# Adempimenti NIS 2

## Guida pratica e suggerimenti operativi per le aziende interessate

**Ispettore Antonio Fiorentino**

**Sezione Operativa Sicurezza Cibernetica Brescia**

# Un ecosistema normativo in evoluzione

## NIS2 - UE 2022/2555

Amplia la disciplina della NIS 2016, estendendo l'ambito a nuovi settori critici e incrementando le sanzioni. Impone misure tecniche e organizzative di sicurezza, notifiche di incidenti e responsabilità gestionali. In Italia è stata recepita il 16 ottobre 2024, con D.Lgs. 138/2024, che individua **ACN** come autorità nazionale.

## Digital Operational Resilience Act - DORA

Il Regolamento (UE) 2022/2554 tratta la resilienza operativa digitale nel settore finanziario. Prevede requisiti per la gestione del rischio ICT, test di resilienza, notifiche di incidenti e supervisione dei fornitori. Applicabile dal 17 gennaio 2025, è supervisionato da **Banca d'Italia**, **IVASS** e **CONSOB** con coordinamento **ACN**.

## Critical Entities Resilience – CER

Rafforza la resilienza fisica e digitale delle entità critiche in settori come energia, sanità e trasporti. Impone analisi del rischio, piani di resilienza e misure preventive. In Italia è stata recepita il 18 ottobre 2024, con D.Lgs. 134/2024, individuando l'istituzione del Punto di contatto unico (PCU) e designando due Autorità Settoriali Competenti (ASC).

## Data Governance Act (DGA) – UE 2022/0868 Data Act (DA) – UE 2023/2854

DGA e Data Act definiscono regole per la gestione e condivisione dei dati in Europa. Il DGA istituisce gli "intermediari dei dati" e il Data Act promuove accesso e interoperabilità dei dati. Entrambe le normative rafforzano la sovranità e competitività dei dati europei.
Il DGA è applicabile dal 24 settembre 2023, e il DA dal settembre 2025.

## eIDAS 2.0 – UE 2024/1183 e Identità Digitale Europea

Regolamento eIDAS (electronic Identification, Authentication and Trust Services) è il quadro che stabilisce regole e standard per l'identificazione elettronica e i servizi fiduciari nei paesi membri. Entrato in vigore il 20 maggio 2024, avviando un processo di adeguamento che culminerà entro fine 2026 con l'introduzione dell'European Digital Identity Wallet (EUDI Wallet)

## Digital Services Act – DSA – UE 2022/2065 Digital Markets Act – DMA – UE 2022/1925

Il DSA disciplina i servizi digitali e le piattaforme online nell'Unione Europea per rafforzare la tutela degli utenti online. Il DMA introduce un nuovo assetto normativo per i mercati digitali europei, imponendo ai "gatekeeper" regole precise per garantire concorrenza e trasparenza. Il DSA è applicabile dal 17 febbraio 2024, e il DMA dal 2 maggio 2023

## AI Act – UE 2024/1689

Regola lo sviluppo, l'immissione sul mercato e l'uso dei sistemi di IA, per livello di rischio. Stabilisce obblighi di trasparenza, qualità dei dati e sorveglianza umana. Entrato in vigore l'1 agosto 2024, in Italia recepito con D.Lgs. 132/2025in vigore dal 10 ottobre 2025. necessario che le imprese che adottano sistemi di IA predispongano presidi e misure per una governance efficace.

## Cyber Resilience Act – CRA – UE 2024/2847

Il CRA introduce requisiti di sicurezza per i prodotti digitali, imponendo obblighi di progettazione sicura, gestione delle vulnerabilità e aggiornamenti software. Mira a un mercato sicuro basato su "security by design". Entrato in vigore il 10 dicembre 2024. L'attuazione completa è prevista per l'11 dicembre 2027, mentre alcuni obblighi specifici diventeranno effettivi dall'11 settembre 2026.

## European Accessibility Act - UE 2019/882

Introduce requisiti di accessibilità per diverse categorie di prodotti e servizi digitali con l'obbligo per gli operatori economici di garantire la conformità ai requisiti di accessibilità.
Dal 28 giugno 2025 saranno applicabili le disposizioni contenute nel d.lgs. 82/2022.

# La domanda che non dovremmo rimandare

Se in questo momento subissimo un attacco ransomware che cifrasse tutti i nostri sistemi

- sapremmo quali processi di business ripristinare per primi?
- sapremmo entro quanto tempo devono essere ripristinati?
- sapremmo qual è la perdita massima di dati accettabile per i Clienti?
- Le nostre misure di sicurezza attuali sono efficaci?

**Se la risposta non è immediata,**
**non stiamo governando la continuità dei nostri servizi né proteggendo il business**

# Continuità, sicurezza e impatti sul business

Il quadro normativo (NIS, DORA) e il panorama delle minacce attuali (cyber attack, guasti, supply chain) impongono alle aziende di governare la continuità e la sicurezza dei servizi ICT.

Interruzioni e violazioni non sono solo un problema tecnico, generano conseguenze immediate e concatenate:

→ Indisponibilità dei servizi per clienti e controparti

→ Mancati flussi finanziari e impatti economici diretti

→ Rischio reputazionale e perdita di fiducia

→ Obblighi di segnalazione e scrutinio delle Autorità di Vigilanza

# Il recepimento in Italia

In Italia la Direttiva NIS 2 è stata recepita attraverso il **Decreto Legislativo 4 settembre 2024, n. 138** (c.d. Decreto NIS)con cui vengono stabilite misure per assicurare un elevato livello di sicurezza informatica a livello **nazionale**.

A seguito della registrazione, per le medie e grandi imprese, in alcuni casi anche le piccole e microimprese, e le Pubbliche amministrazioni a cui si applica la nuova normativa si avvia un percorso condiviso di rafforzamento della sicurezza informatica.

Per i settori si fa riferimento agli allegati I, II, III e IV del Decreto Legislativo

Le **Determinazioni ACN** completano il quadro operativo attraverso quattro allegati:

**Allegati 1 e 2** - misure di sicurezza di base rivolte ai soggetti **importanti** e essenziali

**Allegati 3 e 4** - criteri per la classificazione degli **incidenti significativi** per soggetti **importanti** e **essenziali**

# Architettura normativa ambito finanziario Italia

1. **Direttiva NIS 2 (UE) 2022/2555 – REGOLAMENTO DORA 2022/2554 (Digital Operation Resilience Act)**
   Quadro europeo di riferimento
2. **Recepimento nazionale - D.Lgs. 138/2024**
   Trasposizione italiana della Direttiva
3. **Determinazioni ACN**
   Stabiliscono modalità operative e adempimenti
4. **Allegato 1**
   **È il documento operativo centrale, contiene le 37 misure di sicurezza**
5. **Framework Nazionale per la Cybersecurity e la Data Protection - Edizione 2025 (v2.1)**
   Allineato al **NIST CSF**, dettaglia i requisiti operativi delle misure di sicurezza (87 requisiti)
6. **Allegato 3**
   Schema per la classificazione degli incidenti significativi, in combinato con l'**Art. 25 del D.Lgs. 138/2024**.

# Collegamento con i framework di riferimento

- **Framework Nazionale per la Cybersecurity e la Data Protection**: strumento sviluppato in Italia per supportare le organizzazioni nella gestione dei rischi cyber, che si allinea agli obblighi del D.Lgs. 138/2024

=

- **NIST Cybersecurity Framework**: fornisce standard, linee guida e best practice per aiutare le organizzazioni a gestire i rischi legati alla sicurezza informatica, su cui si basa il **Framework Nazionale per la Cybersecurity e la Data Protection**

sovrapponibile a

- **ISO 27001/27002 e ANNEX A:** framework certificabile riconosciuto a livello internazionale che fornisce linee guida e best practice per la cybersecurity, che può essere utilizzato per implementare le misure richieste.

# Il ruolo degli organi di amministrazione

L’articolo 23 del decreto 138/2024 costituisce la disposizione cardine in materia di governance della cybersecurity

La norma introduce una responsabilità **diretta, personale** e **non delegabile** degli organi di amministrazione e direttivi nella gestione del rischio cyber

Il primo comma dell’art. 23 stabilisce che gli organi di amministrazione e direttivi dei soggetti essenziali e importanti sono tenuti a:

- approvare le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica di cui all’art. 24
- sovraintendere all’implementazione degli obblighi di cui al capo IV e dell’art. 7
- seguire una formazione specifica in materia ed offrirla periodicamente ai dipendenti

Secondo le indicazioni fornite da ACN nelle FAQ pubblicate per “organi di amministrazione e direttivi” devono intendersi i componenti del Consiglio di Amministrazione

Nel Regolamento DORA la responsabilità è in capo all’ Organo di Gestione che sarebbe il CDA

# Gli adempimenti

☑ Registrazione - Punto di contatto

☑ Aggiornamento delle informazioni - Sostituto del Punto di Contatto – Censimento dei membri degli organi di amministrazione e direttivi - Spazio di indirizzamento IP e nomi di dominio

☑ Referente CSIRT

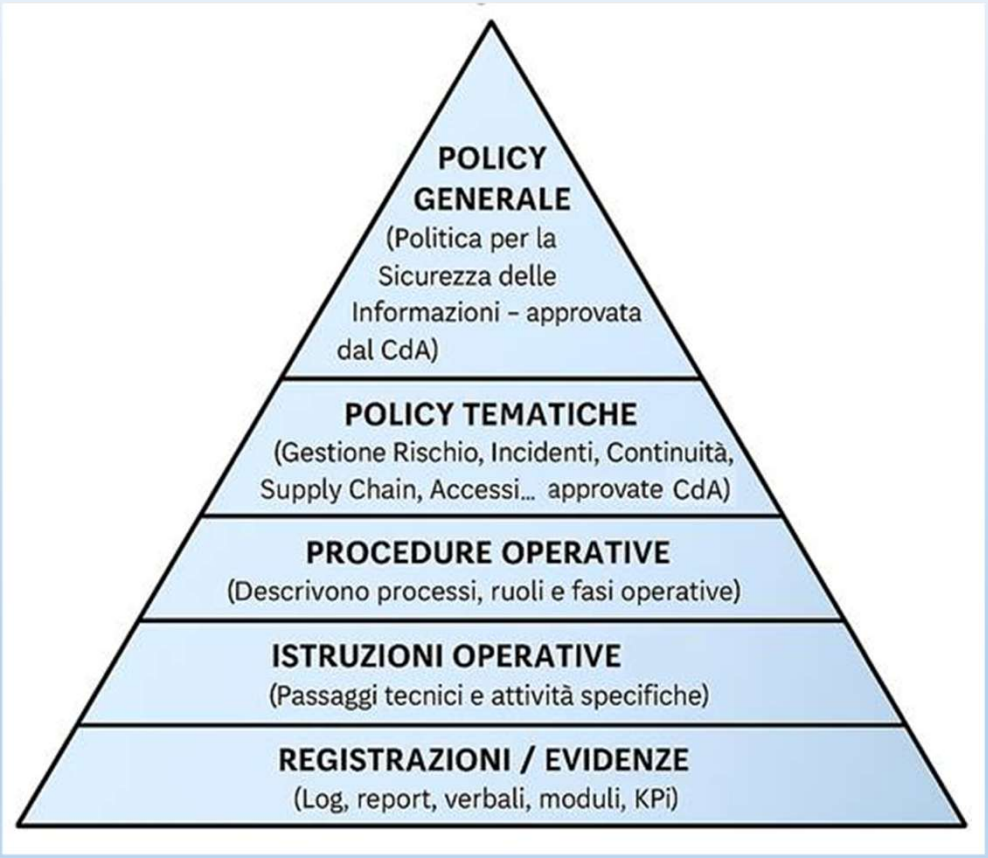
☑ Responsabile per la Cybersecurity

**1° gennaio 2026:** è entrato in vigore l'obbligo di notifica degli incidenti di sicurezza secondo le modalità definite dall'ACN

**1° ottobre 2026:** data ultima per l'adeguamento completo alla normativa NIS 2, con l'implementazione delle misure di sicurezza minime previste:

- I soggetti **importanti** dovranno adottare 37 misure, declinate in 87 requisiti, mentre i soggetti **essenziali (banche e società ambito finanziario)** 43 misure e 116 requisiti

# Approfondimento - Politiche



# Identificazione dei rischi

- Il primo passo consiste nell'**identificare gli eventi che potrebbero influire sugli obiettivi aziendali**, analizzando fonti di rischio, asset coinvolti, possibili minacce e condizioni che possono generare impatti.
- Questo comprende:
- **Individuazione degli asset e dei processi rilevanti**, inclusi dati, servizi critici, infrastrutture e fornitori
- **Identificazione delle fonti di rischio** (interne ed esterne) che possono generare eventi indesiderati
- **Analisi delle minacce** quali attacchi informatici, errori umani, interruzioni operative, malfunzionamenti tecnici

L'identificazione accurata del rischio è fondamentale per adottare contromisure adeguate e mirate

# Valutazione dell'impatto

Una volta individuati i rischi, è necessario analizzarne la gravità e le possibili conseguenze, ad esempio:

- **Impatto economico:** perdite dirette e indirette, costi di interruzione, costi di ripristino e di gestione dell'evento
- **Operativo:** indisponibilità di servizi o attività critiche, rallentamenti, riduzione della produttività
- **Legale e regolamentare:** potenziali violazioni normative, procedimenti, richieste risarcitorie
- **Reputazionale:** perdita di fiducia da parte di clienti, partner e stakeholder

L'analisi dell'impatto permette di stabilire le priorità e assegnare le giuste risorse alla protezione delle aree più critiche.

# Testare i Backup e i DR

Avere backup e piani di Disaster Recovery (DR) non è sufficiente: senza test regolari, aumenta il rischio che nel momento critico non funzionino come previsto.

Testare le procedure di ripristino da backup e da DR permette di verificare che i dati siano effettivamente recuperabili e che l'azienda possa riprendere rapidamente le attività in caso di incidente.

**Perché è fondamentale?**

- Riduce il rischio di perdita di dati dovuta a backup corrotti o incompleti
- Consente di valutare se i tempi di ripristino sono in linea con le esigenze aziendali
- Aiuta a individuare eventuali errori nelle procedure prima che diventino un problema reale

# Criptare i dati

La crittografia è una delle misure più efficaci per proteggere i dati aziendali, rendendoli inaccessibili a utenti non autorizzati. Attraverso l'uso di algoritmi matematici, la crittografia trasforma le informazioni in un formato indecifrabile, che può essere letto solo da chi possiede la chiave di decrittazione.

**Perché è importante?**

- Protegge i dati in caso di furti, attacco o accesso non autorizzato
- Protegge la riservatezza delle informazioni confidenziali e riservate
- Impedire che le informazioni vengano alterate o manipolate da soggetti non autorizzati

# La resilienza nel contesto della cybersecurity

La resilienza digitale rappresenta una componente essenziale della cybersecurity, in quanto è volta a mantenere la continuità dei servizi anche in presenza di incidenti o interruzioni. L'adozione di piani di Continuità Operativa e Disaster Recovery si basa sulla comprensione degli impatti sui servizi.

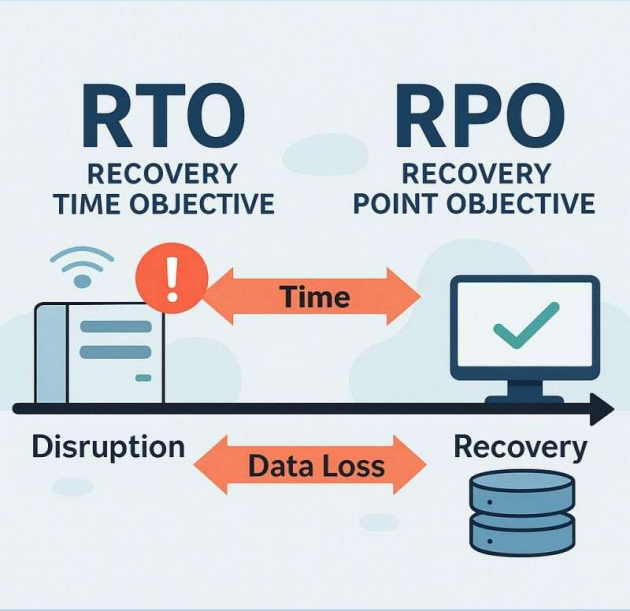
## Comprendere gli impatti

**La BIA (Business Impact Analysis) processo strategico che valuta l'impatto delle interruzioni sui processi aziendali critici, supportando la continuità o perativa e la sicurezza informatica.**

Identificazione dei processi critici e valutazione degli effetti di possibili interruzioni su servizi, dati e operatività, finalizzate alla definizione dei parametri di continiuità operativa (RTO, RPO) e dei livelli di tolleranza all'interruzione.

## Preparare la risposta

Pianificazione delle misure di Business Continuity e Disaster Recovery basate su parametri di continuità operativa identificati, specifici per ciascuna attività o servizio.



# Il tempo trasforma un disservizio in una crisi

Non tutti i processi di business hanno lo stesso peso in caso di interruzione:

→ Alcuni tollerano fermi prolungati senza impatti rilevanti (es. marketing, analisi interne)

→ Altri generano perdite economiche significative in pochi minuti (es. pagamenti, trading, tesoreria e liquidità)

Una **Business Impact Analysis** (BIA) serve per classificare i processi per criticità e definire per ciascuno:

→ Il tempo entro cui il servizio deve essere ripristinato (RTO)

→ la perdita massima tollerabile di dati/transazioni (RPO)

# Gestione degli incidenti

La gestione degli incidenti è un processo volto a rilevare, contenere e rispondere agli eventi che possono compromettere la sicurezza delle informazioni di un'azienda.

Un approccio efficace si basa su una combinazione di **tecnologia, processi e competenze**.

La capacità di rispondere rapidamente a un attacco informatico può fare la differenza tra un evento gestibile e un danno grave per l'azienda, sia in termini operativi che reputazionali.

L'obiettivo della gestione degli incidenti non è solo quello di **risolvere** il problema immediato, ma anche di **imparare** dagli eventi passati, migliorando le difese aziendali e prevenendo il ripetersi di situazioni simili.

# Incidenti significativi

Il Decreto NIS prevede l'obbligo di notifica al CSIRT Italia degli incidenti significativi

**Significativi = se hanno causato o sono in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato o se si sono ripercossi o sono in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli**

Le comunicazioni al CSIRT dovranno avvenire:

- Entro 24 ore dalla conoscenza dell'incidente con una pre-notifica (per attenuare la potenziale diffusione di incidenti e per consentire di chiedere assistenza)
- Entro 72 ore dalla conoscenza dell'incidente con aggiornamenti rispetto alle informazioni fornite con la prenotifica
- Entro 1 mese dalla conoscenza dell'incidente con una relazione finale a completamento del processo di segnalazione (questo per poter trarre insegnamenti preziosi dai singoli incidenti)

# Incident response Plan - Preparazione

La fase di preparazione è il primo passo per una gestione efficace degli incidenti informatici.

Un'organizzazione che investe nella pianificazione e nella prevenzione riduce il rischio di subire danni gravi e può affrontare gli attacchi in modo più tempestivo ed efficiente.

Questa fase prevede la creazione di un **Incident Response Plan** (IRP), un documento che stabilisce ruoli, procedure e strumenti necessari per rispondere agli incidenti di sicurezza.

È fondamentale che la direzione supporti questo processo, allocando risorse adeguate e formando un team dedicato (IRT - **Incident Response Team**), che interviene nella gestione degli incidenti.

Un altro elemento chiave della preparazione è l'implementazione di strumenti di **monitoraggio**, che consentono di rilevare tempestivamente eventuali anomalie nei sistemi.

# Identificazione

Una volta che un incidente si verifica, è essenziale individuarlo il prima possibile per limitarne le conseguenze.

La fase di identificazione si concentra sul monitoraggio e sull'analisi degli eventi sospetti, utilizzando strumenti di sicurezza come SIEM, IDS/IPS e log di sistema.

La rilevazione di un'anomalia può avvenire in modi diversi: SOC, **segnalazioni** da parte degli utenti, **analisi** delle anomalie nel traffico di rete o **confronto** con database di minacce note.

Avere un sistema di monitoraggio attivo e aggiornato aiuta a individuare rapidamente indicatori di compromissione e a classificare l'incidente in base alla sua gravità.

# Incidenti: notifiche e comunicazioni

La gestione degli incidenti informatici richiede un approccio che integri valutazione dell'evento, responsabilità organizzative e flussi di comunicazione verso autorità e stakeholder. Nella gestione dell'incidente informatico è essenziale affrontare correttamente le dinamiche di notifica e comunicazione come parte integrante della resilienza operativa digitale.

| RILEVAZIONE | VALUTAZIONE | NOTIFICA | COMUNICAZIONE |
|---|---|---|---|
| Identificazione dell'evento e attivazione dei processi interni<br>Raccolta delle informazioni iniziali | Classificazione dell'incidente<br>Coinvolgimento delle funzioni di controllo e governance | Comunicazioni verso autorità competenti<br>Coordinamento con obblighi regolatori | Informazione verso stakeholder interni ed esterni<br>Gestione coordinata delle comunicazioni di crisi |

# Organi istituzionali di riferimento

ACN

CSIRT (prenotifica e notifica NIS2)

BANCA D'ITALIA (DORA) notifica incidente informatico

GARANTE PRIVACY – denuncia entro 72 in caso di impatto su dati personali

CENTRO OPERATIVO SICUREZZA INFORMATICA POLIZIA POSTALE querela facoltativa, ma diventa opportuna in caso di attacchi ransomware e DDOS, perché è procedibile d'ufficio e di competenza della DNA.

Il 13 aprile 2026, l'Agenzia per la Cybersicurezza Nazionale (ACN) ha pubblicato due nuove determinazioni che aggiornano il quadro attuativo del D.lgs. 138/2024 (Decreto NIS).

* Determinazione n. 127434/2026 – Termini di adempimento per i nuovi soggetti NIS

Per i soggetti inseriti nell'elenco NIS nel corso del 2026:

* adozione delle misure di sicurezza di base: entro il 31 luglio 2027;

* obbligo di notifica degli incidenti significativi: dal 1° gennaio 2027;

* designazione del Referente CSIRT: entro il 31 dicembre 2026.

Per i soggetti già iscritti nel 2025 e confermati nel 2026, restano invariati i termini precedenti (18 mesi per le misure di sicurezza, 9 mesi per le notifiche, decorrenti dalla comunicazione di inserimento).

* Determinazione n. 127437/2026 – Aggiornamento della piattaforma ACN e nuovi obblighi

Il provvedimento introduce diverse novità operative:

* Fornitori rilevanti NIS: viene definita questa nuova categoria, che comprende i fornitori di servizi/prodotti ICT o la cui interruzione avrebbe un impatto significativo sull'operatività del soggetto NIS. Tra il 15 aprile e il 31 maggio 2026, i soggetti NIS devono censire tali fornitori comunicando denominazione, codice fiscale, Paese di sede e tipologia di fornitura.

* Categorizzazione delle attività e dei servizi: dal 1° maggio al 30 giugno di ogni anno, i soggetti NIS dovranno trasmettere all'ACN l'elenco categorizzato delle proprie attività e servizi tramite il nuovo "Servizio NIS/Categorizzazione". L'ACN effettuerà verifiche a campione con esito comunicato entro 90 giorni.

* Notifiche in emergenza: in caso di indisponibilità del Referente CSIRT e dei suoi sostituti, il punto di contatto è ora formalmente abilitato a effettuare le notifiche obbligatorie e volontarie.

* Registrazione tardiva: il termine per completare l'aggiornamento annuale in caso di registrazione tardiva è fissato in 30 giorni dalla comunicazione di inserimento.

* Esenzione per soggetti DORA: le entità finanziarie soggette al Regolamento DORA sono esentate dagli obblighi di categorizzazione, con possibilità di adesione volontaria.

Novità di rilievo: Art. 18, 20 e 21 – Fornitori rilevanti e categorizzazione delle attività
Questi tre articoli, introdotti ex novo dalla Determinazione n. 127437/2026, rappresentano le novità più significative sul piano operativo e richiedono un'attenzione particolare da parte dei soggetti NIS.

Art. 18 – Censimento dei fornitori rilevanti NIS (deve essere effettuato tramite il "Servizio NIS/Aggiornamento annuale informazioni" nella finestra compresa tra il 15 aprile e il 31 maggio 2026)

L'articolo introduce l'obbligo di identificare e comunicare all'ACN i propri fornitori rilevanti, intesi come quei fornitori di beni o servizi la cui fornitura è di natura ICT oppure la cui eventuale interruzione o compromissione inciderebbe in modo significativo sulla capacità del soggetto NIS di operare, anche per assenza di alternative sul mercato.

La finalità è quella di mappare, lungo la catena di approvvigionamento, i soggetti potenzialmente qualificabili come entità importanti o essenziali ai sensi del Decreto NIS, così da estendere progressivamente le tutele di sicurezza informatica anche ai fornitori critici.

Per ciascun fornitore rilevante devono essere comunicati: denominazione, codice fiscale, Paese della sede legale, codici CPV relativi alle forniture fruite e criterio di rilevanza adottato (fornitura ICT o fornitura non fungibile).

nota: I codici CPV (Common Procurement Vocabulary) sono il sistema di classificazione europeo per gli appalti pubblici, istituito dal Regolamento (CE) n. 2195/2002.

Elencazione e categorizzazione delle attività e dei servizi

art. 20

L'articolo disciplina il nuovo obbligo annuale di comunicare all'ACN l'elenco categorizzato delle proprie attività e servizi, classificati per livello di rilevanza ai sensi dell'art. 30 del Decreto NIS. L'obiettivo è fornire all'Autorità una fotografia strutturata e aggiornata dell'operatività di ciascun soggetto NIS, funzionale alla valutazione del relativo profilo di rischio.

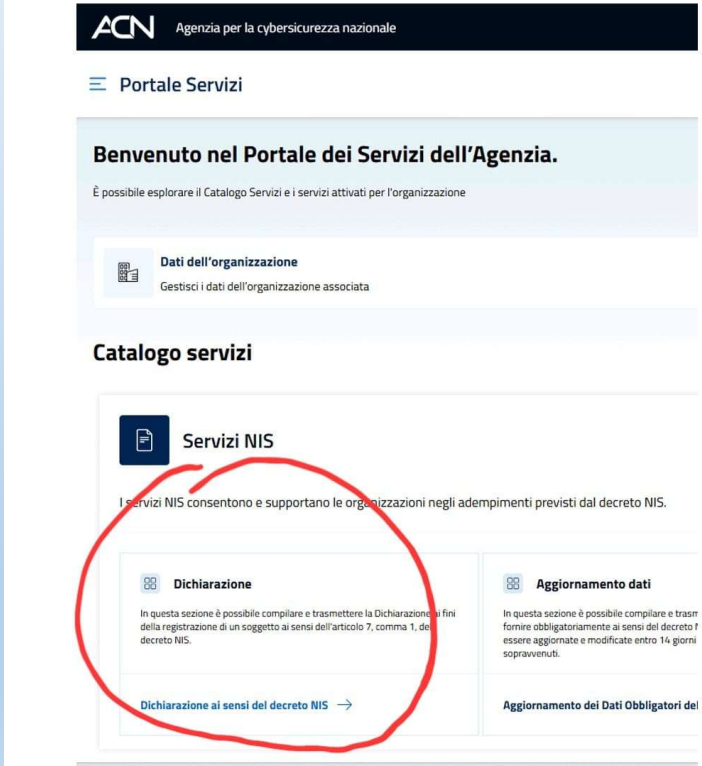
La trasmissione avviene tramite il nuovo «Servizio NIS/Categorizzazione» disponibile sul Portale ACN. Il punto di contatto è responsabile della conferma e dell'invio telematico delle informazioni, con valore di dichiarazione ai sensi del D.P.R. 445/2000. L'ACN provvede all'invio di una copia al domicilio digitale del soggetto.
Una volta decorso il termine, l'elenco si intende definitivamente acquisito e non è più modificabile. Le trasmissioni tardive sono ammesse ma anch'esse non modificabili, salvo comprovate criticità tecnico-operative non imputabili al soggetto.

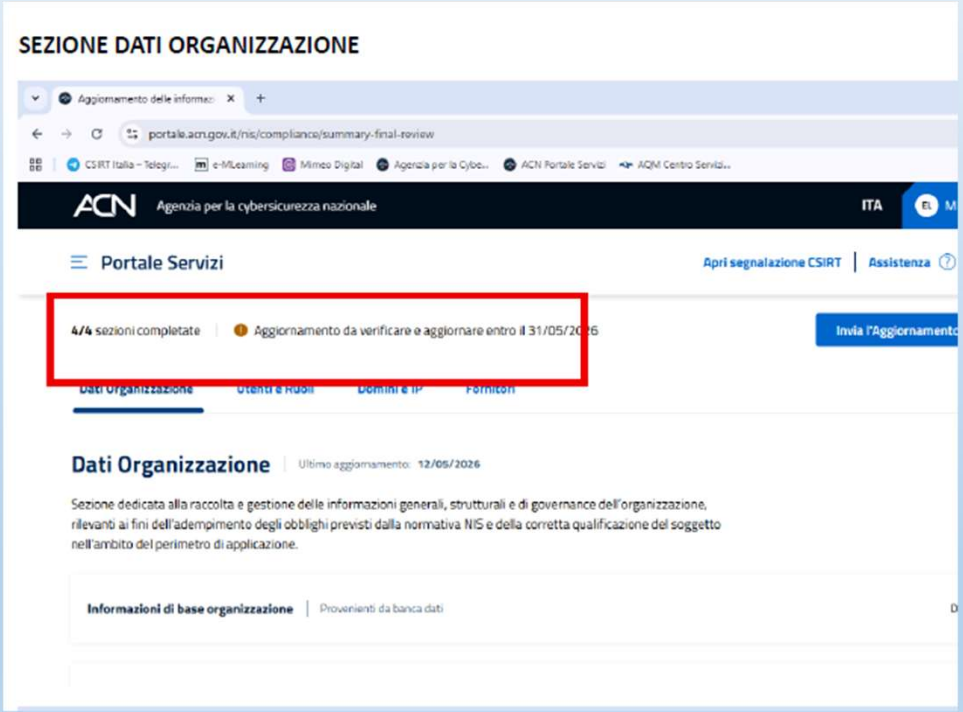
Finestra annuale: dal 1° maggio al 30 giugno di ogni anno. Le entità finanziarie soggette al Regolamento DORA sono esentate da questo obbligo, salva adesione volontaria.

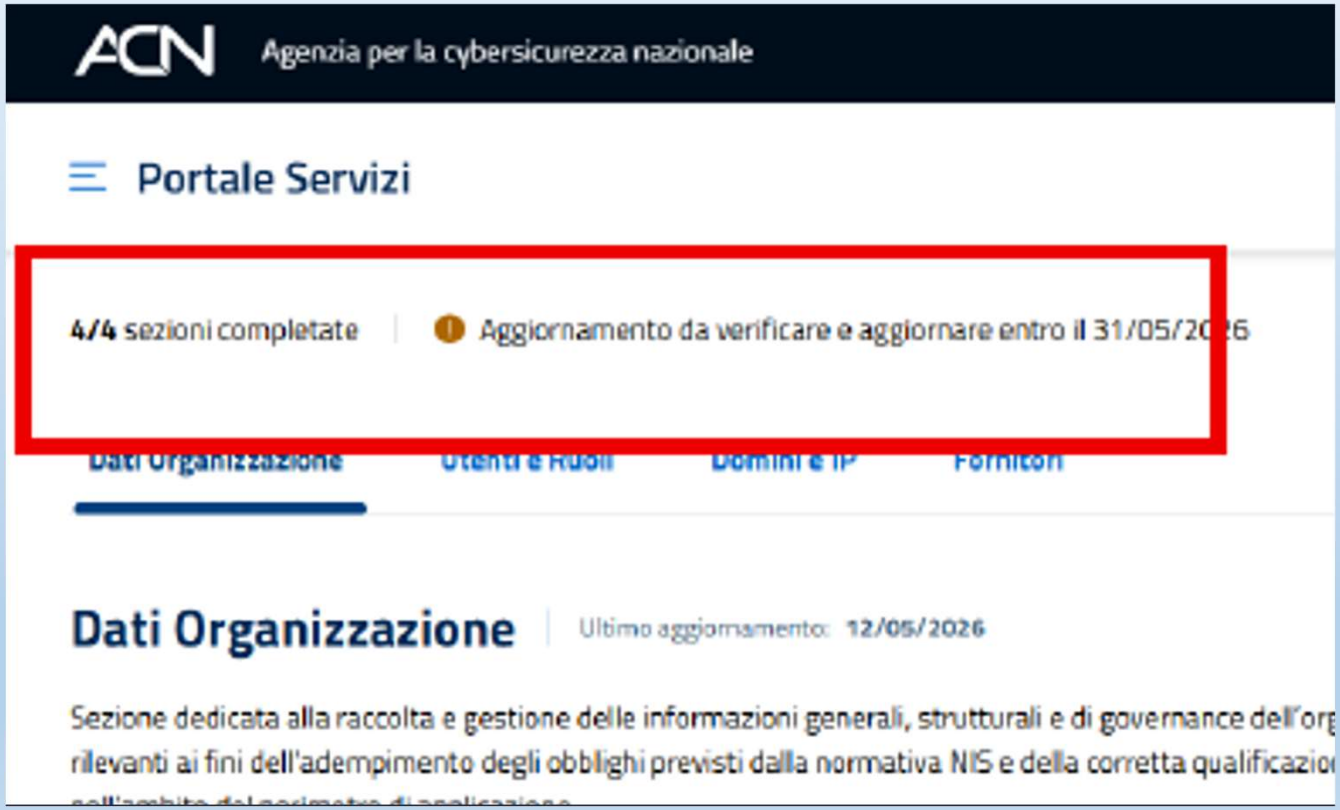
Art. 21 – Verifiche di conformità sulla categorizzazione

L'articolo introduce un meccanismo di controllo a campione da parte dell'ACN sugli elenchi categorizzati trasmessi dai soggetti NIS. Le verifiche sono condotte comparando quanto dichiarato dal soggetto sia con i criteri stabiliti dalla determinazione di riferimento, sia con gli elenchi di soggetti NIS comparabili per settore e dimensione.

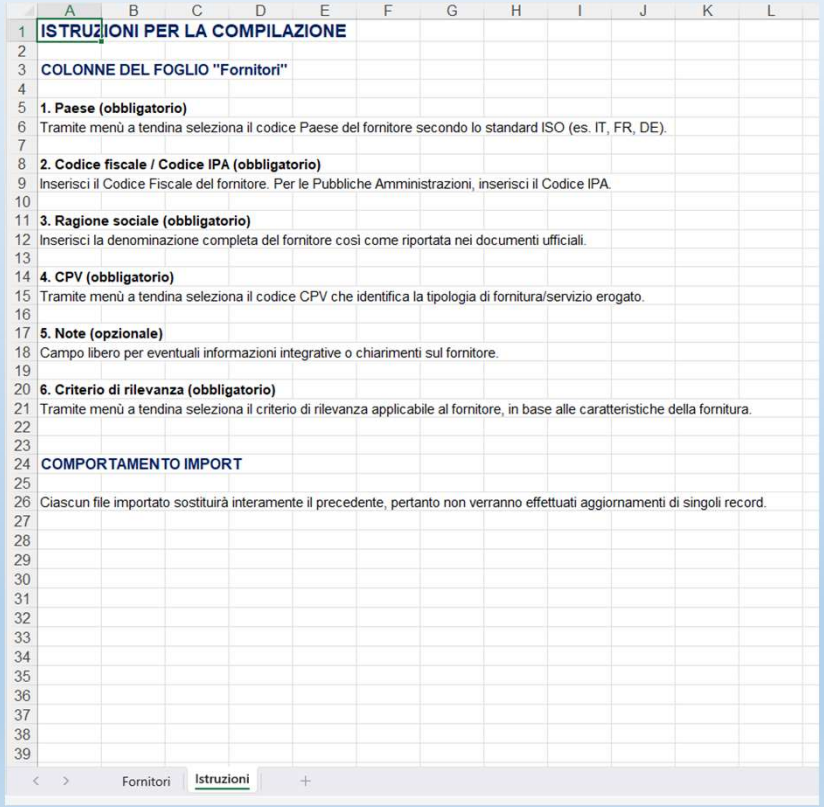
L'esito delle verifiche viene comunicato al soggetto NIS entro 90 giorni dalla trasmissione dell'elenco, con possibilità di proroga da parte dell'ACN.


ACN Agenzia per la cybersicurezza nazionale
Portale Servizi
Benvenuto nel Portale dei Servizi dell'Agenzia.
È possibile esplorare il Catalogo Servizi e i servizi attivati per l'organizzazione
Dati dell'organizzazione
Gestisci i dati dell'organizzazione associata
Catalogo servizi
Servizi NIS
I servizi NIS consentono e supportano le organizzazioni negli adempimenti previsti dal decreto NIS.
Dichiarazione
In questa sezione è possibile compilare e trasmettere la Dichiarazione ai fini della registrazione di un soggetto ai sensi dell'articolo 7, comma 1, del decreto NIS.
Aggiornamento dati
Dichiarazione ai sensi del decreto NIS
Aggiornamento dei Dati Obbligatori del


SEZIONE DATI ORGANIZZAZIONE
portale.acn.gov.it/nis/compliance/summary-final-review
ACN Agenzia per la cybersicurezza nazionale
ITA
Portale Servizi
Apri segnalazione CSIRT
Assistenza
4/4 sezioni completate
Aggiornamento da verificare e aggiornare entro il 31/05/2026
Invia l'Aggiornamento
Dati Organizzazione
Utenti e Ruoli
Domini e IP
Fornitori
Dati Organizzazione
Ultimo aggiornamento: 12/05/2026
Sezione dedicata alla raccolta e gestione delle informazioni generali, strutturali e di governance dell'organizzazione, rilevanti ai fini dell'adempimento degli obblighi previsti dalla normativa NIS e della corretta qualificazione del soggetto nell'ambito del perimetro di applicazione.
Informazioni di base organizzazione
Provenienti da banca dati


ACN
Agenzia per la cybersicurezza nazionale
Portale Servizi
4/4 sezioni completate
Aggiornamento da verificare e aggiornare entro il 31/05/20
Dati Organizzazione
Utenti e Ruoli
Domini e IP
Fornitori
Dati Organizzazione
Ultimo aggiornamento: 12/05/2026
Sezione dedicata alla raccolta e gestione delle informazioni generali, strutturali e di governance dell'org
rilevanti ai fini dell'adempimento degli obblighi previsti dalla normativa NIS e della corretta qualificazio

# Fornitori rilevanti portale ACN



**ISTRUZIONI PER LA COMPILAZIONE**

**COLONNE DEL FOGLIO "Fornitori"**

**1. Paese (obbligatorio)**
Tramite menù a tendina seleziona il codice Paese del fornitore secondo lo standard ISO (es. IT, FR, DE).

**2. Codice fiscale / Codice IPA (obbligatorio)**
Inserisci il Codice Fiscale del fornitore. Per le Pubbliche Amministrazioni, inserisci il Codice IPA.

**3. Ragione sociale (obbligatorio)**
Inserisci la denominazione completa del fornitore così come riportata nei documenti ufficiali.

**4. CPV (obbligatorio)**
Tramite menù a tendina seleziona il codice CPV che identifica la tipologia di fornitura/servizio erogato.

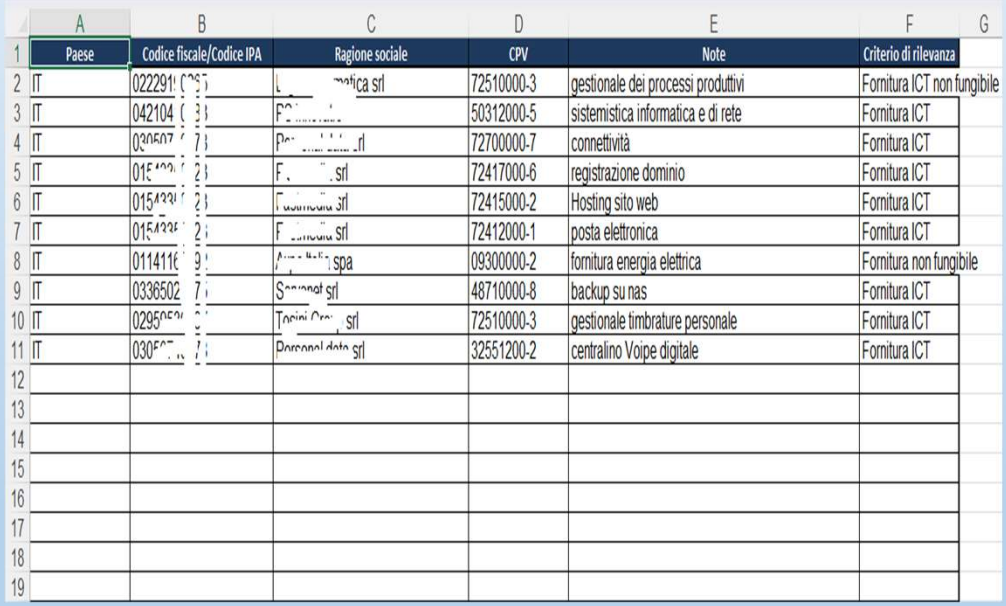
**5. Note (opzionale)**
Campo libero per eventuali informazioni integrative o chiarimenti sul fornitore.

**6. Criterio di rilevanza (obbligatorio)**
Tramite menù a tendina seleziona il criterio di rilevanza applicabile al fornitore, in base alle caratteristiche della fornitura.

**COMPORTAMENTO IMPORT**

Ciascun file importato sostituirà interamente il precedente, pertanto non verranno effettuati aggiornamenti di singoli record.

Fornitori | Istruzioni



| Paese | Codice fiscale/Codice IPA | Ragione sociale | CPV | Note | Criterio di rilevanza |
|---|---|---|---|---|---|
| IT | 022291[illegible] | [illegible]atica srl | 72510000-3 | gestionale dei processi produttivi | Fornitura ICT non fungibile |
| IT | 042104[illegible] | [illegible] | 50312000-5 | sistemistica informatica e di rete | Fornitura ICT |
| IT | 030507[illegible] | [illegible]rl | 72700000-7 | connettività | Fornitura ICT |
| IT | 015[illegible] | [illegible].srl | 72417000-6 | registrazione dominio | Fornitura ICT |
| IT | 015423[illegible] | [illegible]srl | 72415000-2 | Hosting sito web | Fornitura ICT |
| IT | 015423[illegible] | [illegible]srl | 72412000-1 | posta elettronica | Fornitura ICT |
| IT | 011411[illegible] | [illegible]spa | 09300000-2 | fornitura energia elettrica | Fornitura non fungibile |
| IT | 0336502[illegible] | Serverat srl | 48710000-8 | backup su nas | Fornitura ICT |
| IT | 029505[illegible] | Torini Cr[illegible] srl | 72510000-3 | gestionale timbrature personale | Fornitura ICT |
| IT | 030507[illegible] | Personal data srl | 32551200-2 | centralino Voipe digitale | Fornitura ICT |

# categorizzazione servizi portale ACN

**ISTRUZIONI PER LA COMPILAZIONE**

**COLONNE DEL FOGLIO "Elenco categorizzato"**

**1. Macro-area(obbligatoria)**
Seleziona la macro-area dal menu a tendina. Le macro-aree disponibili sono predefinite dal sistema e questo campo determina la categorizzazione di default dell'attività/servizio.

**2. Denominazione Attività/Servizio (obbligatorio)**
Inserisci il nome dell'attività/servizio. Il nome deve essere univoco per organizzazione, ma può essere associato a più macro-aree.

**3. Descrizione (opzionale)**
Descrizione dettagliata dell'attività/servizio rispetto alla macroarea a cui è associato.

**4. Categoria di rilevanza pre-assegnata (automatico)**
Questo campo si calcola automaticamente in base alla macro-area selezionata.
NON è possibile modificare manualmente questo campo.

**5. Categoria di rilevanza attribuita(condizionale)**
Se vuoi assegnare una categorizzazione diversa da quella ereditata, seleziona un valore dal menu a tendina.
Valori possibili: Impatto minimo, impatto basso, impatto medio, impatto alto
Lascia vuoto per mantenere la categorizzazione ereditata.

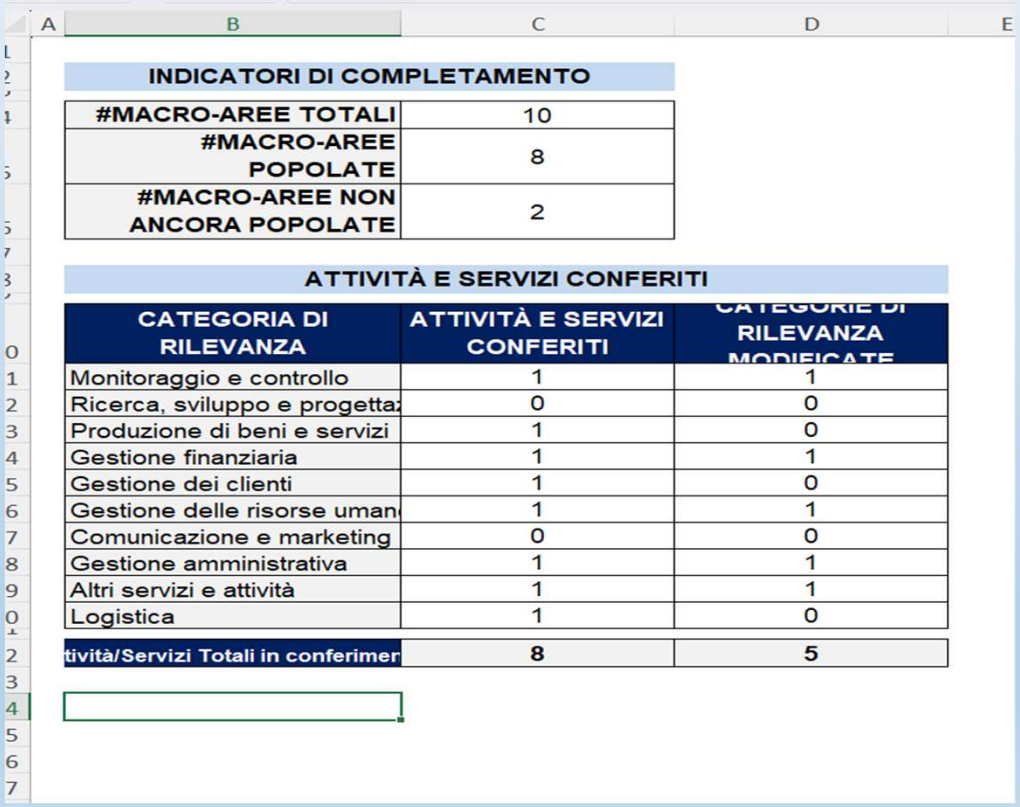
**COMPORTAMENTO IMPORT**

Ciascun file importato sostituirà interamente il precedente, pertanto non verranno effettuati aggiornamenti di singoli record.
La presenza di una riga vuota viene interpretata come fine file. Il sistema considera solo le righe sopra la prima riga vuota.

| Macro-area | Denominazione Attività/Servizio | Descrizione | Categoria di rilevanza pre-assegnata | Categoria di rilevanza attribuita |
|---|---|---|---|---|
| Monitoraggio e controllo | **Audit sicurezza alimentare** | ISO 45001 ISO 14001 | *Impatto alto* | Impatto minimo |
| Produzione di beni e servizi | **lavorazioni e vendita** | [illegible] compreso acquisti materie prime e accessorie | *Impatto medio* | Impatto medio |
| Gestione finanziaria | **rendiconatazione forniture, gestione clienti e dipe** | genstione finanziaria fatturazioni, buste paghe e contratti di fornitura | *Impatto basso* | Impatto medio |
| Gestione dei clienti | **genstione ordini, riscossione fatture** | gestione ordini e pianificazione consegne | *Impatto basso* | Impatto basso |
| Gestione delle risorse umane | **gestione dipendenti** | assunzioni, elaborazioni paghe, diritti lavorativi e fine rapporto | *Impatto basso* | Impatto medio |
| Logistica | **gestione logistica esternalizzata** | contratti con fornitore di trasporti, gestione consegne per forniture | *Impatto basso* | Impatto basso |
| Gestione amministrativa | **contabilittà finanziaria ordinaria** | [illegible], scadenze fiscali e adempimenti amministrativi | *Impatto minimo* | Impatto basso |
| Altri servizi e attività | **manutenzioni impianti** | gestione ditte e esterne per manutenzione impianti produttivi | *Impatto minimo* | Impatto basso |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Dashboard | Elenco categorizzato | Istruzioni

# categorizzazione servizi portale ACN



**INDICATORI DI COMPLETAMENTO**

| | |
|---|---|
| **#MACRO-AREE TOTALI** | 10 |
| **#MACRO-AREE POPOLATE** | 8 |
| **#MACRO-AREE NON ANCORA POPOLATE** | 2 |

**ATTIVITÀ E SERVIZI CONFERITI**

| CATEGORIA DI RILEVANZA | ATTIVITÀ E SERVIZI CONFERITI | CATEGORIE DI RILEVANZA MODIFICATE |
|---|---|---|
| Monitoraggio e controllo | 1 | 1 |
| Ricerca, sviluppo e progettaz | 0 | 0 |
| Produzione di beni e servizi | 1 | 0 |
| Gestione finanziaria | 1 | 1 |
| Gestione dei clienti | 1 | 0 |
| Gestione delle risorse uman | 1 | 1 |
| Comunicazione e marketing | 0 | 0 |
| Gestione amministrativa | 1 | 1 |
| Altri servizi e attività | 1 | 1 |
| Logistica | 1 | 0 |
| **tività/Servizi Totali in conferimer** | **8** | **5** |

Conclusione relativamente art.18 – NIS2

L'introduzione dell'obbligo di censimento dei fornitori rilevanti non è un semplice adempimento da completare entro il 31 maggio 2026. È il segnale di un cambiamento di paradigma: la supply chain, fino ad oggi gestita internamente secondo logiche prevalentemente economiche o contrattuali, entra ufficialmente nel perimetro regolato dall'ACN e diventa oggetto di verifica.

Non basta compilare l'elenco dei fornitori rilevanti: occorre poter dimostrare con quale metodo si è stabilito che un fornitore è rilevante e un altro no. Un elenco costruito sulla base del solo valore contrattuale o della presenza di certificazioni ISO non soddisfa i requisiti della determinazione e, in sede di verifica da parte dell'ACN, risulterebbe contestabile.

La determinazione richiede quindi una valutazione fondata sull'impatto effettivo che ciascun fornitore ha sui processi critici e sulla sicurezza dei sistemi informativi.

Per farlo correttamente, le organizzazioni devono integrare due attività che spesso operano in silos separati: la Business Impact Analysis (BIA), che misura la criticità dei processi interni, e il Third Party Risk Management (TPRM), che valuta l'esposizione al rischio lungo la catena di fornitura.

Solo dall'incrocio di queste due dimensioni è possibile costruire una mappatura dei fornitori rilevanti che sia metodologicamente solida, documentabile e difendibile davanti all'ACN.

# La resilienza nel contesto della cybersecurity

La resilienza digitale rappresenta una componente essenziale della cybersecurity, in quanto è volta a mantenere la continuità dei servizi anche in presenza di incidenti o interruzioni. L'adozione di piani di Continuità Operativa e Disaster Recovery si basa sulla comprensione degli impatti sui servizi.

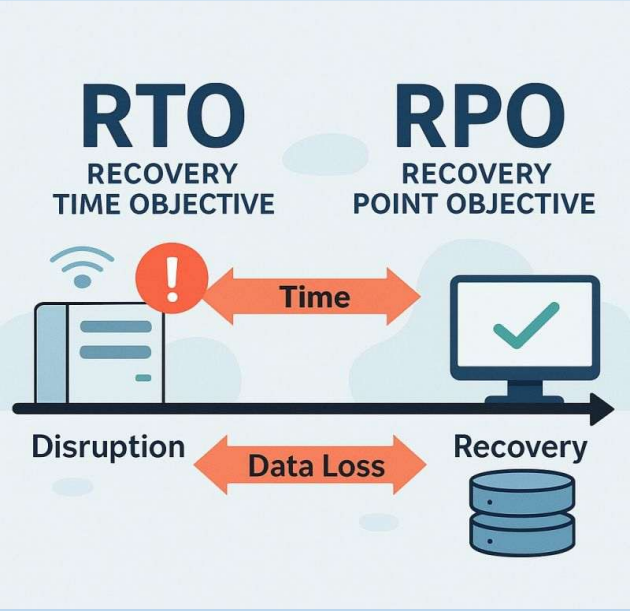
## Comprendere gli impatti

**La BIA (Business Impact Analysis) processo strategico che valuta l'impatto delle interruzioni sui processi aziendali critici, supportando la continuità o perativa e la sicurezza informatica.**

Identificazione dei processi critici e valutazione degli effetti di possibili interruzioni su servizi, dati e operatività, finalizzate alla definizione dei parametri di continiuità operativa (RTO, RPO) e dei livelli di tolleranza all'interruzione.

## Preparare la risposta

Pianificazione delle misure di Business Continuity e Disaster Recovery basate su parametri di continuità operativa identificati, specifici per ciascuna attività o servizio.



Il messaggio è quindi duplice:

Da un lato, agire nell'immediato: la finestra per il censimento è già aperta (15 aprile – 31 maggio 2026) e non ammette proroghe ordinarie. Chi non dispone ancora di un processo strutturato deve avviarlo subito, anche in
forma semplificata, documentando i criteri adottati.

Dall'altro, investire nel metodo nel medio termine: l'obbligo si ripete annualmente e l'ACN effettuerà verifiche a campione. Le organizzazioni che affrontano l'art. 18 come un esercizio una tantum si troveranno ogni anno ad affrontare lo stesso problema da zero. Quelle che invece lo integrano nel proprio sistema di gestione del rischio trasformeranno un vincolo regolatorio in uno strumento concreto di resilienza.

In sintesi: **la NIS2 non chiede solo di dichiarare chi sono i propri fornitori critici. Chiede di saperlo davvero e di poterlo dimostrare.**