DATACONSEC

DATA PROTECTION - CONSULTING - SECURITY

Direttiva NIS2: ambito di applicazione, adempimenti e procedura di registrazione al portale

UNINDUSTRIA REGGIO EMILIA

Webinar, 12 febbraio 2025

INDICE

DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

PARTE 1
Introduzione alla NIS 2: obiettivi e scadenze

DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

Strategia generale UE Cybersecurity

«*La cibersicurezza è una delle principali **priorità** della Commissione UE nonché il fondamento di un'Europa Digitale e connessa. Un alto livello di sicurezza informatica è necessario, non solo per mantenere i **servizi essenziali** e per il funzionamento della **società** e dell'**economia**, ma anche per salvaguardare l'**integrità fisica** dei cittadini*»

PERIODO	DESCRIZIONE
2013	Strategia cibersicurezza UE
2016	**Direttiva NIS** e GDPR
2017	Prima revisione della Strategia cibersicurezza UE
2019	Cybersecurity Act (maggiori poteri all'ENISA e definizione quadro comune per le certificazioni servizi/prodotti ICT)
2020-2030	Seconda revisione della Strategia cibersicurezza UE per il decennio digitale
2023	**Direttiva NIS 2**, DORA e Cyber Resiliency ACT
2024-2025	**17 ottobre 2024** recepimento **Direttiva NIS 2** e 17 gennaio 2025 applicazione DORA

Normativa NIS 2 – Quali novità?

Direttiva NIS2 – 2022/2555

Estensione ambiti di applicazione

- **18 settori: 11 settori altamente critici** (originariamente 8) e **7 settori critici** (originariamente 0)
- **Intera infrastruttura ICT** (originariamente solo reti e sistemi serventi i servizi essenziali)

Processo di identificazione dei soggetti

- **Soggetti** distinti tra entità **essenziali e importanti**
- **Identificazione automatica** sulla base di criteri oggettivi (da **media imprese in su**, salvo eccezioni)
- L'Autorità ha anche la facoltà di identificare ulteriori soggetti

Rafforzamento degli obblighi

- Misure di sicurezza specifiche e **proporzionate rispetto al rischio** posto al sistema informativo e di rete
- Approccio **multi-rischio** (coordinamento con Direttiva CER)
- Processo di notifica più dettagliato
- Poteri di esecuzione, ispettivi e sanzionatori rafforzati (**allineamento alle sanzioni GDPR**)

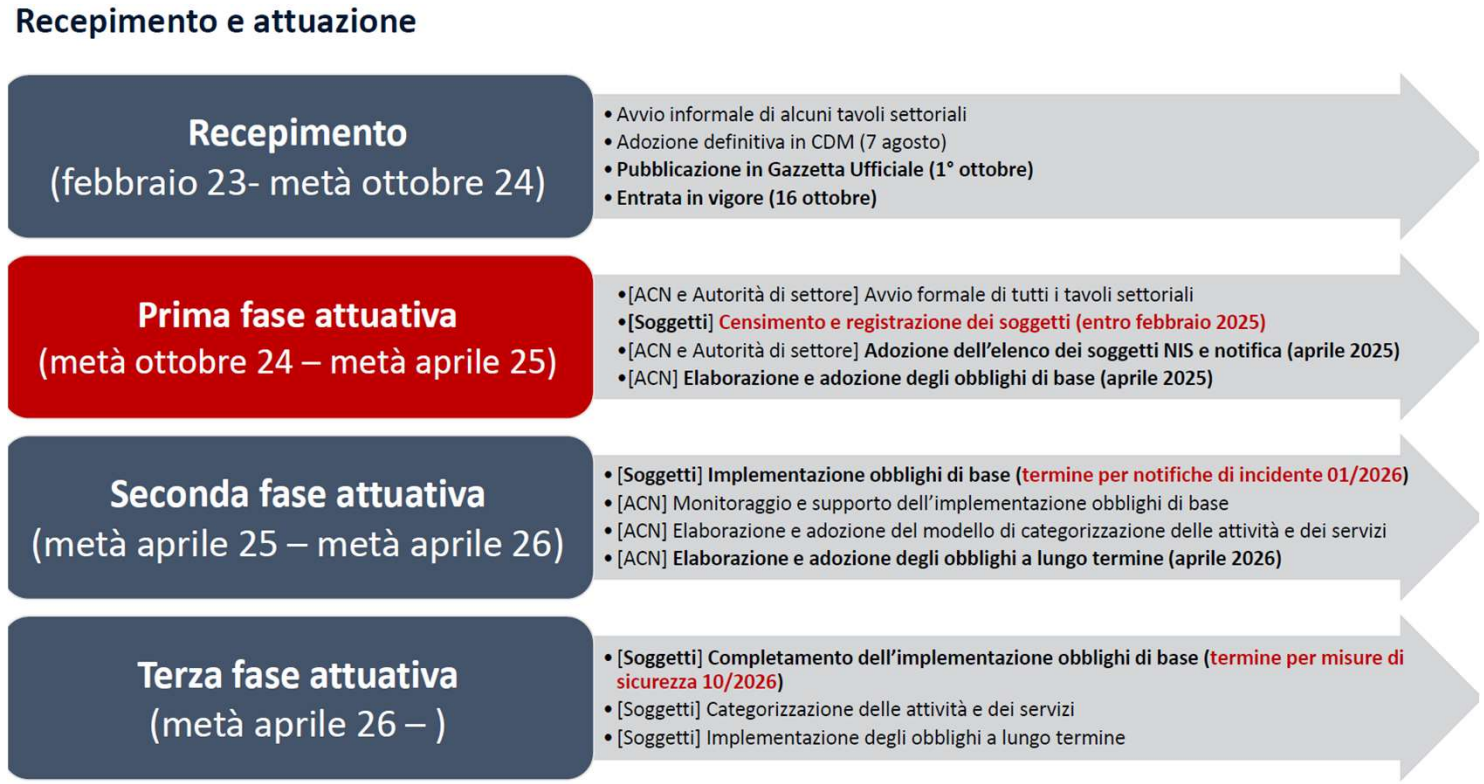
Nuovi strumenti

- **Divulgazione coordinata delle vulnerabilità (CVD)**
- **Cyber crisis liaison organisation network** (CyCLONe) e Autorità nazionale competente per la gestione delle crisi informatiche
- Revisione tra pari e mutua assistenza

D.Lgs. 138/2024 in vigore dal 16 ottobre 2024

DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

Normativa NIS 2 – Recepimento e attuazione



DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

Normativa NIS 2 – Contatti con l'Autorità

DIRETTIVA NIS2

CSIRT ITALIA – Portali e caselle istituzionali

PORTALE PUBBLICO

- **Consultabile liberamente** all'indirizzo **https://www.csirt.gov.it**
- Condivisione **Alert, bollettini, monografie** e **Indicatori** relativi a minacce cyber
- Contenuti e informazioni ad accesso pubblico con **TLP WHITE**

PORTALE COLLABORATION

- Dedicato ai **soggetti NIS, PSNC** ed altri di interesse
- Contenuti ad accesso controllato con **TLP GREEN, AMBER, RED**
- Accreditamento tramite richiesta del soggetto (info@csirt.gov.it)

CASELLE DI POSTA ISTITUZIONALI

- Segnalazioni relative a **eventi** di **cybersicurezza**
- Comunicazioni punto-punto relative a **specifiche evidenze**
- **Interlocuzioni** di **natura tecnica** in materia di cybersicurezza

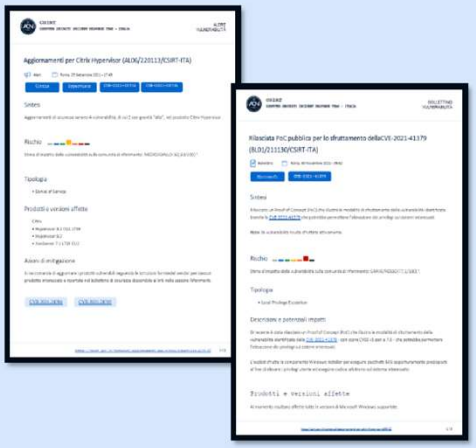
POSTA ELETTRONICA ORDINARIA:
info@csirt.gov.it
POSTA ELETTRONICA CERTIFICATA:
csirt@pec.acn.gov.it

DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

Normativa NIS 2 – Risorse disponibili

DIRETTIVA NIS2

CSIRT ITALIA - Documentazione tecnica



Alert e bollettini su nuove campagne e vulnerabilità, contenenti gli indicatori di compromissione (IoC) e le azioni di mitigazioni consigliate

Pubblicazioni specialistiche su specifiche minacce, contenenti il dettaglio tecnico dei malware e delle TTP impiegate ed i relativi IoC

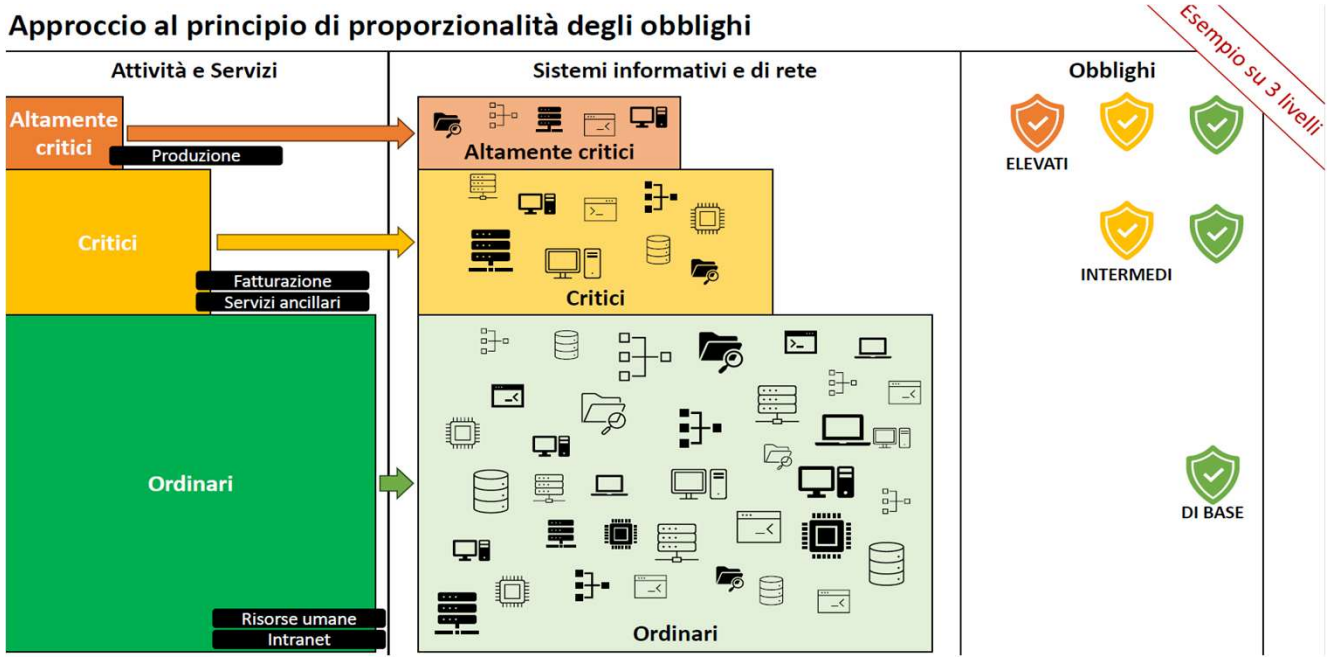
Report contenente l'analisi della postura di sicurezza degli asset esposti su Internet, usando lo stesso punto di vista di una minaccia esterna

DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

PARTE 2
Ambito di Applicazione e casi particolari

DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

Normativa NIS 2 – Proporzionalità e gradualità degli obblighi



SOGGETTI ORDINARI = NON SOGGETTI NIS 2 MA …non devono pensare di non investire in misure di sicurezza anche perché inseriti in filiere e quindi saranno chiamati ad adottare un numero minimo di misure di sicurezza…….

DataConSec
DATA PROTECTION - CONSULTING - SECURITY

Normativa NIS 2 – Settori Altamente critici*

Settore	Dettaglio	Grandi imprese	Medie imprese	Piccole e micro imprese
SETTORI ALTAMENTE CRITICI				
Energia	19 tipologie di soggetto	Essenziali	Importanti *	Fuori ambito **
Trasporti	10 tipologie di soggetto			
Settore bancario	DORA Lex specialis			
Infrastrutture dei mercati finanziari				
Settore sanitario	5 tipologie di soggetto			
Acqua potabile	1 tipologia di soggetto			
Acque reflue	1 tipologia di soggetto			
Infrastrutture digitali	9 tipologie di soggetto			
Gestione dei servizi TIC (b2b)	2 tipologie di soggetto		Importanti *	Fuori ambito **
Spazio	1 tipologia di soggetto			

(*) Il dettaglio degli ambiti di applicazione è riportato al sito: https://www.acn.gov.it/portale/documents/d/guest/faq-1-5_dettaglio-ambiti-di-applicazione

PER VERIFICARE L'APPARTENENZA AD UN SETTORE OCCORRE FARE RIFERIMENTO AL CODICE ATECO e CLASSIFICAZIONE NACE (es. Fabbricazione di apparecchiature elettriche: imprese rientranti nella sezione C, divisione 26 della NACE rev 2.)

DataConSec
DATA PROTECTION - CONSULTING - SECURITY

Normativa NIS 2 – Altri settori Critici

Settore	Sottosettore o tipologia di soggetto	Grandi imprese (occupano almeno 250 dipendenti oppure hanno un fatturato di almeno 50ME oppure hanno un bilancio di almeno 43ME)	Medie imprese (occupano almeno 50 dipendenti oppure hanno un fatturato di almeno 10ME oppure hanno un bilancio di almeno 10ME)	Piccole e micro imprese
1. Servizi postali e di corriere	1. Fornitori di servizi postali quali definiti all'articolo 2, punto 1 bis), della direttiva 97/67/CE, tra cui i fornitori di servizi di corriere	Importanti[1]		Non in ambito[2]
2. Gestione dei rifiuti	1. Imprese che si occupano della gestione dei rifiuti quali definite all'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio, escluse quelle per cui la gestione dei rifiuti non è la principale attività economica			
3. Fabbricazione, produzione e distribuzione di sostanze chimiche	1. Imprese che si occupano della fabbricazione di sostanze e della distribuzione di sostanze o miscele di cui all'articolo 3, punti 9) e 14), del regolamento (CE) n. 1907/2006 del Parlamento europeo e del Consiglio e imprese che si occupano della produzione di articoli quali definite all'articolo 3, punto 3), del medesimo regolamento, da sostanze o miscele			
4. Produzione, trasformazione e distribuzione di alimenti	1. Imprese alimentari quali definite all'articolo 3, punto 2), del regolamento (CE) n. 178/2002 del Parlamento europeo e del Consiglio che si occupano della distribuzione all'ingrosso e della produzione industriale e trasformazione			
5. Fabbricazione	1. Fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro 2. Fabbricazione di computer e prodotti di elettronica e ottica 3. Fabbricazione di apparecchiature elettriche 4. Fabbricazione di macchinari e apparecchiature n.c.a. 5. Fabbricazione di autoveicoli, rimorchi e semirimorchi 6. Fabbricazione di altri mezzi di trasporto			
6. Fornitori di servizi digitali	1. Fornitori di mercati online 2. Fornitori di motori di ricerca online 3. Fornitori di piattaforme di social network			
	4. Fornitori di servizi di registrazione dei nomi di dominio	Importanti[1]		
7. Ricerca	1. Organizzazioni di ricerca	Importanti[1]		Non in ambito[2]

DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

Definizione di PMI secondo l'Allegato alla Raccomandazione 2003/361/CE

Categoria di impresa	Effettivi: unità lavorative-anno (ULA)	Fatturato annuo	o	Totale di bilancio annuo
Medie imprese	< 250	≤ 50 milioni di euro	o	≤ 43 milioni di euro
Piccole imprese	< 50	≤ 10 milioni di euro	o	≤ 10 milioni di euro
Microimprese	< 10	≤ 2 milioni di euro	o	≤ 2 milioni di euro

DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

Impresa Autonoma, Impresa Associata e Impresa Collegata

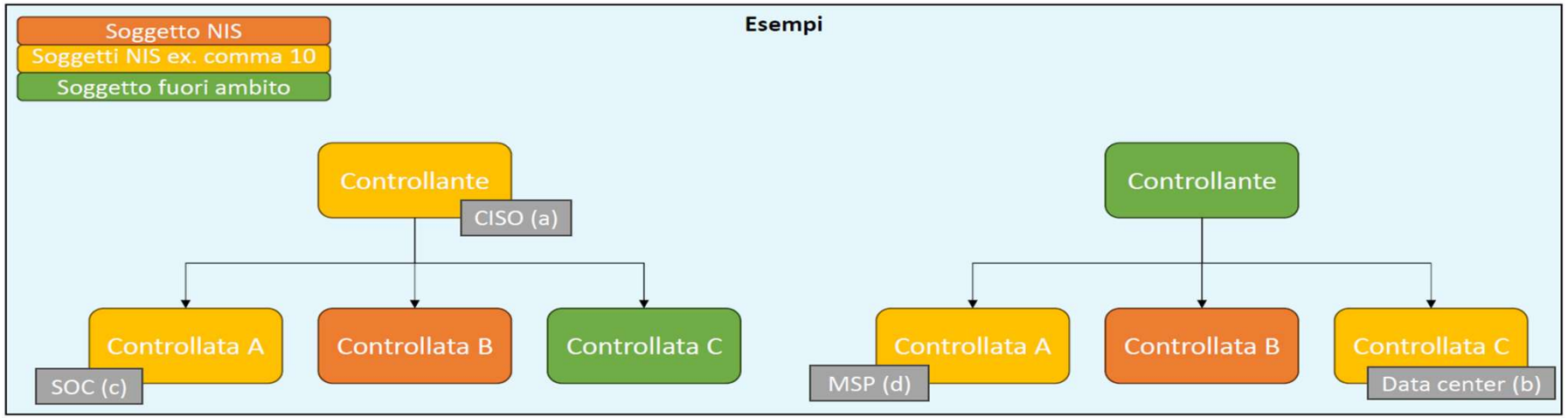
DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

Casi particolari 1: Imprese collegate – Particolari tipologie

Approfondimento sull'ambito di applicazione – Imprese collegate

ARTICOLO 3 – Ambito di applicazione

10. Il presente decreto si applica, infine, indipendentemente dalle sue dimensioni, all'impresa collegata ad un soggetto essenziale o importante, se soddisfa almeno uno dei seguenti criteri:
    a) adotta decisioni o esercita una influenza dominante sulle decisioni relative alle misure di gestione del rischio per la sicurezza informatica di un soggetto importante o essenziale;
    b) detiene o gestisce sistemi informativi e di rete da cui dipende la fornitura dei servizi del soggetto importante o essenziale;
    c) effettua operazioni di sicurezza informatica del soggetto importante o essenziale;
    d) fornisce servizi TIC o di sicurezza, anche gestiti, al soggetto importante o essenziale



DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

Casi particolari 2: Clausola di salvaguardia

Approfondimento sull'ambito di applicazione – Clausola di salvaguardia

ARTICOLO 3 – Ambito di applicazione

4. Per determinare se un soggetto è da considerarsi una media o grande impresa ai sensi dell'articolo 2 dell'allegato della raccomandazione 2003/361/CE, si applica l'articolo 6, paragrafo 2, del medesimo allegato, salvo che ciò non sia proporzionato, tenuto anche conto dell'indipendenza del soggetto dalle sue imprese collegate in termini di sistemi informativi e di rete che utilizza nella fornitura dei suoi servizi e in termini di servizi che fornisce.
12. L'Autorità nazionale competente NIS applica la clausola di salvaguardia di cui al comma 4, secondo i criteri per la determinazione individuati con le modalità di cui all'articolo 40, comma 1.

ARTICOLO 11 – Autorità di settore

4. Le Autorità di settore NIS, per i rispettivi settori e sottosettori di competenza ai fini di cui al comma 1, procedono, in particolare:
   c) all'individuazione dei soggetti a cui si applicano le deroghe di cui all'articolo 3, comma 4;

ARTICOLO 40 – Attuazione

1. Con uno o più decreti del Presidente del Consiglio dei ministri[...]:
   a) sono definiti i criteri per l'applicazione della clausola di salvaguardia di cui all'articolo 3, comma 4;

L'impresa A, operante nel settore della Fabbricazione (sezione C, divisione 27, del NACE), ha 20 dipendenti (inferiore a 50) e un fatturato di 5 M€ (inferiore a 10). Se fosse un'impresa autonoma sarebbe considerata piccola e non rientrerebbe nell'ambito di applicazione del decreto NIS

L'impresa A è collegata all'impresa B (anche non operante in settori NIS) che ha 60 dipendenti e un fatturato di 4 M€. In linea generale, ai sensi dell'articolo 6, paragrafo 2, della raccomandazione 2003/361/CE, si sommano i parametri e quindi l'impresa A è considerata una media impresa operante nel settore della Fabbricazione che rientra nell'ambito di applicazione del decreto NIS.

Tuttavia, l'impresa A può richiedere all'Autorità nazionale competente l'applicazione della clausola di salvaguardia. Qualora, d'intesa con l'Autorità di settore, si ritenessero soddisfatti i criteri del DPCM in materia, verrebbe disapplicato l'articolo 6, paragrafo 2, della raccomandazione 2003/361/CE. L'impresa A verrebbe quindi considerata come autonoma, riconducendola alla categoria delle piccole imprese e non rientrerebbe più nell'ambito di applicazione.

Casi particolari 3 – Individuazione del soggetto da parte di ACN

Approfondimento sull'ambito di applicazione – Individuazioni dell'Autorità

ARTICOLO 3 – Ambito di applicazione

8. Il presente decreto si applica, altresì, indipendentemente dalle loro dimensioni, anche ai soggetti delle tipologie di cui all'allegato IV, individuati secondo le procedure di cui al comma 13.
9. Il presente decreto si applica, altresì, anche ai soggetti dei settori o delle tipologie di cui agli allegati I, II, III e IV, indipendentemente dalle loro dimensioni, individuati secondo le procedure di cui al comma 13, qualora:
   a) il soggetto sia identificato prima della data di entrata in vigore del presente decreto [OSE, ndr];
   b) il soggetto sia l'unico fornitore nazionale di un servizio che è essenziale per il mantenimento di attività sociali o economiche fondamentali;
   c) una perturbazione del servizio fornito dal soggetto potrebbe avere un impatto significativo sulla sicurezza pubblica, l'incolumità pubblica o la salute pubblica;
   d) una perturbazione del servizio fornito dal soggetto potrebbe comportare un rischio sistemico significativo, in particolare per i settori nei quali tale perturbazione potrebbe avere un impatto transfrontaliero;
   e) il soggetto sia critico in ragione della sua particolare importanza a livello nazionale o regionale per quel particolare settore o tipo di servizio o per altri settori indipendenti nel territorio dello Stato;
   f) il soggetto sia considerato critico ai sensi del presente decreto quale elemento sistemico della catena di approvvigionamento, anche digitale, di uno o più soggetti considerati essenziali o importanti.
13. I **soggetti di cui ai commi 8 e 9 sono individuati dall'Autorità nazionale competente NIS, su proposta delle Autorità di settore** [...]. **L'Autorità nazionale competente NIS notifica a tali soggetti** la loro individuazione ai fini della registrazione di cui all'articolo 7, comma 1.

ALLEGATO IV – Ulteriori tipologie di soggetto

1. Soggetti che forniscono servizi di trasporto pubblico locale.
2. Istituti di istruzione che svolgono attività di ricerca.
3. Soggetti che svolgono attività di interesse culturale.
4. Società in house, società partecipate e società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175

Esempi

1. L'impresa A fornisce un servizio di trasporto pubblico locale
   → il MIT, sulla base di propri criteri, può proporne l'individuazione quale soggetto NIS
2. L'impresa B operante nel settore energia è una piccola impresa
   → il MASE può determinare che l'impresa soddisfa almeno uno dei criteri del comma 8 e proporne individuazione quale soggetto NIS.
3. La PA C è considerata importante ai sensi del decreto
   → La PCM può determinare che PA C soddisfa almeno uno dei criteri del comma 8 e proporne individuazione quale soggetto essenziale.

DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

PARTE 3
Procedura di Registrazione al Portale (per soggetti obbligati) entro il 28 febbraio 2025

DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

Registrazione al Portale ACN – Informazioni necessarie

Elenco dei **codici ATECO che caratterizzano le attività svolte e i servizi erogati** dal soggetto, con particolare riferimento all'ambito di applicazione del decreto NIS

Normative europee settoriali citate dal decreto NIS per delimitarne l'ambito di applicazione che si applicano al soggetto

Numero di dipendenti, il **fatturato** e il **bilancio** del soggetto (NB: qualora il soggetto non sia una impresa autonoma, il numero di dipendenti, il fatturato e il bilancio del soggetto calcolato ai sensi della raccomandazione 2003/361/CE, con particolare riguardo all'articolo 6, paragrafo 2, dell'allegato alla raccomandazione medesima)

Elenco delle **tipologie di soggetto di cui agli allegati I, II, III e IV**, a cui è riconducibile il soggetto

Autovalutazione del soggetto quale essenziale, importante o fuori ambito, sulla base di quanto previsto dagli articoli 3 e 6 del decreto NIS

Per i soggetti che non sono imprese autonome (ovvero hanno **imprese collegate, associate e/o fanno parte di un gruppo di imprese**), in fase di registrazione sarà inoltre necessario fornire **specifiche informazioni**

DataConSec
DATA PROTECTION - CONSULTING - SECURITY

Registrazione al Portale ACN – Punto di contatto

Il Punto di contatto è il **rappresentante legale** o un suo **procuratore generale** oppure un **dipendente delegato del soggetto**.

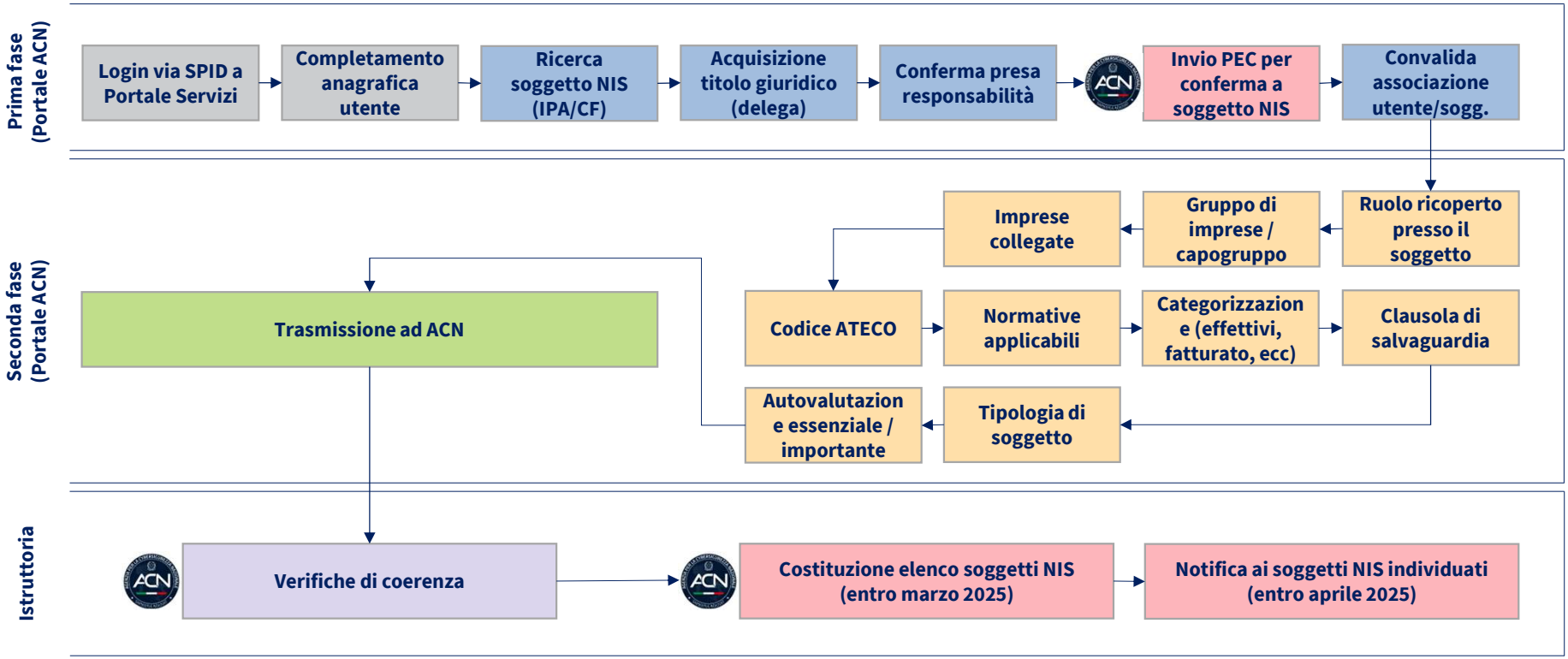
Nel caso in cui il Punto di contatto sia un **dipendente delegato** del soggetto, nel corso della registrazione, si dovrà **caricare il titolo giuridico che lo delega** a operare per conto del soggetto nel contesto NIS.

I soggetti che fanno parte di un **gruppo di imprese** possono **designare** quale punto di contatto il **dipendente di un'altra impresa** che rientra nell'ambito di applicazione del decreto NIS e **che fa parte del medesimo gruppo di imprese**.

- nome e cognome
- luogo e data di nascita
- codice fiscale
- cittadinanza
- paese di residenza e, ove richiesto, di domicilio
- indirizzo di posta elettronica ordinaria, preferibilmente individuale, nonché di servizio, aziendale o professionale
- ove disponibile, un indirizzo di posta elettronica certificata, preferibilmente individuale, nonché di servizio, aziendale o professionale
- numero di telefono, preferibilmente individuale, nonché di servizio, aziendale o professionale
- ove disponibile, un numero alternativo di telefono, preferibilmente individuale di servizio, aziendale o professionale
- codice fiscale soggetto NIS

DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

Registrazione al Portale ACN – Processo



DataConSec
DATA PROTECTION - CONSULTING - SECURITY

PARTE 4
Adeguamento alla NIS 2: ambiti di intervento (per i soggetti obbligati) e consigli (per tutti)

DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

Adeguamento alla NIS 2: da dove partire?

PRIMA FASE – GAP ANALYSIS E PIANO DI RIMEDIO

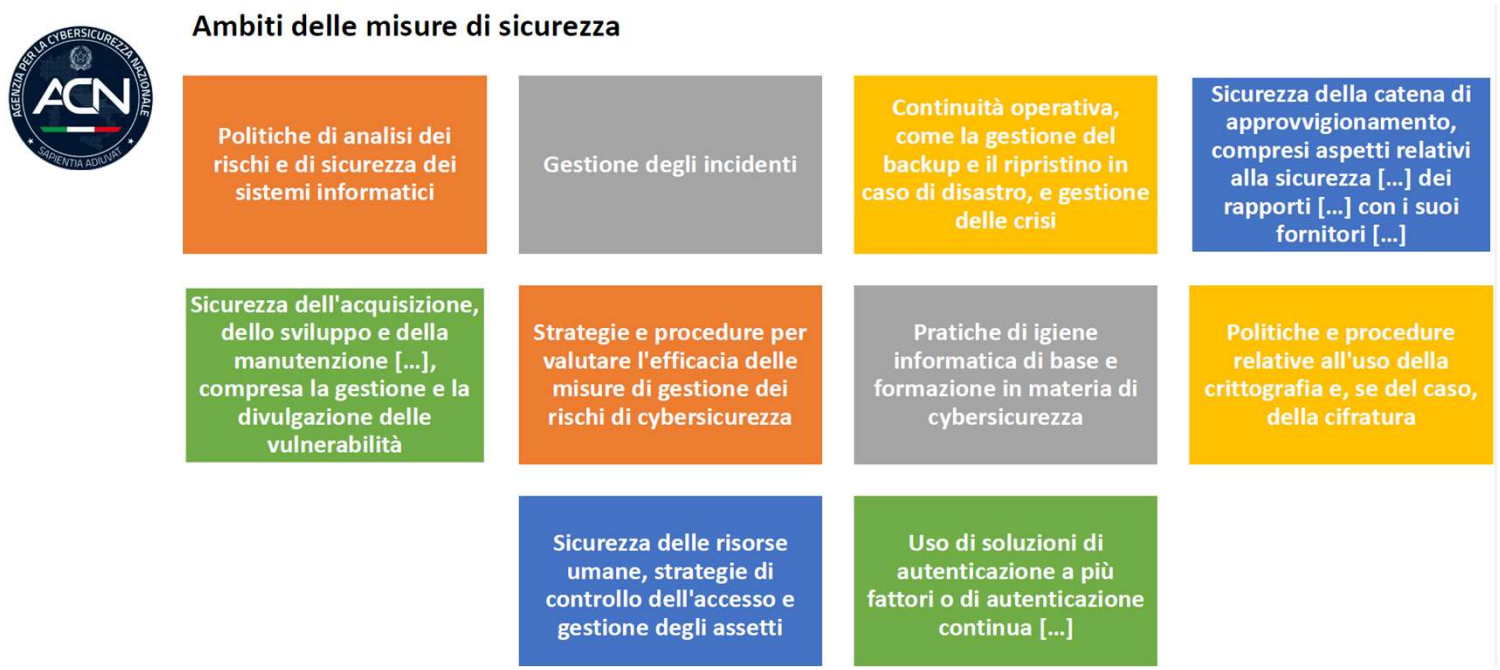
- Identificazione dei **processi** critici
- Determinazione degli **asset informatici** a supporto dei processi critici
- Valutazione dei **gap** con la normativa
- Stesura piano di **rimedio** con le priorità di azione

SECONDA FASE – IMPLEMENTAZIONE

- Svolgimento **analisi dei rischi**
- Stesura **policy** e **procedure** (focus gestione **incidenti)**
- Implementazioni **misure di sicurezza**
- **Formazione**
- Revisione contratti e sicurezza della **catena di fornitura**

DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

Normativa NIS 2 – Ambiti delle misure di sicurezza



Nota 1: La sicurezza della catena di approvvigionamento impatta anche sui soggetti fuori dal perimetro NIS 2, qualora questi offrano servizi a soggetti essenziali o importanti.

Nota 2: In generale, organi di amministrazione e direttivi dei soggetti NIS2 hanno un ruolo fondamentale: sono chiamati ad approvare piani, sovraintendere, formarsi, promuovere la formazione del personale, ecc.

Normativa NIS 2 – Gli adempimenti per i soggetti obbligati

- **Politiche di analisi dei rischi e di sicurezza dei sistemi informatici**
- **Gestione degli incidenti**
- **Continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi**
- **Sicurezza della catena di approvvigionamento**
- **Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità**
- **Strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza**
- **Pratiche di igiene informatica di base e formazione in materia di cibersicurezza**
- **Politiche e procedure relative all'uso della crittografia e, se del caso, cifratura**
- **Sicurezza delle risorse umane, strategie di controllo dell'accesso e asset mgmt**

ALCUNE ATTIVITÀ DI CONFORMITÀ:

- Definizione della **Governance** (Atti CdA, deleghe, ruoli responsabilità e politica cyber di alto livello)
- Analisi dei **rischi**, VA&PT periodici
- Procedura gestione **incidenti**
- BIA, Business **Continuity** Plan, Disaster Recovery Plan, Procedura back up e ripristino, procedura gestione delle **crisi**
- Revisione clausole **contrattuali** con i fornitori, NDA, check-list e report di audit
- Procedura **sviluppo** software sicuro
- **Audit** interni
- Regolamenti interni utenti, **formazione** cyber
- Regole sull'utilizzo della **cifratura**
- Procedure di **controllo accessi** logici, MFA, asset inventory
- Sicurezza **fisica** (perimetro, accessi, cablaggi, UPS)

DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

Normativa NIS 2 – Suggerimenti per i soggetti coinvolti nella filiera (non obbligati NIS 2)

Gestione degli incidenti

Continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi

Sicurezza della catena di approvvigionamento

Pratiche di igiene informatica di base e formazione in materia di cibersicurezza

Sicurezza delle risorse umane, strategie di controllo dell'accesso e asset mgmt

ALCUNE ATTIVITÀ SUGGERITE:

- Procedura gestione **incidenti**
- BIA, Business **Continuity** Plan, Disaster Recovery Plan, Procedura back up e ripristino, procedura gestione delle **crisi**
- Revisione clausole **contrattuali** con i fornitori, NDA, check-list e report di audit
- Regolamenti interni utenti, **formazione** cyber
- Procedure di **controllo accessi** logici, MFA, asset inventory
- Sicurezza **fisica** (perimetro, accessi, cablaggi, UPS)

DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

Focus – Sanzioni

Sanzioni amministrative (articolo 38)

Violazioni gravi

- Mancata osservanza degli obblighi relativi agli organi di amministrazione, alle misure di sicurezza e alle notifiche di incidente
- Inottemperanza alle disposizioni dell'Autorità nazionale competente NIS
- Sanzioni pecuniarie fino a 10 MEUR o 2% per soggetti essenziali e fino a 7 MEUR o 1,4% per soggetti importanti

Altre violazioni

- Mancata registrazione, comunicazione dei dati, osservanza degli obblighi relativi alle certificazioni, alla registrazione dei nomi di dominio e alle previsioni settoriali specifiche
- Sanzioni pecuniarie fino a 0,1% per soggetti essenziali e fino a 0,07% per soggetti importanti

Maggiorazione per reiterazione e sanzioni accessorie (anche per le persone fisiche)

Strumenti deflattivi del contenzioso

Regime più favorevole per la PA

DataConSec

DATA PROTECTION - CONSULTING - SECURITY

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