

# UPSKILL

*Società dedicata alla formazione e  
ai servizi formativi di*

ergonGROUP

# Chi siamo

Siamo Upskill, società di ErgonGroup **specializzata nella formazione e nei servizi formativi**. Grazie all'eredità acquisita dalla holding, abbiamo sviluppato una consolidata esperienza, in aziende di ogni settore e dimensione, **nella gestione dell'intero processo formativo**.

Non ci limitiamo a trasferire nuove competenze, ma a saperle utilizzare in modalità vincente.

## SIAMO PARTE DI ERGONGROUP

Nata come **"società del sapere"**, con gli anni e l'esperienza ErgonGroup ha sviluppato un know-how sempre più esteso in risposta alle esigenze di persone, aziende e istituzioni che necessitano di crescere colmando gap, acquisendo tecnologie, sviluppando eccellenze individuali di team e di organizzazione.

Oggi ErgonGroup rinnova la propria promessa al mercato evolvendo il proprio modello di business in **tre grandi società votate all'iper-specializzazione**:

- **Resolve** **divisione dedicata alla consulenza** che affianca imprenditori e manager, del settore pubblico e privato, nel delineare strategie e calarle nelle organizzazioni in modo semplice, tecnologico e sostenibile.
- **Jobros**, **agenzia per il lavoro non convenzionale** specializzata nel mondo Digital & IT che accompagna persone e imprese nella loro crescita.

**RESOL/E**  
Consulenza strategica,  
digitalizzazione e sostenibilità

**UPSKILL**  
Formazione per le imprese  
e le persone

**JObros**  
Agenzia per il lavoro  
non convenzionale

---

**ergonGROUP**  
Più competenti. Più intelligenti. Più veloci.

**UPSKILL**



## PRESENTIAMOCI

**SPEAKER**  
**IVANO DI SANTO**

**Consulente di sicurezza informatica**

Consulente di sicurezza informatica e componente della sezione della supply chain finance di AITI. Membro fondatore dell'Associazione "Digital Security Festival" che ha lo scopo di divulgare i concetti della sicurezza informatica a vari livelli della società.



# OGGI PARLIAMO DI:

- 1. Panoramica sulla Direttiva NIS2**
- 2. Differenze tra NIS1 e NIS2**
- 3. Come essere compliant con la NIS2**
- 4. Coinvolgimento della supply chain**



# **Conformità alla NIS2 come prepararsi al nuovo scenario**

# 📈 Contesto e Obiettivi della NIS2 - Breve storia della NIS

**NIS (2016):** La prima direttiva NIS è stata adottata nel luglio 2016 e si concentrava su tre aspetti principali:

- ❖ Aumentare le capacità nazionali di cybersecurity dei singoli Stati membri
- ❖ Migliorare la cooperazione tra gli Stati membri
- ❖ Imporre obblighi di sicurezza e notifiche agli operatori di servizi essenziali e ai fornitori di servizi digitali



# Contesto e Obiettivi della NIS2 – Motivazioni dietro l'aggiornamento alla NIS2

- Evoluzione rapida delle minacce informatiche
- Pandemia COVID-19



Adozione della NIS2  
nel **dicembre 2022**



## 📈 Contesto e Obiettivi della NIS2 - Obiettivi chiave della NIS2

Ampliamento  
del campo di  
applicazione

Norme più  
rigorose

Migliore  
cooperazione

Sanzioni più  
severe

## ↑ Implicazioni Generali - Soggetti

La presente direttiva si applica ai soggetti pubblici o privati delle tipologie di cui all'allegato I o II che sono considerati medie imprese ai sensi all'articolo 2, paragrafo 1, dell'allegato alla raccomandazione 2003/361/CE, o che superano i massimali per le medie imprese di cui al paragrafo 1 di tale articolo, e che prestano i loro servizi o svolgono le loro attività all'interno dell'Unione

### **Articolo 2**

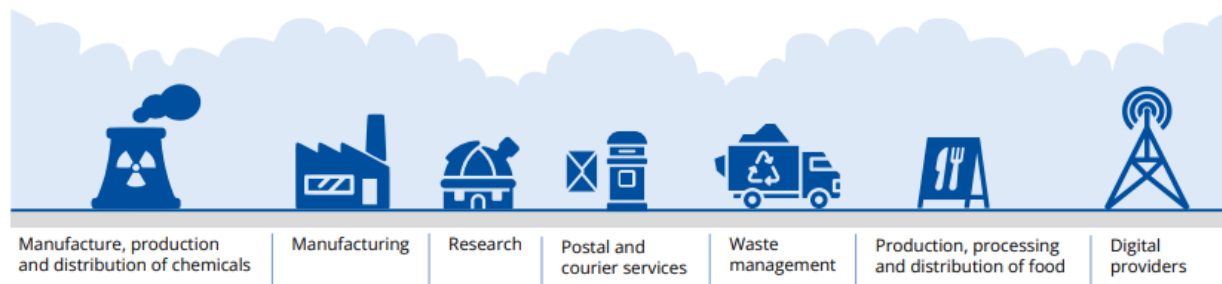
Effettivi e soglie finanziarie che definiscono le categorie di imprese

1. La categoria delle microimprese, delle piccole imprese e delle medie imprese (PMI) è costituita da imprese che occupano meno di 250 persone, il cui fatturato annuo non supera i 50 milioni di euro oppure il cui totale di bilancio annuo non supera i 43 milioni di euro.
2. Nella categoria delle PMI si definisce piccola impresa un'impresa che occupa meno di 50 persone e realizza un fatturato annuo o un totale di bilancio annuo non superiori a 10 milioni di euro.  
...(omissis)

# Implicazioni Generali - Settori interessati



High criticality sectors



Other critical sectors

# ⬆ Implicazioni Generali - Principali cambiamenti introdotti





# Differenze tra NIS e NIS2

# ⬆ Differenze tra NIS e NIS2 - Copertura Estesa

## Settori e servizi aggiuntivi coinvolti

- **Ampliamento dei Settori Coperti**
  - Servizi postali e logistici
  - Gestione dei rifiuti
  - Industria alimentare (produzione e distribuzione)
  - Produzione di sostanze chimiche
  - Amministrazione pubblica e spazi pubblici
- **Maggiore Inclusività per le PMI Critiche**
- **Riorganizzazione delle Categorie di Settori**
- **Miglioramento della Sicurezza della Catena di Fornitura**
- **Aggiornamento dei Requisiti per i Servizi Digitali**

## Requisiti Rafforzati – Maggiore attenzione alla gestione del rischio



Miglioramento  
nella Gestione  
del Rischio



Valutazione della  
Sicurezza nella  
Catena di  
Fornitura



Requisiti di Cyber  
Hygiene



Piani di  
Continuità  
Operativa e  
Recupero



Obblighi di  
Segnalazione più  
Stringenti



Formazione e  
Consapevolezza

## Requisiti Rafforzati - Rafforzamento delle misure di sicurezza



Adozione di Standard di Sicurezza Avanzati



Protezione dei Sistemi Operativi Critici



Sicurezza delle Reti e Monitoraggio Continuo



Resilienza della Catena di Fornitura



Protezione contro gli Attacchi DDoS e Malware



Test Periodici di Sicurezza



Miglioramento della Governance e delle Responsabilità

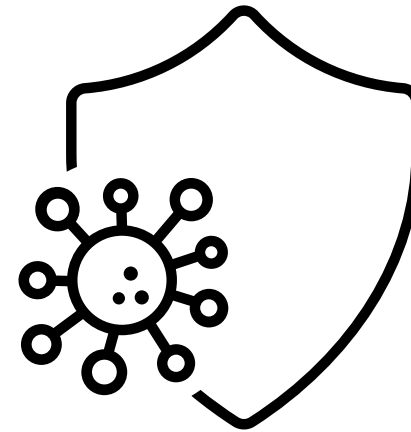


Obiettivo del Rafforzamento



# Supervisione e Enforcement – Nuove responsabilità per le autorità competenti

- Poteri di Supervisione Ampliati
- Valutazioni di Conformità
- Piani di Risposta alle Emergenze
- Imposizione di Sanzioni Severe
- Coordinamento tra Stati Membri
- Supporto al Settore Privato
- Raccolta e Analisi dei Dati sugli Incidenti,
- Obiettivo delle Nuove Responsabilità

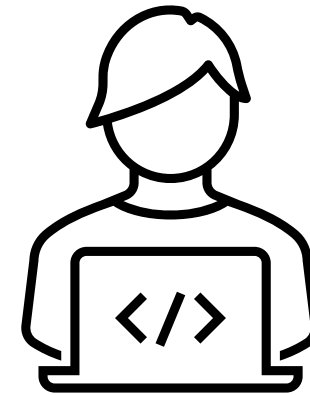




# **Come essere compliant con la NIS2**

# Valutazione del Rischio – Identificazione delle vulnerabilità e minacce

- Identificazione delle Vulnerabilità
- Identificazione delle Minacce
  - Attacchi informatici
  - Minacce fisiche
  - Minacce interne
- Processo di Valutazione del Rischio
- Implementazione delle Misure di Sicurezza
- Obbligo di Reportistica



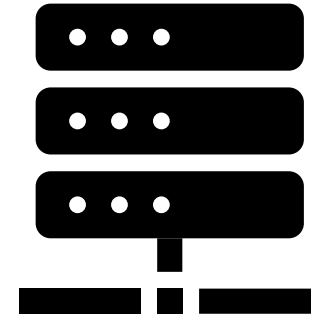
# ⬆️ Valutazione del Rischio – Implementazione di piani di gestione del rischio

- Identificazione dei rischi
- Valutazione delle probabilità e impatti
- Definizione dei controlli e delle misure di mitigazione
- Monitoraggio continuo e aggiornamenti



# Valutazione del Rischio – Implementazione di piani di gestione del rischio

- Definizione degli obiettivi e delle priorità
- Identificazione e classificazione dei rischi
- Adozione di misure di sicurezza
- Piani di risposta e recupero
- Test e simulazioni
- Comunicazione e reportistica
- Monitoraggio e miglioramento continuo



## ↑↑ Misure di Sicurezza – Adozione di misure tecniche e organizzative

Le **misure tecniche** si riferiscono alle soluzioni tecnologiche che un'organizzazione può implementare per prevenire, rilevare, e rispondere ai rischi informatici. Alcune delle misure tecniche previste dalla NIS 2 sono:

- Protezione perimetrale
- Crittografia
- Autenticazione forte e gestione degli accessi
- Monitoraggio e rilevamento degli incidenti
- Gestione delle vulnerabilità
- Backup e recupero dei dati
- Segmentazione della rete

## ↑↑ Misure di Sicurezza – Adozione di misure tecniche e organizzative

Le **misure organizzative** riguardano le politiche, i processi e la gestione interna che l'organizzazione deve implementare per garantire la sicurezza delle proprie reti e sistemi informativi. Queste misure includono:

- Gestione dei rischi e della sicurezza informatica
- Politiche di sicurezza informatica
- Formazione e sensibilizzazione del personale
- Controllo dei fornitori e terze parti
- Piani di continuità operativa
- Comunicazione e collaborazione con le autorità competenti

## ↑↑ Misure di Sicurezza – Adozione di misure tecniche e organizzative

Le misure tecniche e organizzative devono essere **proporzionate** al rischio che l'organizzazione affronta



Adottare misure efficaci nel ridurre i rischi

- Dimensioni
- Complessità
- Risorse a disposizione



# Misure di Sicurezza – Monitoraggio continuo e aggiornamenti regolari

## Elementi Chiave del Monitoraggio Continuo:

- Monitoraggio in tempo reale
- Monitoraggio delle vulnerabilità
- Rilevamento delle anomalie
- Analisi dei log
- Sicurezza della rete e monitoraggio del traffico

# ↑↑ Misure di Sicurezza – Monitoraggio continuo e aggiornamenti regolari

## Obblighi secondo la NIS2 per il Monitoraggio:

- Monitorare continuamente le proprie reti e sistemi informativi
- Adottare misure di rilevamento
- Raccogliere e archiviare i log di sicurezza per un periodo sufficiente a garantire l'analisi post-incidente e il rispetto delle normative
- Utilizzare tecnologie di rilevamento avanzate (ad es. SIEM)

# ↑↑ Misure di Sicurezza – Monitoraggio continuo e aggiornamenti regolari

## **Aggiornamenti Regolari:**

- Patch Management
- Aggiornamento delle definizioni antivirus e antimalware
- Aggiornamenti dei sistemi di monitoraggio e sicurezza
- Aggiornamento della configurazione di sicurezza
- Aggiornamento delle procedure di sicurezza



# Documentazione e Reportistica – Preparazione e mantenimento di documentazione adeguata

## 1. Preparazione e Mantenimento della Documentazione Adeguata

- Politiche di sicurezza informatica
- Piani di gestione del rischio
- Misure di sicurezza adottate
- Formazione del personale
- Gestione delle vulnerabilità e dei fornitori



# Documentazione e Reportistica – Preparazione e mantenimento di documentazione adeguata

## 2. Obblighi di Reportistica sugli Incidenti di Sicurezza

- Notifica degli incidenti
- Rapporti e follow-up post-incidente
- Documentazione per audit e controlli



# Documentazione e Reportistica – Preparazione e mantenimento di documentazione adeguata

## 3. Documentazione della Conformità alla NIS2

- Verifiche interne e audit di sicurezza
- Attività di sensibilizzazione e formazione
- Sistemi di monitoraggio
- Aggiornamenti delle politiche e procedure



# Documentazione e Reportistica – Preparazione e mantenimento di documentazione adeguata

## 4. Obblighi Specifici di Reportistica e Comunicazione con le Autorità

- Notifiche agli enti di regolamentazione
- Comunicazione con i clienti e partner



# Documentazione e Reportistica – Requisiti di segnalazione degli incidenti

## Definizione di Incidente di Sicurezza

La direttiva NIS 2 definisce un incidente di sicurezza come un evento che compromette la sicurezza di reti e sistemi informativi e che ha un impatto significativo sulla continuità dei servizi essenziali.

- Attacchi informatici (es. malware, ransomware, DDoS)
- Data breaches (violazioni di dati sensibili)
- Interruzioni o malfunzionamenti dei sistemi che compromettono la disponibilità dei servizi critici
- Attacchi mirati (es. attacchi alla supply chain o agli approvvigionamenti)

Un incidente è significativo quando ha un impatto negativo sui servizi offerti o quando potrebbe danneggiare la sicurezza delle informazioni o dei dati trattati



# Documentazione e Reportistica – Requisiti di segnalazione degli incidenti

## Obbligo di Notifica agli Organismi Competenti

l'obbligo per le organizzazioni di segnalare gli incidenti significativi alle autorità competenti, come i CERT (Computer Emergency Response Team) nazionali o altre entità designate per la gestione della sicurezza informatica

Tempistiche di notifica:

- Entro 24 ore dalla scoperta dell'incidente
- Relazione dettagliata entro 72 ore
- In Italia <https://www.csirt.gov.it/segnalazione>

## Documentazione e Reportistica - Requisiti di segnalazione degli incidenti

Dettagli da includere nella segnalazione:

**Descrizione dell'incidente**

**Gravità e impatto**

**Cause e origine dell'incidente**

**Azioni intraprese**

**Piani di recupero e prevenzione futura**

**Impatto sul business e sugli utenti**



# Documentazione e Reportistica – Requisiti di segnalazione degli incidenti

## **Reportistica Post-Incidente (cosa deve contenere la relazione finale)**

1. Un'analisi delle cause radice (*root cause analysis*)
2. Le lezioni apprese dall'incidente, comprese eventuali debolezze identificate nei sistemi di difesa
3. Le misure correttive e preventive intraprese per ridurre la probabilità di futuri incidenti simili



# Documentazione e Reportistica – Requisiti di segnalazione degli incidenti

## **Riservatezza e Protezione delle Informazioni**

- Deve avvenire in un contesto di protezione delle informazioni sensibili

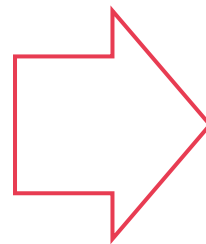
## **Cooperazione tra le Autorità e le Organizzazioni**

- La segnalazione tempestiva consente alle autorità di attivare misure di supporto, di monitorare la situazione e di ridurre i rischi di incidenti su larga scala.



## Formazione e Consapevolezza – Programmi di formazione per il personale

**La formazione del personale deve  
essere continua, mirata e documentata**



**Obblighi Generali di Formazione e  
Consapevolezza:**

- Migliorare la consapevolezza
- Garantire che i dipendenti comprendano
- Formare in modo specifico il personale



# Formazione e Consapevolezza – Programmi di formazione per il personale

Tipologie di Formazione Necessaria

## 1. Formazione Generale sulla Sicurezza Informatica

- Phishing
- Uso sicuro delle password
- Sicurezza dei dispositivi mobili
- Protezione dei dati



# Formazione e Consapevolezza – Programmi di formazione per il personale

## 2. Formazione Avanzata per il Personale Tecnico e IT

- Gestione delle vulnerabilità
- Rilevamento delle minacce
- Gestione degli incidenti di sicurezza
- Monitoraggio delle reti e dei sistemi



# Formazione e Consapevolezza – Programmi di formazione per il personale

## 3. Formazione Avanzata per il Personale Tecnico e IT

- Gestione delle vulnerabilità
- Rilevamento delle minacce
- Gestione degli incidenti di sicurezza
- Monitoraggio delle reti e dei sistemi



# Formazione e Consapevolezza – Programmi di formazione per il personale

## 4. Formazione sui Piani di Continuità Operativa e Recupero Disastri

- Piani di risposta agli incidenti
- Esercitazioni di simulazione



# Formazione e Consapevolezza – Programmi di formazione per il personale

## 5. Formazione per la Leadership e la Gestione dei rischi aziendali

- Gestione dei rischi aziendali
- Conformità normativa e regolamentare
- Comunicazione in caso di incidente



# Formazione e Consapevolezza – Programmi di formazione per il personale

## Frequenza e Aggiornamento della Formazione

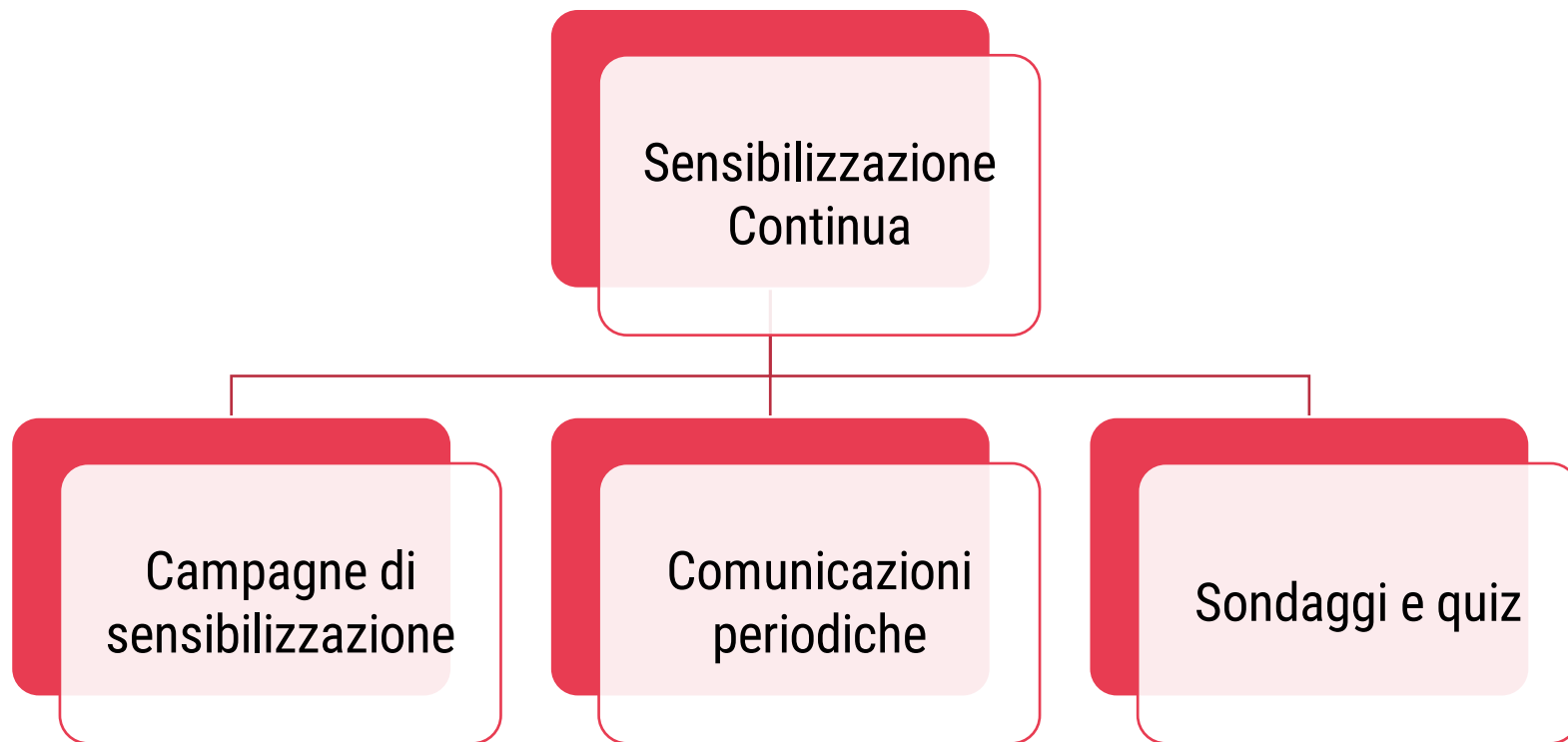
- deve essere aggiornata regolarmente e periodicamente
- simulazioni e gli esercizi pratici

## Documentazione della Formazione

- I corsi completati dal personale
- I materiali di formazione
- I risultati delle esercitazioni



# Formazione e Consapevolezza – Programmi di formazione per il personale





# Formazione e Consapevolezza - Sensibilizzazione sull'importanza della sicurezza informatica

Obblighi di Sensibilizzazione secondo la Direttiva NIS 2

1. Importanza della Sensibilizzazione sulla Sicurezza Informatica
2. Iniziative di Sensibilizzazione secondo la NIS 2
3. Sensibilizzazione per Diversi Livelli dell'Organizzazione
4. Integrazione della Sensibilizzazione nella Cultura Aziendale
5. Monitoraggio e Valutazione dell'Efficacia



# Coinvolgimento della Supply Chain



# Importanza della Supply Chain nella Sicurezza Informatica – Come la supply chain può rappresentare un punto di vulnerabilità

## La Supply Chain come Punto di Vulnerabilità

- Fornitori con livelli di sicurezza più bassi
- Sofisticati attacchi di supply chain hacking
- Software e componenti compromessi
- Inadeguata gestione dei dati
- Relazioni di fiducia deboli



# Importanza della Supply Chain nella Sicurezza Informatica – Come la supply chain può rappresentare un punto di vulnerabilità

## Sicurezza della Supply Chain

- Identificare e valutare i rischi legati alla supply chain
- Estendere i controlli di sicurezza ai fornitori:
- Gestire e monitorare i fornitori critici
- Definire procedure di gestione degli incidenti con i fornitori
- Rendere trasparenti le pratiche di sicurezza
- Integrare la sicurezza della supply chain nei processi di gestione del rischio



# Importanza della Supply Chain nella Sicurezza Informatica – Come la supply chain può rappresentare un punto di vulnerabilità

## Strategie per Ridurre i Rischi dalla Supply Chain

- Valutazione dei fornitori
- Politiche di sicurezza
- Monitoraggio continuo
- Piani di risposta agli incidenti comuni
- Test di resilienza e simulazioni



# Importanza della Supply Chain nella Sicurezza Informatica – Esempi di incidenti di sicurezza legati alla supply chain

Alcuni incidenti noti

1. L'incidente SolarWinds (2020)
2. L'incidente Kaseya (2021)
3. L'incidente con il Fornitore di Chip di Taiwan (2020)
4. Attacco a Target (2013)
5. L'incidente Log4j (2021)



# Requisiti per la Supply Chain secondo la NIS2 – Valutazione dei fornitori

## Requisiti per la Supply Chain

- **Identificazione e Valutazione dei Rischi nella Supply Chain**
  - **Mappatura dei fornitori critici**
  - **Valutazione dei rischi associati ai fornitori**
    - La **sicurezza informatica** dei fornitori
    - La **resilienza operativa** del fornitore in caso di attacchi informatici o altri incidenti
    - La gestione dei **dati sensibili** e la conformità alle normative di protezione dei dati, come il **GDPR**
    - La **continuità del servizio** e la capacità di recupero in caso di incidenti



# Requisiti per la Supply Chain secondo la NIS2 – Valutazione dei fornitori

## Adozione di Misure di Sicurezza per i Fornitori

- Obbligo di misure di sicurezza
- Sicurezza nella fornitura di servizi
  - Protezione contro gli attacchi informatici.
  - Messa in atto di meccanismi di monitoraggio e rilevamento delle anomalie.
  - Capacità di risposta agli incidenti e gestione delle crisi
- Contratti con clausole di sicurezza



# Requisiti per la Supply Chain secondo la NIS2 – Valutazione dei fornitori

## Monitoraggio e Revisione dei Fornitori Critici

- Monitoraggio continuo
- Revisione periodica
- Gestione delle vulnerabilità





# Requisiti per la Supply Chain secondo la NIS2 – Valutazione dei fornitori

## Gestione degli Incidenti di Sicurezza e Notifica

La NIS 2 pone un'attenzione particolare alla gestione degli **incidenti di sicurezza**, specialmente quando coinvolgono i fornitori. Le organizzazioni sono obbligate a **notificare gli incidenti significativi** alle autorità competenti e agli stakeholder. Se un incidente coinvolge un fornitore, l'organizzazione deve collaborare per risolverlo rapidamente e garantire che le **misure correttive** vengano adottate in modo appropriato

- Notifica degli incidenti
- Collaborazione con i fornitori
- Piani di risposta e continuità



# Requisiti per la Supply Chain secondo la NIS2 – Valutazione dei fornitori

## Gestione del Rischio Complessivo della Supply Chain

- Integrazione nei processi aziendali
- Comunicazione dei rischi



# Requisiti per la Supply Chain secondo la NIS2 – Inclusione dei fornitori nei piani di continuità operativa e di gestione del rischio

Requisiti della NIS 2 per l'Inclusione dei Fornitori nei Piani di Continuità Operativa e Gestione del Rischio

Integrazione dei Fornitori nei Piani di Continuità Operativa

- Identificazione dei fornitori critici
- Definizione di interruzioni possibili nella supply chain
- Misure di mitigazione
- Contingency planning (piani di emergenza)



## Requisiti per la Supply Chain secondo la NIS2 - Inclusione dei fornitori nei piani di continuità operativa e di gestione del rischio

### Inclusione dei Fornitori nei Piani di Gestione del Rischio (ERM)

- Valutazione dei rischi legati ai fornitori
- Gestione del rischio condiviso
- Monitoraggio continuo del rischio
- Gestione delle vulnerabilità e incidenti



# Requisiti per la Supply Chain secondo la NIS2 - Inclusione dei fornitori nei piani di continuità operativa e di gestione del rischio

## Comunicazione e Collaborazione con i Fornitori in Caso di Incidenti

- Protocollo di notifica tempestiva
- Collaborazione per la gestione degli incidenti
- Test di resilienza



# Requisiti per la Supply Chain secondo la NIS2 - Inclusione dei fornitori nei piani di continuità operativa e di gestione del rischio

## Fornitori e Contratti: Clausole di Continuità e Sicurezza

- SLA e contratti di sicurezza: I contratti
- Clausole di risposta agli incidenti



# Strategie di Coinvolgimento – Comunicazione e collaborazione con i fornitori

## Strategie di Coinvolgimento nella NIS 2: Comunicazione e Collaborazione con i Fornitori

### 1. Stabilire Canali di Comunicazione Sicuri e Chiari

- Canali di comunicazione protetti
- Punti di contatto dedicati

### 2. Accordi di Sicurezza e SLA con i Fornitori

- Clausole di sicurezza nei contratti
- Monitoraggio e conformità

# ⬆️ Strategie di Coinvolgimento – Comunicazione e collaborazione con i fornitori

## 3. Condivisione di Informazioni sulla Sicurezza

- Condivisione tempestiva delle vulnerabilità
- Collaborazione proattiva su minacce e attacchi

# ⬆️ Strategie di Coinvolgimento – Comunicazione e collaborazione con i fornitori

## 4. Piani di Risposta agli Incidenti Condivisi

- Piani di risposta agli incidenti congiunti
- Notifica tempestiva degli incidenti
- Test e simulazioni

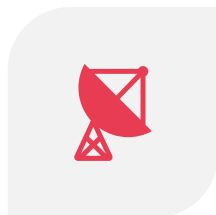
# ⬆️ Strategie di Coinvolgimento – Comunicazione e collaborazione con i fornitori

## 5. Monitoraggio e Gestione dei Fornitori Critici

- Monitoraggio continuo della sicurezza dei fornitori
- Valutazioni del rischio della supply chain



# Strategie di Coinvolgimento – Implementazione di standard e requisiti di sicurezza per la supply chain



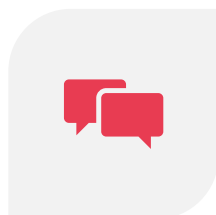
STABILIRE CANALI DI  
COMUNICAZIONE  
SICURI E CHIARI



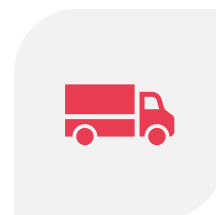
ACCORDI DI  
SICUREZZA E SLA CON  
I FORNITORI



CONDIVISIONE DI  
INFORMAZIONI SULLA  
SICUREZZA



PIANI DI RISPOSTA  
AGLI INCIDENTI  
CONDIVISI



MONITORAGGIO E  
GESTIONE DEI  
FORNITORI CRITICI

# ⬆️ Strategie di Coinvolgimento – Monitoraggio e audit periodici dei fornitori

Strategie di Coinvolgimento nella NIS 2: Monitoraggio e Audit Periodici dei Fornitori

1. Monitoraggio Continuo dei Fornitori Critici
2. Audit Periodici dei Fornitori
3. Valutazione Continua delle Performance di Sicurezza dei Fornitori
4. Revisione e Aggiornamento degli Accordi con i Fornitori
5. Risposta agli Incidenti e Cooperazione con i Fornitori

# ↑ Sanzioni

## Tipologie di Sanzioni

### 1. Sanzioni Amministrative Pecuniarie:

le sanzioni pecuniarie sono una delle forme principali di punizione per le violazioni della NIS 2. Queste sanzioni sono stabilite dalle autorità competenti e variano in base alla **gravità dell'infrazione**, alla **dimensione dell'organizzazione** e alle **circostanze del caso**.

- **Multe fino a 10 milioni di euro** o il 2% del fatturato annuo globale: Questa sanzione si applica per le violazioni più gravi, come il mancato rispetto degli obblighi di sicurezza, il non invio tempestivo delle notifiche in caso di incidente di sicurezza, o l'assenza di piani di gestione del rischio.
- **Multe fino a 7 milioni di euro** o il 1,4% del fatturato annuo globale: Sanzioni per violazioni minori, come la non attuazione di misure preventive di sicurezza o l'insufficiente collaborazione con le autorità competenti in caso di incidente.



# ↑ Sanzioni

## 2. Sanzioni per Mancato Rispetto degli Obblighi di Notifica

Una violazione grave della NIS 2 è il **mancato rispetto dell'obbligo di notifica** in caso di incidente di sicurezza che abbia un impatto significativo. Le organizzazioni devono notificare gli incidenti entro **72 ore** dalla loro rilevazione, e se non lo fanno, possono essere soggette a **sanzioni pecuniarie**.

Le **sanzioni** possono essere applicate quando l'incidente non viene notificato tempestivamente o in modo incompleto, impedendo alle autorità di prendere azioni correttive tempestive.



# Sanzioni

**3. Sanzioni per Non Adozione di Misure di Sicurezza Appropriate**

**4. Ordini di Correzione e Misure Sostitutive**

**5. Sanzioni per Mancato Coinvolgimento dei Fornitori Critici**

**6. Sanzioni per la Non Cooperazione con le Autorità Competenti**

**7. Sanzioni per la Violazione della Privacy e della Protezione dei Dati**



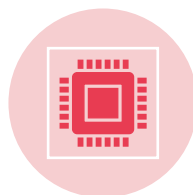


**DECRETO LEGISLATIVO**  
**4 settembre 2024, n. 138**

# ↑ Effetti del recepimento



Recepisce la Direttiva NIS2 in Italia



Stabilisce misure per assicurare un livello elevato di sicurezza informatica in ambito nazionale



Contribuisce a migliorare il funzionamento del mercato interno

# ↑ Principali Adempimenti del Decreto



**Auto-registrazione:** Le aziende devono auto-registrarsi sulla piattaforma dell'Agenzia per la Cybersicurezza Nazionale (ACN) indicando le proprie attività e servizi



**Conformità:** L'ACN valuterà la conformità delle aziende alla NIS2 e fornirà indicazioni per l'adeguamento



**Scadenze:** Le aziende devono completare la registrazione entro il 31 marzo 2025 e adempiere agli obblighi di adeguamento entro 9 mesi per gli incidenti e 18 mesi per le misure di sicurezza

# ↑ Principali Adempimenti del Decreto - Scadenze

[SOGGETTI] Registrazione sulla piattaforma ACN (articolo 7, comma 1, articolo 42, comma 1, lettera a):

- entro il 17 gennaio 2025 per i fornitori di servizi di sistema dei nomi di dominio, i gestori di registri dei nomi di dominio di primo livello, i fornitori di servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, fornitori di servizi di data center, fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network che rientrano nell'ambito di applicazione del decreto (v. FAQ 1.4);
- entro il 28 febbraio 2025 per tutti gli altri soggetti che rientrano nell'ambito di applicazione del decreto (v. FAQ 1.4).

[AUTORITÀ NAZIONALE COMPETENTE NIS] Entro metà aprile 2025:

- costituzione dell'elenco dei soggetti NIS e notifica agli stessi della loro inclusione (articolo 7, commi 2 e 3);
- adozione degli obblighi di base in materia di misure di sicurezza informatica e notifica di incidenti.

[SOGGETTI] Entro metà maggio 2025, trasmissione e aggiornamento, tempestivo (comunque non oltre 14 giorni dalla modifica) delle informazioni dei soggetti NIS (articolo 7, commi 4, 5 e 7).

[SOGGETTI] Entro gennaio 2026 (entro 9 mesi dalla ricezione della notifica di inserimento nell'elenco dei soggetti NIS), adempimento agli obblighi di base in materia di notifica di incidente.

[SOGGETTI] Entro ottobre 2026 (entro 18 mesi dalla ricezione della notifica di inserimento nell'elenco dei soggetti NIS), adempimento agli obblighi di base in materia di sicurezza informatica.

<https://www.acn.gov.it/portale/faq/nis>



# UPSKILL

by ErgonGroup

**BENVENUTO  
AL LIVELLO  
SUCCESSIVO**

[www.upskill-formazione.it](http://www.upskill-formazione.it)