DATACONSEC

DATA PROTECTION - CONSULTING - SECURITY

NIS 2
Obblighi in evoluzione – Stato dell'arte, scadenze e azioni concrete.

13 maggio 2026

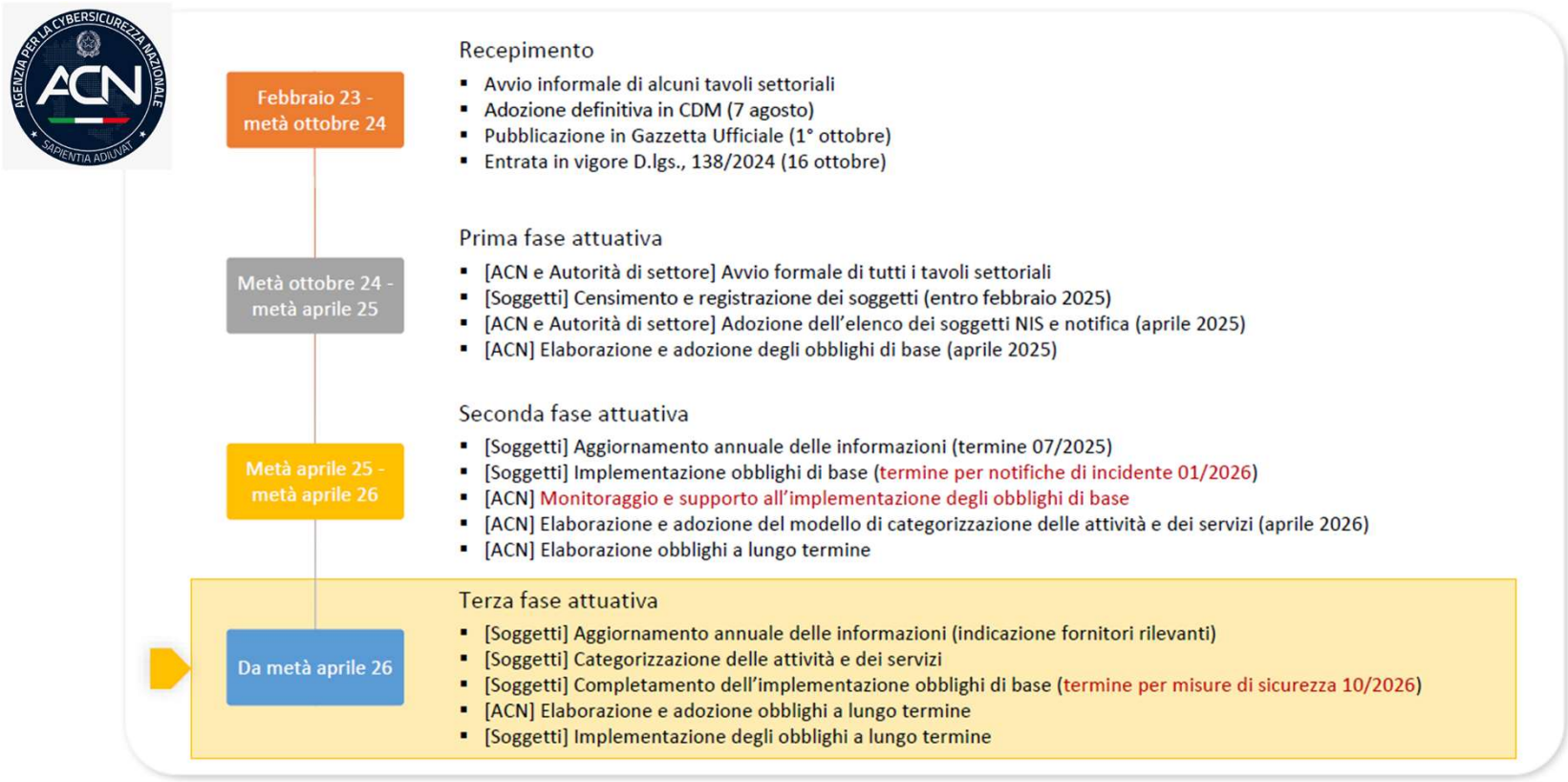
Agenda

- ❑ Recepimento e attuazione e prossime scadenze
- ❑ Aggiornamento annuale delle informazioni
- ❑ Accordi di condivisione delle informazioni e individuazione dei fornitori rilevanti (Determinazione ACN n. 127437/2026)
- ❑ Categorizzazione delle attività e dei servizi
- ❑ Sicurezza della catena di approvvigionamento
- ❑ Appendice – Link utili

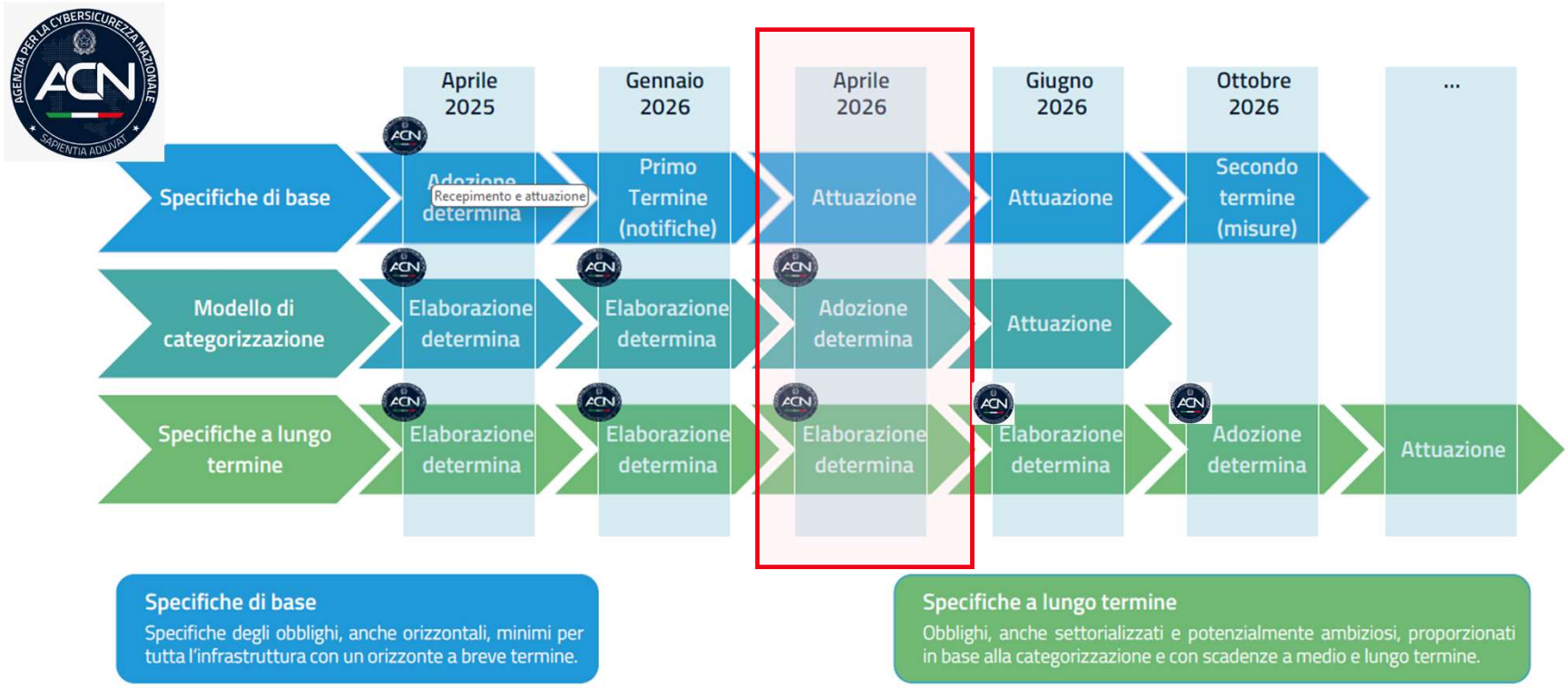
Agenda

- ➢ **Recepimento e attuazione e prossime scadenze**
- ❑ Aggiornamento annuale delle informazioni
- ❑ Accordi di condivisione delle informazioni e individuazione dei fornitori rilevanti (Determinazione ACN n. 127437/2026)
- ❑ Categorizzazione delle attività e dei servizi
- ❑ Sicurezza della catena di approvvigionamento
- ❑ Appendice – Link utili

Recepimento e attuazione 1/2



Recepimento e attuazione 2/2



Le scadenze previste nel 2026

GEN 2026

Notifica incidenti

Operativo l'obbligo di notifica degli incidenti significativi al CSIRT Italia (9 mesi dalla comunicazione apr. 2025)

15 APR – 31 MAG

Aggiornamento annuale

I **Soggetti NIS** devono procedure ad ggiornare dati art. 7 (organi direttivi, IP, domini) + nuovo obbligo: elenco fornitori rilevanti (Det. 127437/2026)

1° MAG – 30 GIU

Categorizzazione

I **Soggetti NIS** devono comunicare ad ACN elenco categorizzato attività e servizi tramite piattaforma ACN (Det. 155238/2026 – Art. 30)

ENTRO 31 OTT

Misure di sicurezza di base

Adozione completa delle misure di base (Det. 379907/2025): 37 misure / 87 req. (importanti), 43 / 116 (essenziali), da parte dei **Soggetti NIS**

ENTRO FINE 2026

Obblighi a lungo termine

Attesa adozione **da parte ACN** delle misure di sicurezza a lungo termine, modulate sulle categorie di rilevanza

Nuovi soggetti NIS (inseriti nel 2026): referente CSIRT entro 31/12/2026 | notifica incidenti dal 1/1/2027 | misure di base entro 31/7/2027

Agenda

- Recepimento e attuazione e prossime scadenze
- **Aggiornamento annuale delle informazioni**
- Accordi di condivisione delle informazioni e individuazione dei fornitori rilevanti (Determinazione ACN n. 127437/2026)
- Categorizzazione delle attività e dei servizi
- Sicurezza della catena di approvvigionamento
- Appendice – Link utili

Aggiornamento delle informazioni 2026 1/2

Determinazione ACN n. 127437/2026

Per tutti i Soggetti NIS: verificare correttezza e aggiornamento di

a) dati anagrafici e di contatto del **punto di contatto, sostituto punto di contatto** designati e della **segreteria (ove presente)**. Ove presente la delega, il punto di contatto e il sostituto punto di contatto si assicurano che sia aggiornata, corretta e conforme alla normativa NIS

b) dati anagrafici e di contatto del **soggetto NIS** (codice fiscale, la denominazione, l'indirizzo della sede legale, l'indicazione del rappresentante legale, l'elenco dei procuratori generali, il numero di telefono, il domicilio digitale e un indirizzo di posta elettronica ordinaria funzionale)

c) elenco dei **componenti degli organi di amministrazione e direttivi** (es: membri del Cda) **e relativi dati** (codici fiscali e indirizzi PEC)

d) ove applicabile, elenco dei servizi che rientrano nell'ambito di applicazione della NIS 2 che il soggetto NIS offre nell'UE e indicando in quali **Stati membri**

e) spazio di **indirizzamento IP pubblico** e dei **nomi di dominio in uso o nella disponibilità** del soggetto NIS

f) elenco degli **accordi di condivisione delle informazioni**

g) dati identificativi del **referente CSIRT e degli eventuali sostituti**

h) dell'elenco dei **fornitori rilevanti NIS**

i) per i soggetti NIS che hanno designato il proprio rappresentante NIS in Italia, i dati anagrafici e di contatto del **rappresentante NIS**

Ai **soggetti già inseriti nell'elenco dei soggetti NIS 2025**, all'avvio dell'aggiornamento annuale delle informazioni per l'anno 2026, sono presentate le **informazioni precompilate** sulla base di quelle trasmesse fino al 14 aprile 2026 tramite i Servizi NIS

Fermo restando quanto previsto dall'articolo 38, comma 10, lettera b), del decreto NIS, in caso di registrazione tardiva, il **termine per completare l'aggiornamento annuale** è fissato in **30 giorni dalla ricezione della comunicazione** di cui all'articolo 7, comma 3, lettera a).

Aggiornamento delle informazioni 2026 2/2

Determinazione ACN n. 127437/2026

Processo per l'aggiornamento continuo delle informazioni

Casi in cui può essere effettuato	Modalità	Tempistiche	Casi particolari
Laddove sopraggiungano **modifiche alle informazioni trasmesse ad ACN** a seguito del perfezionamento dell'aggiornamento annuale	Tramite il Portale dei Servizi ACN, "**Servizio NIS/ Aggiornamento continuo informazioni**". Gli utenti forniscono le informazioni aggiornate per conto del soggetto per cui operano, assicurandone la **correttezza**. **Il punto di contatto conferma le informazioni** fornite e le trasmette ad ACN tramite il servizio suddetto. Una **copia delle informazioni** è inviata via PEC al Soggetto NIS per ricevuta	L'aggiornamento continuo delle informazioni è possibile **fino al 14 aprile di ogni anno successivo alla ricezione della comunicazione** di cui all'articolo 7, comma 3, lettere a) e b), del decreto NIS (comunicazione di qualificazione quale Soggetto NIS). Le modifiche devono essere **comunicate tempestivamente**, e in ogni caso **entro 14 giorni** dalla data della modifica (art. 7, co. 7, Decreto NIS)	La **modifica**, confermata da punto di contatto, dell'indicazione del **rappresentante legale** o dell'**elenco dei procuratori generali** del soggetto NIS è sottoposta alla convalida del soggetto medesimo, secondo la procedura telematica indicata nella richiesta inviata al domicilio digitale di quest'ultimo.

Agenda

- Recepimento e attuazione e prossime scadenze
- Aggiornamento annuale delle informazioni
- **Accordi di condivisione delle informazioni e individuazione dei fornitori rilevanti (Determinazione ACN n. 127437/2026)**
- Categorizzazione delle attività e dei servizi
- Sicurezza della catena di approvvigionamento
- Appendice – Link utili

Accordi di condivisione delle informazioni 1/3

Cosa sono e cosa si condivide

I soggetti NIS possono scambiarsi, **su base volontaria**, **informazioni sulla sicurezza informatica con altri soggetti NIS e/o terze parti** (inclusi fornitori).

Informazioni condivisibili:
Minacce informatiche, quasi-incidenti, vulnerabilità, IoC, tattiche avversarie, allarmi di sicurezza, raccomandazioni configurazione strumenti.

Finalità:
Prevenire e rilevare gli incidenti, aumentare il livello complessivo di sicurezza informatica.

Lo scambio deve essere **regolato da accordi formali** che definiscano perimetro e strumenti di tutela delle informazioni (art. 17, c. 2).

Obblighi operativi e notifica

Notifica ad ACN:
I soggetti notificano **tramite il Portale dei Servizi ACN** la partecipazione ad accordi di condivisione delle informazioni.
Eventuali modifiche (nuovi, risoluzioni, variazioni) vanno comunicate entro 14 giorni (tempistiche dell'aggiornamento continuo).

Cosa va notificato (FAQ ACN ACI.4):
Contratti con oggetto servizi di sicurezza informatica: SOC, CERT, Vulnerability Assessment, Penetration Testing, Cyber Threat Intelligence, MSSP.

Cosa NON va notificato:
Contratti che non abbiano come oggetto Servizi di sicurezza informatica in cui il fornitore segnala solo su base volontaria eventi di sicurezza.

Accordi di condivisione delle informazioni 2/3

Tipo servizio	Esempi clausole contrattuali da comunicare
NOC (*Network Operation Centre*)	**Oggetto del servizio** (perimetro di monitoraggio, asset coperti) **Tipologia di alert e notifiche** (quali eventi vengono segnalati al cliente) **Modalità e frequenza di reporting** (report periodici, accesso a dashboard, canali di comunicazione) **Gestione dei log** (retention, accessibilità, formati) **Clausole di riservatezza** sulle informazioni scambiate
MDR (*Managed Detection and Response*)	**Oggetto del servizio** (capacità di detection e response, tecnologie impiegate) **Flussi informativi** (tipologia di alert, IoC condivisi, report di incidente) **Escalation e notifiche** (tempi, canali, livelli di gravità) **Azioni di risposta** (perimetro di intervento autonomo del fornitore) **Riservatezza e trattamento dati** relativi a incidenti e vulnerabilità
SOC (*Security Operation Centre*)	**Oggetto e perimetro** (fonti di log, asset monitorati, use case implementati) **Tipologia degli output** (alert, report periodici, notifiche di incidente) **Procedure di escalation** (SLA di notifica, matrice di escalation) **Modalità di condivisione** (portale, email, ticketing, formati) **Riservatezza e NDA** sulle informazioni di sicurezza trattate

Tipo servizio	Esempi clausole contrattuali da comunicare
CSOC (*Cyber Security Operation Centre*)	**Come per il SOC**, con integrazioni su: **Attività di threat hunting** (scope, frequenza, output) **Supporto forense** (perimetro, deliverable, catena di custodia) **Condivisione di intelligence operativa** (feed, bollettini, briefing)
CERT (*Computer Emergency Response Team*)	**Oggetto del servizio** (incident response, advisory, coordinamento) **Flussi informativi** (bollettini, advisory, IoC, report post-incidente) **Modalità di attivazione** (on-demand, retainer, SLA di intervento) **Deliverable di incident response** (report, root cause analysis, remediation plan) **Riservatezza e regole di condivisione** verso terzi (TLP o equivalenti)
VA/PT (*Vulnerability Assessment e Penetration Test*)	**Oggetto e scope** (target, tipologia di test, metodologia adottata) **Deliverable** (report tecnico, executive summary, formato) **Gestione dei risultati** (chi riceve il report, canali di trasmissione sicuri) **Riservatezza rafforzata** (i risultati contengono info sulle vulnerabilità del cliente) **Retention e distruzione dei dati** e delle evidenze raccolte

Accordi di condivisione delle informazioni 3/3

Tipo servizio	Esempi clausole contrattuali da comunicare
Red Teaming	**Oggetto e regole di ingaggio** (scope, scenari, limiti operativi, finestra temporale) **Deliverable** (report tecnico, executive debrief, presentazione risultati) **Gestione delle informazioni sensibili** (vulnerabilità critiche scoperte, percorsi di attacco) **Riservatezza e need-to-know** (distribuzione limitata dei risultati) **Retention e distruzione di evidenze**, tool, accessi temporanei

Tipo servizio	Esempi clausole contrattuali da comunicare
Cyber Threat Intelligence	**Oggetto del servizio** (tipologia di intelligence: strategica, tattica, operativa) **Output e formati** (feed automatici, report, bollettini, frequenza) **Regole di condivisione** (TLP, restrizioni di ridistribuzione) **Personalizzazione** (intelligence contestualizzata al settore/perimetro del cliente)

La tabella fornisce, a titolo esemplificativo e non esaustivo, un'indicazione delle sezioni contrattuali che è opportuno includere nell'estratto da comunicare ad ACN per ciascuna tipologia di fornitura di servizi di sicurezza informatica elencata nella FAQ ACI.4 (https://www.acn.gov.it/portale/faq/nis/aggiornamento-delle-informazioni). In assenza di linee guida specifiche da parte dell'Autorità, le indicazioni riportate rappresentano un'interpretazione operativa ragionevole.

Quanto indicato ha pertanto finalità esclusivamente orientativa. Si raccomanda di verificare le indicazioni, ove necessario, con l'Autorità competente.

Individuazione dei fornitori rilevanti 1/2

Un fornitore è “**rilevante NIS**” se fornisce servizi/prodotti a un Soggetto NIS e soddisfa almeno uno dei seguenti criteri:

Criterio A — Fornitura ICT

La fornitura è riconducibile alle attività/servizi dell'Allegato I, punti 8 (**infrastrutture digitali**) e 9 (**gestione servizi TIC B2B**) del decreto NIS.

Criterio B — Fornitura non fungibile

L'interruzione/compromissione della fornitura comporta un **impatto significativo sulle attività NIS**, anche per **indisponibilità di fornitori alternativi**.

Informazioni da comunicare per ogni fornitore rilevante (art. 18, Determinazione ACN n. 127437/2026)

Denominazione	**Codice fiscale**	**Paese sede legale**	**Codici CPV**	**Criterio rilevanza**
Ragione sociale del fornitore	CF / Partita IVA del fornitore	Stato della sede legale del fornitore	Reg. CE 2195/2002 relativi alla fornitura	A (ICT), B (non fungibile) o entrambi

Finestra di comunicazione: 15 aprile – 31 maggio di ogni anno | In caso di dubbio, ACN suggerisce un approccio prudenziale

Individuazione dei fornitori rilevanti 2/2

Esempi di forniture rilevanti e relative codici CPV

Tipo fornitura	Criterio	Codici CPV
Connettività (dati/voce, fissa/mobile) — se non ridondata	**B – Fornitura non fungibile**	72400000-4, 72411000-4, 72318000-7
Corrente elettrica — se non ridondata	**B – Fornitura non fungibile**	65310000-9, 65300000-6
Servizi cloud computing	**A – Fornitura ICT**	72310000-1, 72320000-4, 72322000-8
Servizi DNS, registri TLD	**A – Fornitura ICT**	72400000-4
Reti di distribuzione contenuti (CDN)	**A – Fornitura ICT**	72400000-4, 72310000-1
Reti pubbliche di comunicazione elettronica	**A – Fornitura ICT**	64200000-8, 64210000-1
Servizi gestiti e MSSP	**A – Fornitura ICT**	72500000-0, 72510000-3, 72250000-2, 72600000-6, 72800000-8
Data center (colocation, hosting)	**A – Fornitura ICT**	72310000-1, 72317000-0

Note operative

- Rientrano tutte le dipendenze digitali e **anche quelle non digitali non sostituibili** senza impatto significativo (FAQ FRN.4).
- Codici CPV: riferimento ufficiale su EUR-Lex (Reg. CE 213/2008: https://ted.europa.eu/it/simap/cpv, https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32008R0213). La tabella ATECO-CPV del Codice Appalti è solo orientativa.
- Soggetti DORA (Reg. UE 2554/2022) in ambito NIS sono esonerati da questo adempimento (partecipazione volontaria).

Agenda

- Recepimento e attuazione e prossime scadenze
- Aggiornamento annuale delle informazioni
- Accordi di condivisione delle informazioni e individuazione dei fornitori rilevanti (Determinazione ACN n. 127437/2026)
- **Categorizzazione delle attività e dei servizi**
- Sicurezza della catena di approvvigionamento
- Appendice – Link utili

Contesto normativo e finalità della categorizzazione

Decreto NIS
D.Lgs. 138/2024 recepisce la Direttiva UE 2022/2555 per un livello comune elevato di cybersicurezza nell'Unione

Art. 30, comma 1, Decreto NIS
Dal 1° maggio al 30 giugno di ogni anno, i soggetti NIS comunicano l'elenco categorizzato delle proprie attività e servizi

Art. 40, comma 5, lett. i), Decreto NIS
ACN stabilisce categorie di rilevanza, processo, modalità e criteri per l'elencazione e categorizzazione

Determinazione ACN 155238/2026
Adottata il 14 aprile 2026 su parere del Tavolo NIS del 9 aprile 2026, efficace dal 1° maggio 2026

Perché categorizzare

- **Aggregare** attività/servizi **per categorie di impatto**
- Applicare misure di sicurezza **proporzionate** alla rilevanza
- **Differenziare le misure a lungo termine** in base alla categoria
- Assicurare livelli adeguati di sicurezza **limitando l'investimento al necessario**

Architettura del modello di categorizzazione di ACN 1/4

Il modello struttura le attività e i servizi in **macro-aree**, ciascuna con una **categoria di rilevanza pre-assegnata**.

10

Macro-aree

Coprono tutti gli ambiti dell'organizzazione

4

Categorie

Da impatto minimo a impatto alto

2

Allegati

Per diverse tipologie di soggetto NIS

Ogni macro-area è caratterizzata da:

Denominazione	Descrizione	Categoria di rilevanza pre-assegnata

Architettura del modello di categorizzazione di ACN 2/4

La **categoria di rilevanza** misura l'**impatto** di una compromissione sulla **capacità del soggetto di svolgere le attività e i servizi NIS**.

IMPATTO ALTO	Associato a macro-aree che aggregano **funzioni centrali del Soggetto NIS**, in relazione a supporto ai vertici, coordinamento e sicurezza. **Effetti negativi elevati**, **immediati** e **a lungo termine** sullo svolgimento di servizi e attività NIS
IMPATTO MEDIO	Associato a macro-aree che rappresentano il **core-business del Soggetto NIS**. Una compromissione (in termini di RID) potrebbe avere **effetti negativi significativi**, anche immediati, **eventualmente in parte reversibili**
IMPATTO BASSO	Associato a macro-aree che, in caso di **compromissione estensiva/prolungata** o il **disvelamento di informazioni sensibili** gestite in tali ambiti, possono **incidere sulla capacità di svolgere attività e servizi NIS**. rischio di fallimento. Presenza di dati personali
IMPATTO MINIMO	Associato a macro-aree che aggregano funzioni che, qualora compromesse, determinerebbero **effetti di minore entità sulla capacità di svolgere le attività e i servizi NIS**

Architettura del modello di categorizzazione di ACN 3/4

A **ciascuna macro-area** individuata dal modello è **assegnata di *default*** una **categoria di rilevanza specifica**, come di seguito illustrato:

Monitoraggio e controllo	**ALTO**	**Gestione risorse umane**	**BASSO**
Produzione di beni e servizi	**MEDIO**	**Logistica (*)**	**MIN./BASSO**
Ricerca, sviluppo e progettazione	**MEDIO**	**Comunicazione e marketing**	**MINIMO**
Gestione finanziaria	**BASSO**	**Gestione amministrativa**	**MINIMO**
Gestione dei clienti	**BASSO**	**Altri servizi e attività**	**MINIMO**

(*) Allegato 1 alla Determinazione ACN 155238/2026: tipologie All. I (nn. 1,2,5,6,7,10), All. II (nn. 1-5), All. IV (n. 1) del Decreto NIS (D. Lgs. 138/2024).
Allegato 2 alla Determinazione ACN 155238/2026 : tutti gli altri soggetti NIS.

Architettura del modello di categorizzazione di ACN 4/4

A **ciascuna macro-area** individuata dal modello è **assegnata di *default*** una **categoria di rilevanza specifica**, come di seguito illustrato:

Macro-area	Allegato 1, Det. ACN 155238/2026	Allegato 2, Det. ACN 155238/2026
Monitoraggio e controllo	Impatto alto	Impatto alto
Produzione di beni e servizi	Impatto medio	Impatto medio
Ricerca, sviluppo e progettazione	Impatto medio	Impatto medio
Gestione finanziaria	Impatto basso	Impatto basso
Gestione dei clienti	Impatto basso	Impatto basso
Gestione delle risorse umane	Impatto basso	Impatto basso
Logistica	Impatto basso	Impatto minimo
Comunicazione e marketing	Impatto minimo	Impatto minimo
Gestione amministrativa	Impatto minimo	Impatto minimo
Altri servizi e attività	Impatto minimo	Impatto minimo

ALLEGATO 1 — Logistica = impatto basso

Allegato I del decreto NIS:
n. 1 Energia, n. 2 Trasporti, n. 5 Settore sanitario, n. 6 Acqua potabile, n. 7 Acque reflue, n. 10 Spazio

Allegato II del decreto NIS:
n. 1 Servizi postali e di corriere, n. 2 Gestione dei rifiuti, n. 3 Fabbricazione/distribuzione sostanze chimiche, n. 4 Produzione/distribuzione alimenti, n. 5 Fabbricazione

Allegato IV del decreto NIS:
n. 1 (amministrazioni centrali, regionali, locali, ecc)

ALLEGATO 2 — Logistica = impatto minimo

Tutti i soggetti NIS non riconducibili alle tipologie dell'Allegato 1. Tra questi, i settori rimanenti del decreto:

Allegato I del decreto NIS:
n. 3 Settore bancario, n. 4 Infrastrutture dei mercati finanziari, n. 8 Infrastrutture digitali, n. 9 Gestione dei servizi TIC (B2B)

Allegato II del decreto NIS:
n. 6 Fornitori di servizi digitali, n. 7 Ricerca

Allegato III, Allegato IV (escluso n. 1) del decreto NIS

Le tre fasi del processo di categorizzazione

FASE 1
Identificazione

Individuare tutte le attività svolte e i servizi erogati supportati da sistemi informativi e di rete

Oggetto	Ogni attività/servizio ha una denominazione e, opzionalmente, una descrizione
Denominazione	Individuare tutte le attività e i servizi supportati da sistemi informativi e di rete
Dettaglio	Livello di dettaglio a discrezione del soggetto; attività sufficientemente unitarie per categoria
Metodologie	Top-down (processi/organigramma), bottom-up (inventario IT) o combinato
Max per macro-area	Al più 4 attività/servizi per macro-area (una per categoria di rilevanza)

FASE 2
Mappatura

Associare ogni attività/servizio alla macro-area che meglio ne rappresenta finalità e caratteristiche

Criterio	Associare ogni attività/servizio alla macro-area che meglio ne rappresenta finalità e caratteristiche
Unicità	Ogni attività/servizio va associato a una sola macro-area; se riconducibile a più, scomporlo ulteriormente
Copertura	Le 10 macro-aree coprono tutti gli ambiti; «Altri servizi e attività» funge da residuale
Facoltativo	Non è necessario indicare attività/servizi per macro-aree in cui il soggetto non opera

FASE 3
Attribuzione

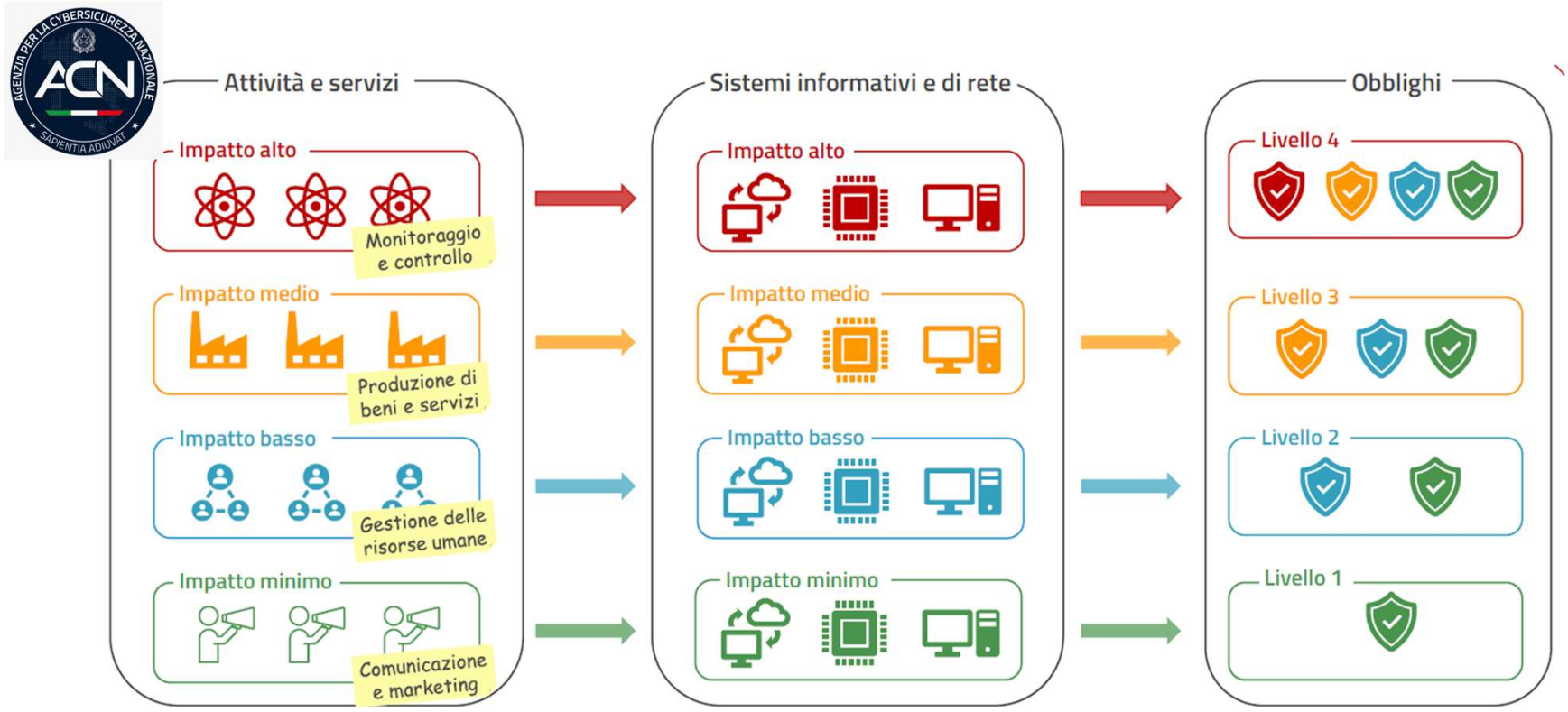
Assegnare a ogni attività/servizio una categoria di rilevanza (default: pre-assegnata)

Regola generale	Le attività/servizi acquisiscono automaticamente la categoria di rilevanza pre-assegnata alla propria macro-area.
Deroga motivata	Il soggetto può indicare una categoria diversa sulla base di una BIA semplificata (riservatezza, integrità, disponibilità). Deve conservare la documentazione.

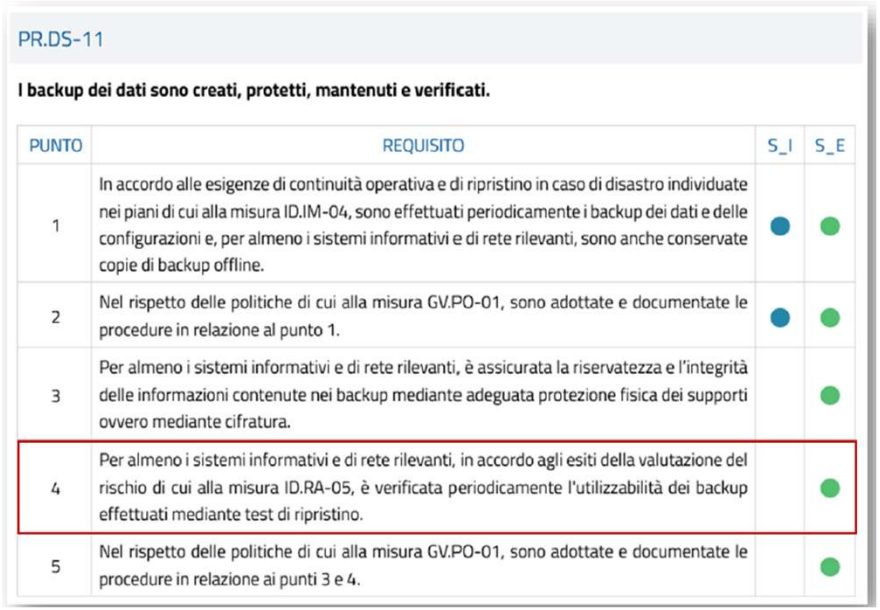
Criteri per applicare la deroga

- Coordinamento delle attività e dei servizi NIS
- Incidenza sulle funzioni di sicurezza
- Interdipendenza con le attività e i servizi NIS
- Natura e/o volume dei dati trattati
- Continuità operativa delle attività e dei servizi NIS

Categorizzazione e obblighi a lungo termine



Le misure di sicurezza di base (Det. ACN 379907/2025)



PR.DS-11

I backup dei dati sono creati, protetti, mantenuti e verificati.

PUNTO	REQUISITO	S_I	S_E
1	In accordo alle esigenze di continuità operativa e di ripristino in caso di disastro individuate nei piani di cui alla misura ID.IM-04, sono effettuati periodicamente i backup dei dati e delle configurazioni e, per almeno i sistemi informativi e di rete rilevanti, sono anche conservate copie di backup offline.	●	●
2	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.	●	●
3	Per almeno i sistemi informativi e di rete rilevanti, è assicurata la riservatezza e l'integrità delle informazioni contenute nei backup mediante adeguata protezione fisica dei supporti ovvero mediante cifratura.		●
4	Per almeno i sistemi informativi e di rete rilevanti, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, è verificata periodicamente l'utilizzabilità dei backup effettuati mediante test di ripristino.		●
5	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 3 e 4.		●

Linee Guida NIS – Specifiche di base – Guida alla lettura (settembre 2025) [https://www.acn.gov.it/portale/documents/d/guest/guida-alla-lettura-specifiche-di-base]

Agenda

- Recepimento e attuazione e prossime scadenze
- Aggiornamento annuale delle informazioni
- Accordi di condivisione delle informazioni e individuazione dei fornitori rilevanti (Determinazione ACN n. 127437/2026)
- Categorizzazione delle attività e dei servizi
- **Sicurezza della catena di approvvigionamento**
- Appendice – Link utili

Sicurezza della catena di approvvigionamento: perché è importante

La catena di approvvigionamento è sempre più esposta a minacce informatiche.

La supply chain come "punto debole"
- Gli attaccanti mirano ai fornitori **terzi**, spesso **meno protetti**, per penetrare nelle reti delle aziende clienti.
- **Attacchi "a cascata"**: una vulnerabilità in un fornitore può propagarsi lungo tutta la filiera.

Visibilità limitata
- Le aziende raramente conoscono l'**intera filiera** (es. fornitori di 3° o 4° livello).
- La **mancanza di trasparenza** rende difficile la gestione proattiva del rischio

Rischi tipici lungo la catena di fornitura
- **Software compromesso** (es. aggiornamenti con malware)
- **Fornitori IT non conformi** agli standard di sicurezza richiesti
- **Componenti** hardware o firmware **alterati**
- **Subappaltatori non tracciati** o fuori controllo dell'organizzazione

Conseguenze potenziali
- Furto di dati, **compromissione dei sistemi**, **interruzione dell'operatività**
- **Responsabilità legale e reputazionale** anche per eventi generati da terze parti
- Impatti su conformità normativa (NIS2 impone responsabilità diretta sulle catene di fornitura critiche)

Le misure di sicurezza di base in materia di sicurezza della catena di approvvigionamento

Determinazione ACN n. 379905/2025

GV.SC-01	**Programma e strategia**	Stabilire **programma, strategia, obiettivi, politiche e processi di gestione del rischio supply chain**. I processi in ambito vedono il coinvolgimento delle funzioni di sicurezza informatica, a partire dalla fase di identificazione e progettazione della fornitura. Sono **definiti requisiti di sicurezza coerenti con la valutazione del rischio**.
GV.SC-02	**Ruoli e responsabilità**	Definire e comunicare alle strutture interne del Soggetto NIS **ruoli e responsabilità in materia di cybersecurity** di **fornitori e partner**
GV.SC-04	**Inventario fornitori**	Mantenere un **inventario aggiornato** dei fornitori di **forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete**, prioritizzati in base alla criticità. Sono tracciati almeno: estremi di **contatto del referente**; **tipologia di fornitura**
GV.SC-05	**Requisiti contrattuali**	Integrare i **requisiti di sicurezza** in **contratti, bandi di gara e accordi** con i fornitori di forni**ture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete** (es: obblighi di sicurezza, audit e ispezioni, recesso, gestione incidenti, supporto nei rapporti con l'autorità competente)
GV.SC-07	**Valutazione del rischio**	**Valutare, registrare, trattare e monitorare i rischi posti dal fornitore nel corso della relazione**. Sono valutati almeno: a) il **livello di accesso** del fornitore ai sistemi informativi; b) **accesso del fornitore a dati** del Soggetto NIS; c) impatto di **grave interruzione** della fornitura; d) **tempi e costi di ripristino** in caso di indisponibilità dei servizi; e) **ruoli e responsabilità** del fornitore nel governo dei sistemi informativi e di rete.

Ruoli e responsabilità nel processo

CdA / Vertice aziendale	Approva la governance per la sicurezza della *supply chain*. Riceve report periodici. Delibera su risk acceptance e piani di trattamento ad alto impatto.
AD / Direttore Generale	Assicura l'attuazione delle decisioni del CdA e la disponibilità di risorse. Presidia l'escalation su fornitori critici e situazioni ad alto rischio.
Resp. Sicurezza Informatica	Supervisiona l'applicazione della procedura. Definisce requisiti minimi, criteri di classificazione, metodologie di due diligence e riesame.
Procurement	Coordina l'intero ciclo di vita della fornitura: selezione, contrattualizzazione, monitoraggio. Conserva l'inventario fornitori.
Process Owner (PO)	Identifica il fabbisogno, collabora alla valutazione del rischio e supporta il monitoraggio in corso di rapporto.
Responsabile protezione dati personali (DPO)	Coinvolto quando la fornitura comporta il trattamento di dati personali per le opportune valutazioni.

Il processo di gestione del rischio della catena di approvvigionamento sulla sicurezza

Il processo si applica a tutte le forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete, inclusi:

- Servizi **IT/Cloud** (IaaS, PaaS, SaaS)
- **Connettività e telecomunicazioni**
- **Sviluppo e manutenzione software**
- **Hardware** e **componenti di rete**
- **Servizi di sicurezza gestiti** (MSSP/SOC)
- **Outsourcing** di processi IT e OT

Suggerimenti sugli strumenti operativi del processo da adottare per la conformità

Procedura di gestione della sicurezza della *supply chain*

Documento che formalizza il processo end-to-end: ambito di applicazione, fasi, ruoli, responsabilità, criteri di valutazione e monitoraggio.

Risk assessment e inventario

Documentazione per la pre-valutazione del rischio della fornitura, la definizione dei requisiti proporzionati e il tracciamento dell'inventario fornitori.

Questionari di qualifica

Questionari specifici per livello di rischio (es: Basso, Medio, Alto, Molto Alto) con controlli attesi, criteri di adeguatezza e documentazione a supporto.

Agenda

- Recepimento e attuazione e prossime scadenze
- Aggiornamento annuale delle informazioni
- Accordi di condivisione delle informazioni e individuazione dei fornitori rilevanti (Determinazione ACN n. 127437/2026)
- Categorizzazione delle attività e dei servizi
- Sicurezza della catena di approvvigionamento
- **Appendice – Link utili**

Appendice – Link utili

Decreto NIS – D. Lgs 138/2024

- https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2024-09-04;138!vig=

Misure di sicurezza e incidenti di sicurezza informatica di base:

- https://www.acn.gov.it/portale/nis/modalita-specifiche-base (pagina generale)
- https://www.acn.gov.it/portale/documents/d/guest/detacn_obblighi_2511-v3_signed (Determinazione ACN 379907/2025)
- https://www.acn.gov.it/portale/documents/d/guest/allegato-1-v2 (Det. ACN 379907/2025, Allegato 1 – Soggetti importanti)
- https://www.acn.gov.it/portale/documents/d/guest/allegato-2-v2 (Det. ACN 379907/2025, Allegato 2 – Soggetti essenziali)
- https://www.acn.gov.it/portale/documents/d/guest/allegato-3-v2 (Det. ACN 379907/2025, Allegato 3 – Soggetti importanti)
- https://www.acn.gov.it/portale/documents/d/guest/allegato-4-v2 (Det. ACN 379907/2025, Allegato 4 – Soggetti essenziali)

Aggiornamento delle informazioni:

- https://www.acn.gov.it/portale/documents/d/guest/detacn_piattaformanis_251218-v9_signed (Determinazione ACN 127437/2026)

Fornitori rilevanti – Codici CPV:

- https://ted.europa.eu/it/simap/cpv (Regolamento CE 213/2008)

Categorizzazione delle attività e dei servizi:

- https://www.acn.gov.it/portale/documents/d/guest/detacn_categorizzazione_260409-v8_signed (Determinazione ACN 155238/2026)
- https://www.acn.gov.it/portale/documents/d/guest/allegato_1_modello260409-v1 (Det. ACN 155238/2026 - Allegato 1)
- https://www.acn.gov.it/portale/documents/d/guest/allegato_2_modello260409-v1 (Det. ACN 155238/2026 - Allegato 2)
- https://www.acn.gov.it/portale/documents/d/guest/modello-di-categorizzazione-nis-guida-alla-lettura (Modello di categorizzazione - Guida alla lettura)

DataConSec

DATA PROTECTION - CONSULTING - SECURITY

V.le Fratti, 56 Parma - Italia
Tel. e Fax: +39 0521 77 12 98
e-mail: info@dataconsec.com
web: www.dataconsec.com