minimo	Approvvigionamento di beni e servizi
Minimo	Comunicazione e marketing
Minimo	Gestione amministrativa e conformità
Minimo /Basso	Logistica
Basso	Gestione dei clienti
Basso	Gestione delle risorse umane
Basso	Gestione finanziaria
Basso	Protezione delle sedi
Medio	Produzione di beni e servizi
Medio	Progettazione
Alto	Monitoraggio e controllo
Alto	Ricerca e sviluppo

Modello di categorizzazione per soggetti pubblici

Elementi del modello

- ✓ Riutilizzare i risultati derivanti da classificazione dei dati e servizi effettuata ai fini del regolamento Cloud che prevede che le PA predispongano e aggiornano un elenco dei propri dati e dei propri servizi digitali, comprensivo di tutti gli elementi necessari alla loro caratterizzazione ai fini della relativa classificazione.

Categorie di rilevanza

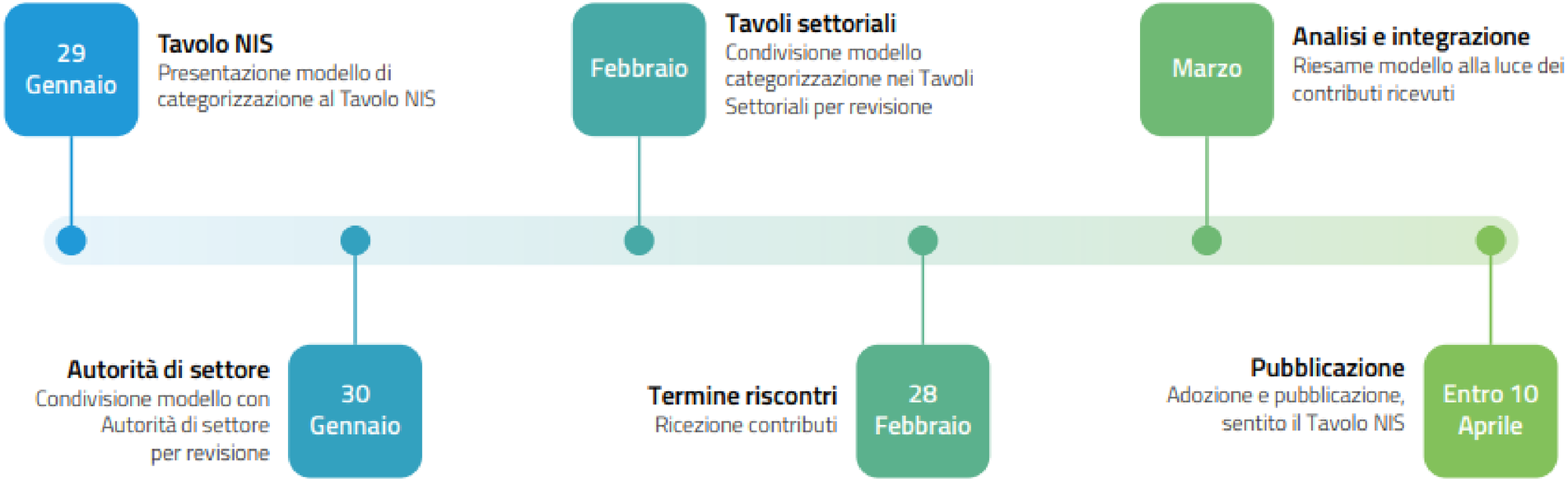
- ✓ La categorizzazione delle attività e servizi coincide con la classificazione dei dati e servizi effettuata ai fini del Regolamento Cloud (dati e servizi "ordinari", "critici", "strategici").

Misure di sicurezza e modello di implementazione

Proporzionalità delle misure

- ✓ I sistemi informativi e di rete ereditano la categoria di rilevanza del servizio o dell'attività che abilitano (ossia che supportano, svolgono o erogano).
- ✓ Qualora i sistemi informativi e di rete abilitino servizi o attività con categorie di rilevanza differenti, ereditano la categoria rilevanza con impatto maggiore.
- ✓ Gli obblighi a lungo termine definiranno 4 *set* di misure di sicurezza definite su 4 livelli di mitigazione del rischio crescente (L1, L2, L3, L4) e differenziate tra soggetti essenziali e importanti:
  - per i **soggetti privati**, ognuna delle 4 categoria di rilevanza corrisponde a un set di misure di sicurezza;
  - per i **soggetti pubblici**, i sistemi informativi e di rete oggetto del regolamento cloud classificati come ordinari, critici, strategici implementano le misure di sicurezza L2, L3 e L4, i restanti sistemi informativi e di rete (infrastruttura informatica client) implementano le misure di sicurezza di livello L1.

Processo adozione modello di categorizzazione



L'ANALISI DEL RISCHIO

La Direttiva NIS2 richiede ai **soggetti essenziali** e **importanti** di adottare un approccio basato sul rischio nella gestione della sicurezza delle reti e dei sistemi informativi. Le fasi in cui dovrebbe essere articolata la valutazione del rischio è la seguente:

- Stabilire un quadro di gestione del rischio → devono essere individuati i criteri di sicurezza di base, la scala del rischio, la propensione al rischio e la valutazione del rischio basata sugli scenari o sugli asset
- Identificare i rischi → che possono influenzare la riservatezza, integrità e disponibilità delle informazioni
- Analizzare i rischi → Identificare le minacce e le vulnerabilità che si applicano a ciascuna risorsa
- Valutazione del rischio → rispetto ai livelli predeterminati di rischio accettabile, e stabilire la priorità di trattamento dei rischi.
- Selezionare le opzioni di trattamento del rischio → 1- Accetto: rischio accettabile per regola o decisione, 2-Riduco: penso a contromisure che abbassino la probabilità o impatto, 3-Trasferisco: faccio gestire il processo ad un outsourcer, 4-Evito: cesso il processo o lo modifico per evitare il rischio (esempio non tratto dato personale)

L’analisi del rischio consente di:

- **identificare servizi essenziali e asset critici** dell’organizzazione
- **individuare minacce e vulnerabilità** che potrebbero compromettere i sistemi informativi
- valutare il **potenziale impatto degli incidenti informatici** sui dati
- definire e implementare **misure tecniche** e **organizzative adeguate** e proporzionate al rischio

MISURE DI SICUREZZA DI BASE PER I SOGGETTI IMPORTANTI ED ESSENZIALI

GV.RM-03 (GOVERN – Risk Management): Le attività e gli esiti della gestione del rischio di cybersecurity sono parte integrante dei processi di gestione del rischio dell'organizzazione. Nell'ambito dei processi di gestione del rischio del soggetto NIS è definito, attuato, aggiornato e documentato un piano di gestione dei rischi per la sicurezza informatica per identificare, analizzare, valutare, trattare e monitorare i rischi.

ID.RA-05 (IDENTIFY – Risk Assessment): Minacce, vulnerabilità, probabilità e impatti sono utilizzati per comprendere il rischio inerente e per informare la prioritizzazione della risposta al rischio.

In accordo al piano di gestione dei rischi per la sicurezza informatica di cui alla misura GV.RM-03, è eseguita e documentata la valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete, anche con riferimento alle eventuali dipendenze da fornitori e partner terzi

ID.RA-06 (IDENTIFY – Risk Assessment): Le risposte al rischio sono scelte, prioritizzate, pianificate, monitorate e comunicate. È inoltre definito, documentato, eseguito e monitorato un piano di trattamento del rischio che comprende almeno:

a) le opzioni di trattamento e le misure da attuare in merito al trattamento di ciascun rischio individuato e le relative priorità;

b) le articolazioni competenti per l'attuazione delle misure di trattamento dei rischi e le tempistiche per tale attuazione;

c) la descrizione e le ragioni che giustificano l'accettazione di eventuali rischi residui al trattamento.

A livello generale, i **soggetti essenziali** di cui all'allegato 2 della normativa di recepimento della Direttiva Nis 2 devono adottare un **numero maggiore di misure di sicurezza di base** (43 misure/116 requisiti) **rispetto ai soggetti importanti** (37 misure/87 requisiti) di cui all'allegato 1.

Inoltre, la **differenza principale** tra soggetti essenziali e importanti risiede nel **regime di vigilanza**: i primi subiscono controlli ex-ante (preventivi) e rigorosi, mentre i secondi ex-post (reattivi). Sebbene entrambi debbano applicare sostanzialmente le stesse misure di base, per i soggetti essenziali sono previsti un **maggior livello di controllo e supervisione, adempimenti più stringenti e sanzioni più elevate** rispetto ai soggetti importanti.

Q&A

Contatti: