La nuova disciplina NIS

11/11/2025

Agenda

1. Principi generali
2. Governo e supervisione
3. Obblighi
4. Specifiche di base
5. Misure di sicurezza
6. Incidenti di sicurezza
7. Prossimi passi

Principi generali

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** su sistemi informativi e di rete
- Approccio **multi-rischio** (coordinamento con CER)
- Processo di notifica più dettagliato
- Poteri di esecuzione, ispettivi e sanzionatori rafforzati (**allineamento sanzioni GDPR**)

Nuovi strumenti

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

Ambito di applicazione

Settori, sottosettori e tipologie di soggetti introdotti dalla NIS2

[1] Possibile identificazione dell'Autorità come essenziali

[2] Possibile identificazione dell'Autorità come importanti o essenziali

Settore	Dettaglio	Grandi imprese	Medie imprese	Piccole e micro imprese
SETTORI ALTAMENTE CRITICI				
Energia (+)	19 tipologie di soggetto	Essenziali	Importanti[1]	Fuori ambito[2]
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			
Spazio	1 tipologia di soggetto			
SETTORI CRITICI				
Servizi postali e di corriere	1 tipologia di soggetto			
Gestione dei rifiuti	1 tipologia di soggetto			
Fabbricazione, produzione e distribuzione di sostanze chimiche	1 tipologia di soggetto			
Produzione, trasformazione e distribuzione di alimenti	1 tipologia di soggetto			
Fabbricazione	6 tipologie di soggetto			
Fornitori di servizi digitali (+)	4 tipologie di soggetto			
Ricerca	1 tipologia di soggetto			
ULTERIORI TIPOLOGIE DI SOGGETTI				
Pubblica Amministrazione centrale		Identificazione dell'Autorità		
Pubblica Amministrazione regionale e locale	11 categorie di PA			
Ulteriori tipologie di soggetti	4 tipologie e 2 criteri aggiuntivi			

I numeri

Oltre 30K organizzazioni censite

Oltre 20K soggetti NIS

Oltre 5K soggetti essenziali

Oltre 1K richieste di revisione e registrazioni tardive

Oltre 40K ticket evasi

Recepimento e attuazione

Febbraio 23 - metà ottobre 24

Recepimento

- Avvio informale di alcuni tavoli settoriali
- Adozione definitiva in CDM (7 agosto)
- **Pubblicazione in Gazzetta Ufficiale (1° ottobre)**
- **Entrata in vigore (16 ottobre)**

Metà ottobre 24 - metà aprile 25

Prima fase attuativa

- [ACN e Autorità di settore] Avvio formale di tutti i tavoli settoriali
- **[Soggetti]** Censimento e registrazione dei soggetti (entro febbraio 2025)
- [ACN e Autorità di settore] **Adozione dell'elenco dei soggetti NIS e notifica (aprile 2025)**
- [ACN] **Elaborazione e adozione degli obblighi di base (aprile 2025)**

Metà aprile 25 - metà ottobre 26

Seconda fase attuativa

- **[Soggetti] Aggiornamento annuale** (termine 07/2025)
- **[Soggetti] Implementazione obblighi di base** (termine per notifiche di incidente 01/2026)
- [ACN] Monitoraggio e supporto dell'implementazione obblighi di base
- [ACN] Elaborazione e adozione del modello di categorizzazione delle attività e dei servizi
- [ACN**] Elaborazione e adozione degli obblighi a lungo termine (aprile 2026)**

Da metà aprile 26

Terza fase attuativa

- **[Soggetti] Completamento dell'implementazione obblighi di base (**termine per misure di sicurezza 10/2026**)**
- [Soggetti] Categorizzazione delle attività e dei servizi
- [Soggetti] Implementazione degli obblighi a lungo termine

Governo e supervisione

Autorità e Tavolo interministeriale

Autorità nazionale competente NIS

Autorità di settore NIS

Altri membri del tavolo

Agenzia per la cybersicurezza nazionale

PCM

MEF

MIMIT

MASAF

MASE

MIT

MUR

MIC

MSAL

Conferenza permanente
per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano

Autorità nazionale competente NIS

Autorità nazionale competente NIS

- Sovrintende all'implementazione e all'attuazione del decreto NIS e predispone i provvedimenti
- Svolge le funzioni e le attività di regolamentazione, anche adottando linee guida, raccomandazioni e orientamenti non vincolanti
- Individua i soggetti essenziali e i soggetti importanti nonché **redige l'elenco dei soggetti NIS**;
- Partecipa al Gruppo di cooperazione NIS, nonché ai consessi e alle iniziative promosse a livello di Unione europea relativi all'attuazione della direttiva NIS2
- **Definisce gli obblighi in materia di registrazione** (art. 7), di **responsabilità degli organi di amministrazione e direttivi** (art. 23), di **misure di sicurezza** (art. 24), di **notifica di incidente** (art. 25) e di registrazione dei nomi di dominio (art. 29)
- Svolge le **attività di monitoraggio, analisi e supporto** (art. 35)
- Esercita i **poteri ispettivi** (art. 36), di **esecuzione** (art. 37) e **sanzionatori** (art. 38)

Autorità di settore NIS e Tavoli di settore

Autorità di settore NIS

- **Verificano l'elenco dei soggetti NIS**
- **Supportano l'individuazione dei soggetti essenziali e dei soggetti importanti**
- Individuano i soggetti a cui si applicano le deroghe di cui all'articolo 3, comma 4;
- Supportano le funzioni e le attività di regolamentazione
- Elaborano dei contributi per la relazione annuale
- **Istituiscono e coordinano i tavoli settoriali**, al fine di contribuire **all'efficace e coerente attuazione settoriale** del decreto NIS nonché al relativo **monitoraggio**.
- Partecipano alle attività settoriali del Gruppo di Cooperazione NIS

Tavoli di settore

- **Camera di compensazione e confronto con i settori/soggetti NIS** per una efficace attuazione della disciplina
- Individuazione di criticità e condivisione di approcci in fase legislativa e regolamentare
- Monitoraggio dell'attuazione


AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT

Obblighi

Base giuridica

D.Lgs. 138/2024

Art. 23
Organi di amministrazione e direttivi

Art. 24
Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica

Art. 25
Obblighi in materia di notifica di incidente

Art. 31
Proporzionalità e gradualità degli obblighi

Art. 40
Attuazione

Art. 42
Fase di prima applicazione

Det. ACN 164179/2025

Allegato 1
Misure di sicurezza di base soggetti importanti

Allegato 2
Misure di sicurezza di base soggetti essenziali

Allegato 3
Incidenti significativi di base soggetti importanti

Allegato 4
Incidenti significativi di base soggetti essenziali

Organi di amministrazione e direttivi

- Approvano modalità implementazione misure di sicurezza
- Sovrintendono all'implementazione degli obblighi
- Sono responsabili delle eventuali violazioni

- Sono tenuti a seguire formazione in materia di cybersicurezza
- Promuovono la formazione dei propri dipendenti

Elementi misure di sicurezza

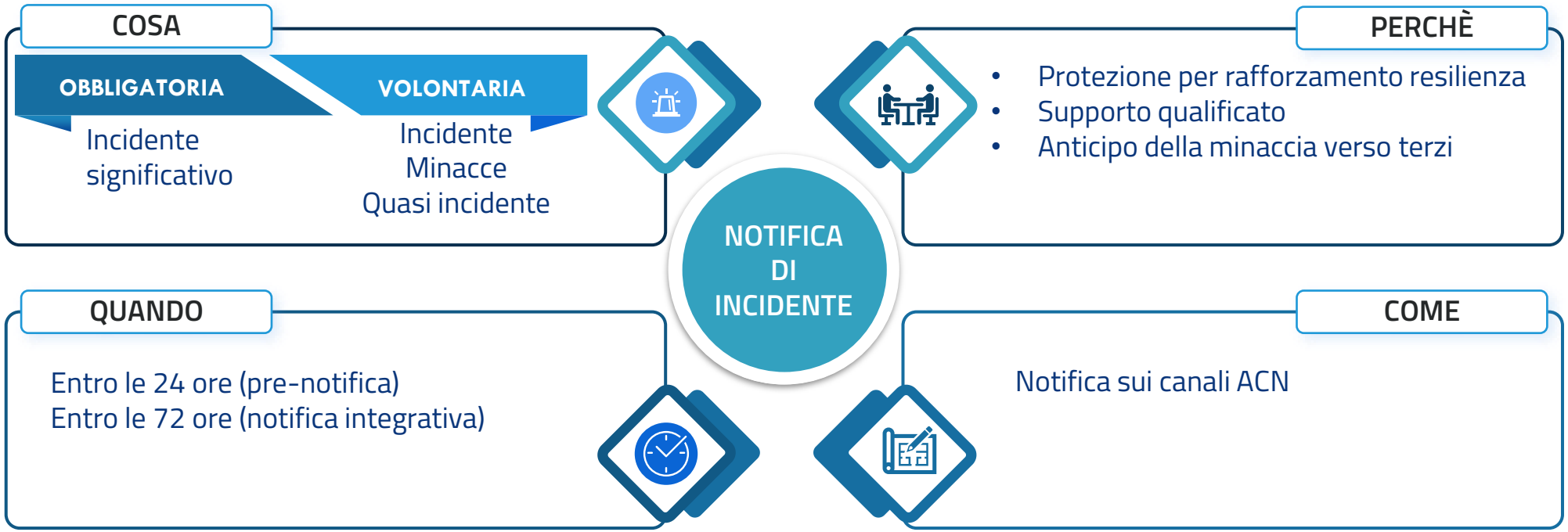
a) Politiche di analisi dei rischi e di sicurezza dei sistemi informativi.	b) Gestione degli incidenti.	c) Continuità operativa, inclusa la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi.	d) Sicurezza catena di approvvigionamento, compresi aspetti relativi sicurezza rapporti con diretti fornitori o fornitori di servizi.	e) Sicurezza acquisizione, sviluppo e manutenzione sistemi informativi e di rete, ivi compresa gestione e divulgazione vulnerabilità.
f) Politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza.	g) Pratiche di igiene informatica di base e formazione in materia di cybersicurezza.	h) Politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura.	i) Sicurezza risorse umane, strategie di controllo dell'accesso e gestione degli assetti.	j) Uso di soluzioni di autenticazione a più fattori o di autenticazione continua e di sistemi di comunicazione protetti.

Elementi obblighi in materia di misure di gestione dei rischi per la sicurezza informatica (art. 24, c. 2 d.lgs. 138/2024)

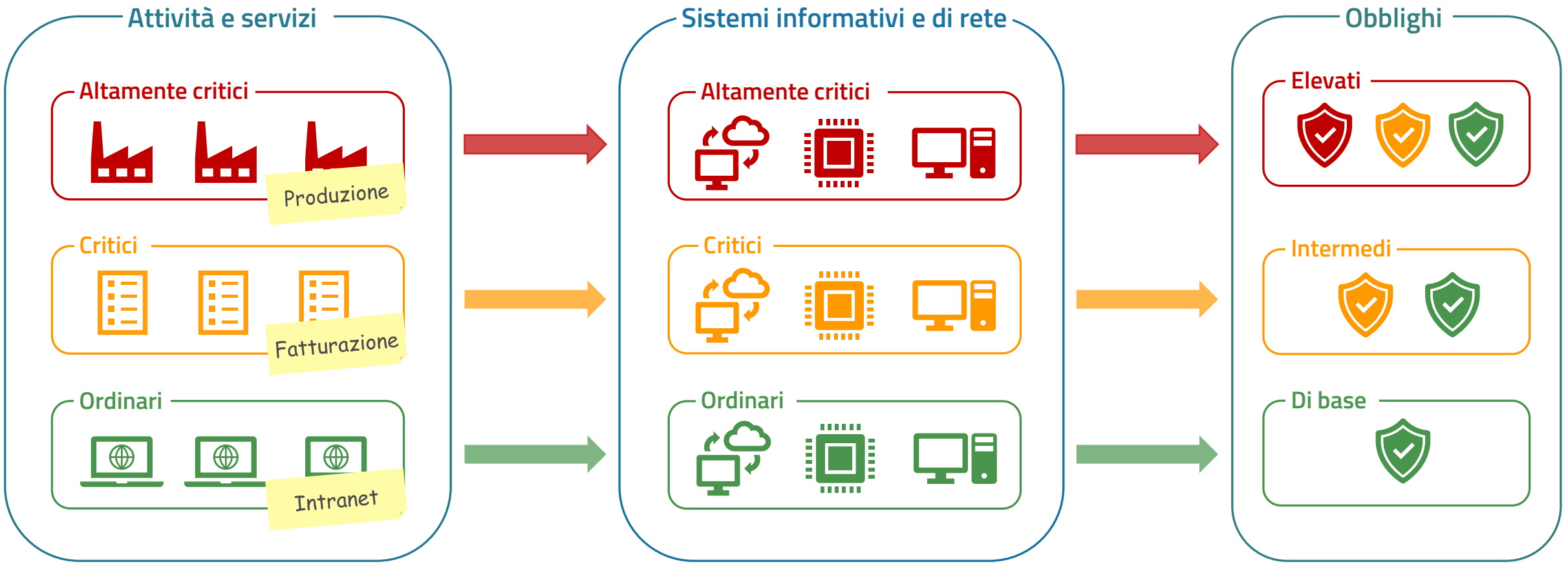
Notifiche di incidente

L'OBBLIGO DI NOTIFICA DECORRE A PARTIRE DAL 1 GENNAIO 2026

NOTIFICHE VOLONTARIE POSSIBILI FIN DA SUBITO



Proporzionalità degli obblighi



Gradualità degli obblighi

Specifiche di base

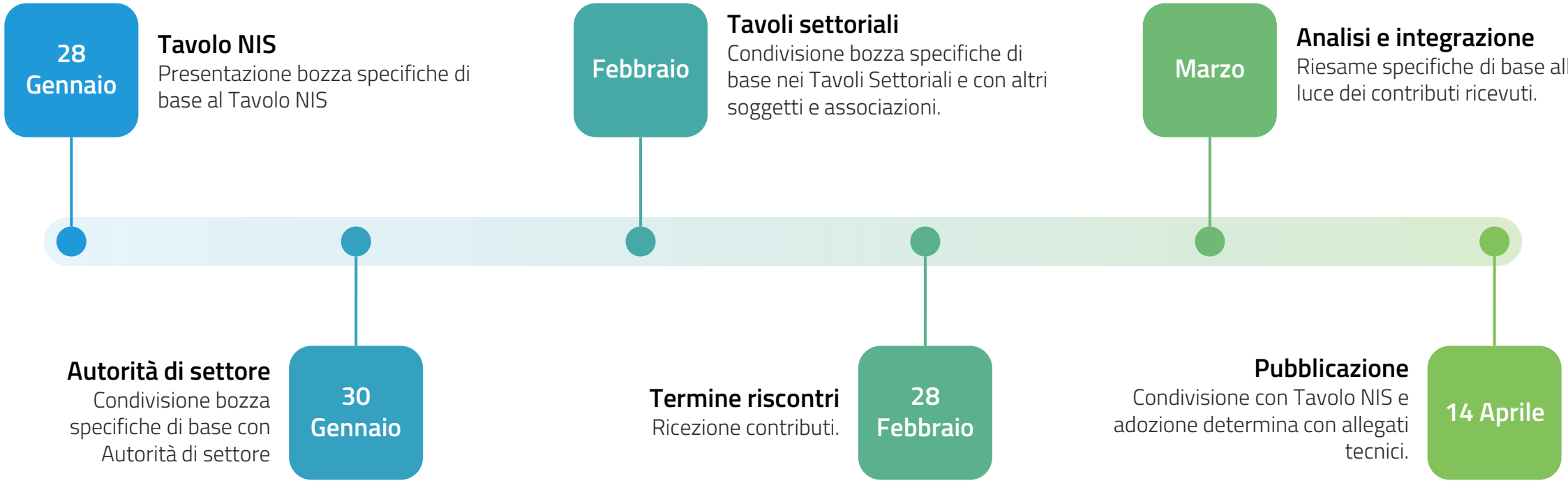
Specifiche degli obblighi, anche orizzontali, minimi per tutta l'infrastruttura con un orizzonte a breve termine.

Specifiche a lungo termine

Obblighi, anche settorializzati e potenzialmente ambiziosi, proporzionati in base alla categorizzazione e con scadenze a medio e lungo termine.

Specifiche di base

Processo di adozione



Processo di sviluppo

Framework Core

Edizione 2025

Funzioni	Categorie	Sottocategorie	Informative References
GOVERNO (GV)			
IDENTIFICAZIONE (ID)			
PROTEZIONE (PR)			
RILEVAMENTO (DE)			
RISPOSTA (RS)			
RIPRISTINO (RC)			

Framework contestualizzato

42 sotto-categorie

Funzioni	Categorie	Sottocategorie	Informative References
GOVERNO (GV)			
IDENTIFICAZIONE (ID)			
PROTEZIONE (PR)			
RILEVAMENTO (DE)			
RISPOSTA (RS)			
RIPRISTINO (RC)			

Misure di sicurezza

ALLEGATO 2

Misure di sicurezza di base per i soggetti essenziali

1. GOVERNO (GOVERN)

1.1. **Contesto organizzativo (GV.OC)**: Il contesto – missione, aspettative degli stakeholder, dipendenze e requisiti legali, normativi e contrattuali – che influisce sulle decisioni di gestione del rischio di cybersecurity dell'organizzazione è compreso[1].

1.1.1. **GV.OC-4**: Gli obiettivi, le capacità e i servizi critici dai quali gli stakeholder dipendono o che si aspettano dall'organizzazione sono compresi e comunicati.

1. È mantenuto un elenco aggiornato dei sistemi informativi e di rete rilevanti.

1.2. **Strategia di gestione del rischio (GV.RM)**: Le priorità, i vincoli, le dichiarazioni sulla tolleranza e la propensione al rischio, e le assunzioni dell'organizzazione sono stabilite, comunicate e utilizzate per supportare le decisioni sul rischio operativo.

1.2.1. **GV.RM-03**: Le attività e gli esiti della gestione del rischio di cybersecurity sono parte integrante dei processi di gestione del rischio dell'organizzazione.

1. Nell'ambito dei processi di gestione del rischio del soggetto NIS e nel rispetto delle politiche di cui alla misura GV.PO-01, è definito, attuato, aggiornato e documentato un piano di gestione dei rischi per la sicurezza informatica per identificare, analizzare, valutare, trattare e monitorare i rischi.

Selezione sottocategorie

Definizione requisiti

Previsioni normative
ambiti, specificità, obiettivi

Best practices

Approccio basato sul rischio (1/2)

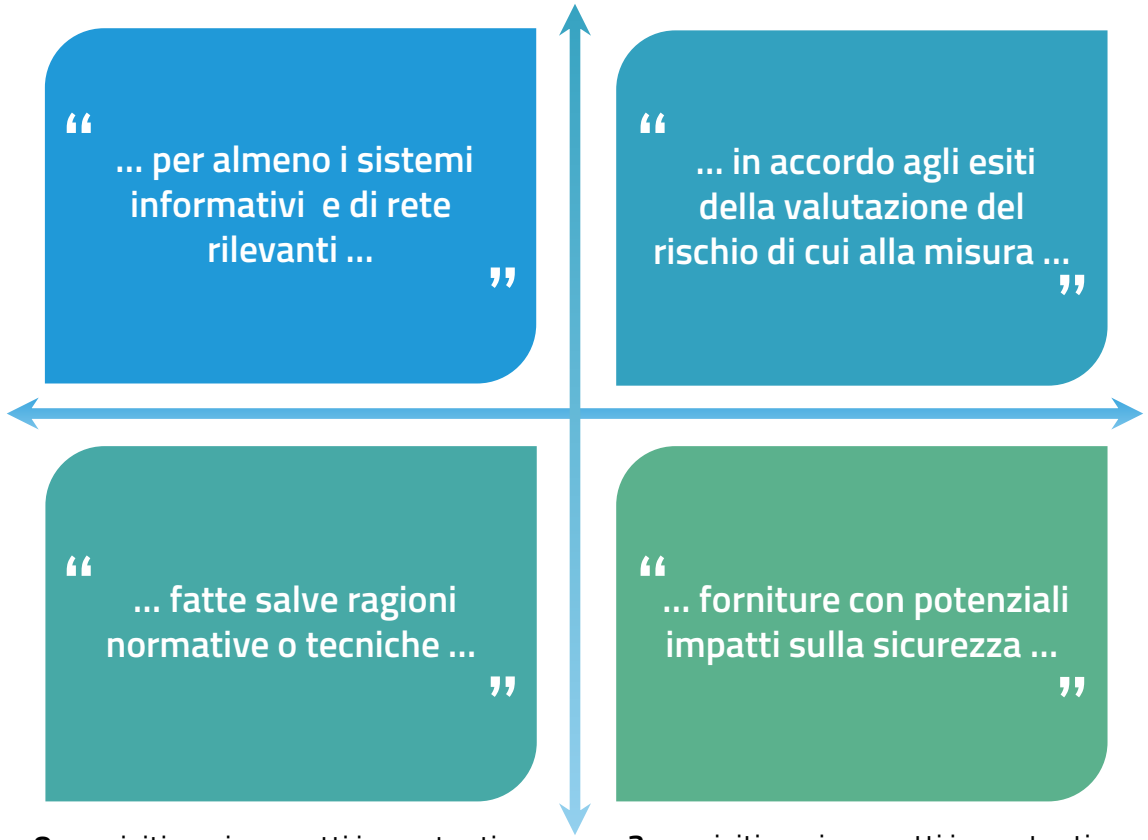
Ambito	Livello di rischio	Proporzionalità	Approccio	Clausole
Le misure di sicurezza si applicano a tutti i sistemi informativi e di rete del soggetto.	Ogni sistema informativo e di rete è caratterizzato da un proprio livello di rischio.	L'art. 31 del decreto prevede che si tenga conto, nello stabilire gli obblighi, del grado di esposizione dei soggetti ai rischi.	Le misure di sicurezza sono state sviluppate secondo un approccio basato sul rischio.	Previsione per i requisiti di maggiore complessità di specifiche clausole.

Approccio basato sul rischio (2/2)

13 requisiti per i soggetti importanti e **22** per i soggetti essenziali

5 requisiti per i soggetti importanti e **8** per i soggetti essenziali

Facoltà di limitare l'ambito di applicazione per specifici requisiti ai sistemi informativi di rete la cui compromissione determina un impatto significativo su R, I, D per i servizi e le attività per i quali il soggetto rientra nell'ambito di applicazione del decreto NIS



Possibilità di adattare le modalità di attuazione di specifici requisiti sulla base degli esiti della valutazione del rischio.

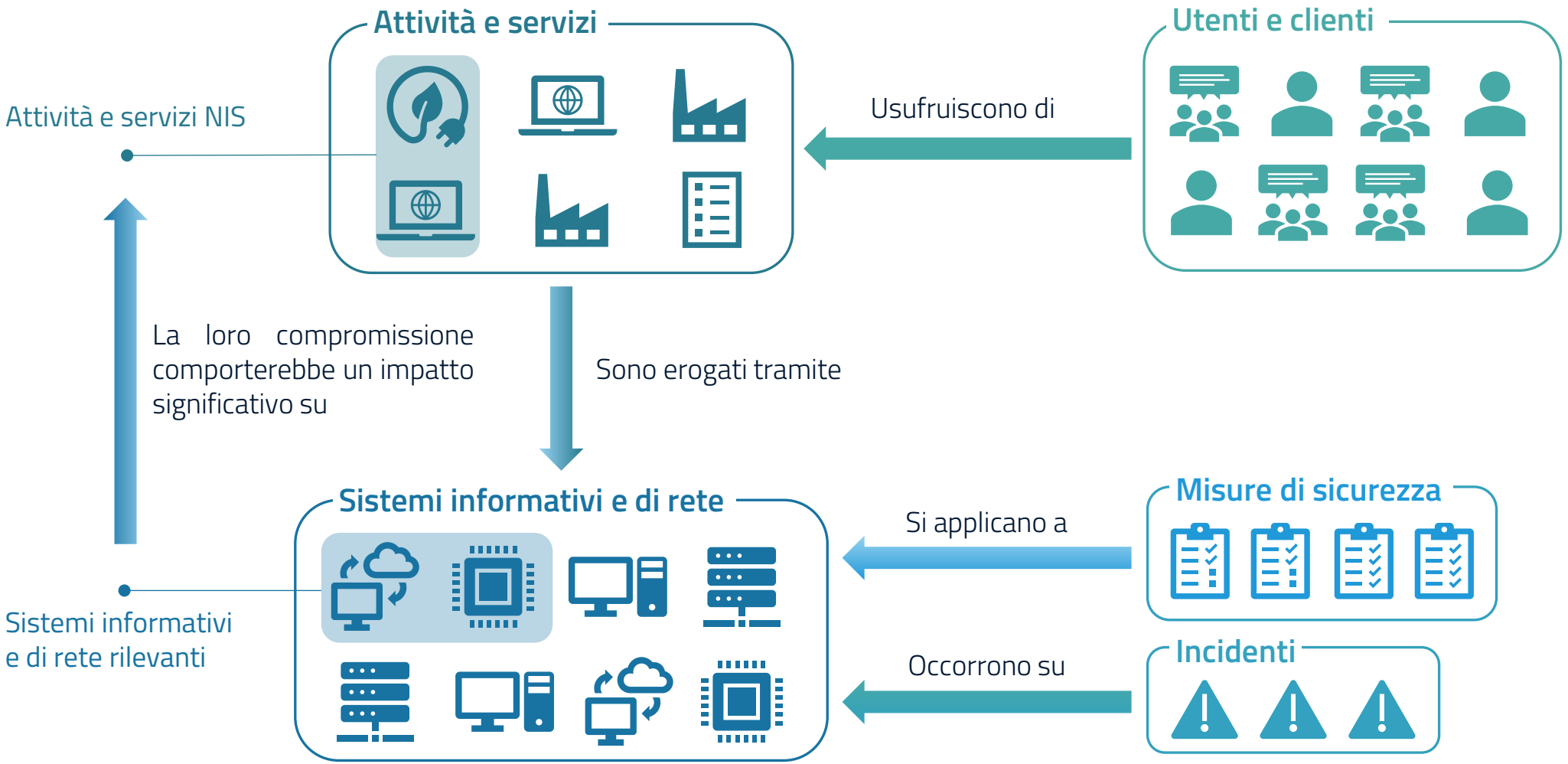
Deroga all’applicazione del requisito se sussistono vincoli normativi (ad esempio, leggi o regolamenti) o tecnici (ad esempio, limiti tecnologici o operativi) che non ne permettano l’implementazione

Sono considerate le forniture la cui eventuale compromissione può determinare effetti sulla sicurezza dei sistemi informativi e di rete.

8 requisiti per i soggetti importanti e **10** per i soggetti essenziali

3 requisiti per i soggetti importanti e per i soggetti essenziali

Modello concettuale



Misure di sicurezza

Linee guida

- Guida alla lettura
- Processo di gestione degli incidenti
- Notifica degli incidenti
- …

Misure di sicurezza di base (1/2)

Struttura misura

Codice | **Descrizione** | **Requisiti**

- Il codice identificativo e la descrizione della misura fanno riferimento al FNCS versione 2025.
- I requisiti indicano ciò che è richiesto ai fini dell'implementazione.

Misure di sicurezza

- **37** per soggetti importanti ed essenziali.
- **6** per i soli soggetti essenziali.

Requisiti

- **87** per soggetti importanti ed essenziali.
- **29** per i soli soggetti essenziali.

Misure di sicurezza di base (2/2)

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, 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.		●

Incidenti significativi

Incidenti significativi di base (1/2)

IS-1	Il soggetto NIS ha evidenza della perdita di riservatezza, verso l'esterno, di dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.
IS-2	Il soggetto NIS ha evidenza della perdita di integrità, con impatto verso l'esterno, di dati di sua proprietà o sui quali esercita il controllo, anche parziale.
IS-3	Il soggetto NIS ha evidenza della violazione dei livelli di servizio attesi dei suoi servizi e/o delle sue attività, sulla base dei livelli di servizio atteso (SL) definiti ai sensi della misura DE.CM-01.
IS-4	Il soggetto NIS ha evidenza, anche sulla base di parametri quali-quantitativi definiti ai sensi della misura DE.CM-01, dell'accesso, non autorizzato o con abuso dei privilegi concessi, a dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.

Soggetti importanti ed essenziali
3 tipologie di incidenti

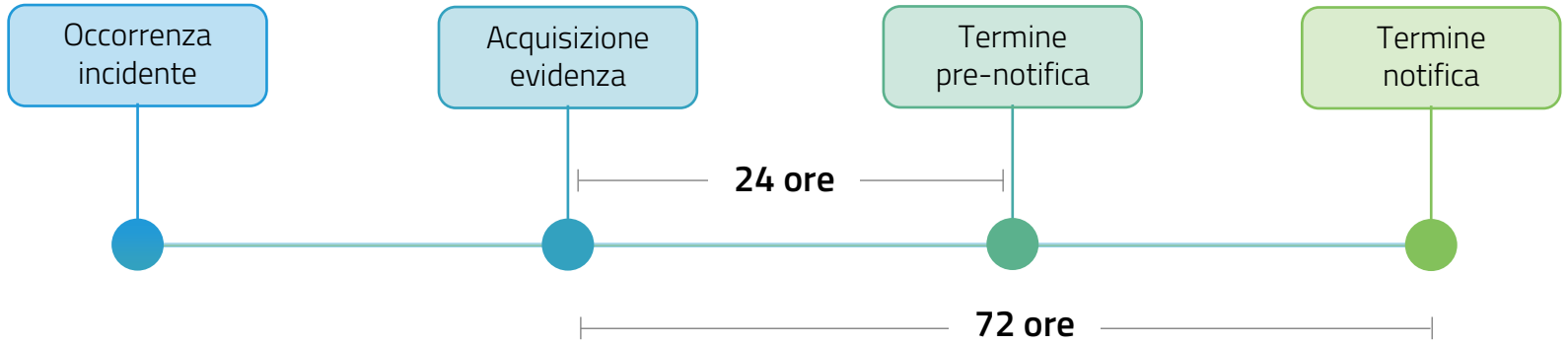
Solo soggetti essenziali
1 tipologia di incidente

Incidenti significativi di base (2/2)

Evidenza dell'incidente

Ai fini dell'adempimento dell'obbligo di notifica degli incidenti ciò che rileva è che il soggetto abbia evidenza del verificarsi di una delle tipologie di incidente indicate.

L'acquisizione dell'evidenza definisce il momento dal quale decorre il termine per l'obbligo di notifica.



Abuso dei privilegi concessi

Fattispecie in cui un operatore abbia l'autorizzazione tecnica (ossia la disponibilità di credenziali che sono configurate per accedere ai dati) per accedere a determinati dati ma tale acceso sia effettivamente illecito in quanto, ad esempio, effettuato in violazione delle politiche del soggetto o risulti strumentale al perseguimento di scopi estranei alle necessità funzionali di accesso..

Prossimi passi

Ruoli previsti e censiti in piattaforma

Componenti degli organi di amministrazione e direttivi

- Sono i vertici dell'organizzazione
  i.e., Rappresentante legale, CDA (o equivalente) monocratico o collegiale, etc.
- Approvano e sovrintendono all'implementazione degli obblighi
- Sono responsabili delle violazioni

Punto di contatto

- Cura l'attuazione degli obblighi e interloquisce con l'Autorità nazionale competente NIS
- È supportato dal sostituto punto di contatto
- Entrambi sono persone fisiche interne al soggetto (o altra PA soggetto NIS)

Referente CSIRT

- Interloquisce con lo CSIRT Italia ed effettua le notifiche obbligatorie e volontarie
- Può essere coadiuvato da sostituti referenti CSIRT
- Possiede almeno competenze di base e conosce l'infrastruttura ICT del soggetto

Scadenze

Ottobre 25
- Aggiornamento annuale

Dicembre 25
- Referente CSIRT

Gennaio 26
- Notifiche di incidente

Febbraio 26
- Registrazione annuale

Maggio 26
- Aggiornamento annuale

Giugno 26
- Categorizzazione

Ottobre 26
- Misure di sicurezza

…
- Comunicazione


AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT