Il sistema Anci a supporto
della digitalizzazione
dei Comuni

DIPARTIMENTO
PER LA TRASFORMAZIONE
DIGITALE

anci

Finanziato
dall'Unione europea
NextGenerationEU

Rapporti e differenze tra L. 90/2024 e NIS 2

Nicolò Rivetti di Val Cervo

Capo Divisione NIS e discipline unionali, Servizio Regolazione, ACN

Identificare alcuni elementi chiave

Comprendere le differenze tra la Legge 28 giugno 2024, n. 90 - **Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici** e la **Direttiva NIS 2** (Direttiva UE 2022/2555)

Decreto Legislativo NIS 2 (principi generali)

La Direttiva NIS 2 – 2022/2555

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

anci

Finanziato dall'Unione europea NextGenerationEU

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)
- Il Governo 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
- Estensione Strategia

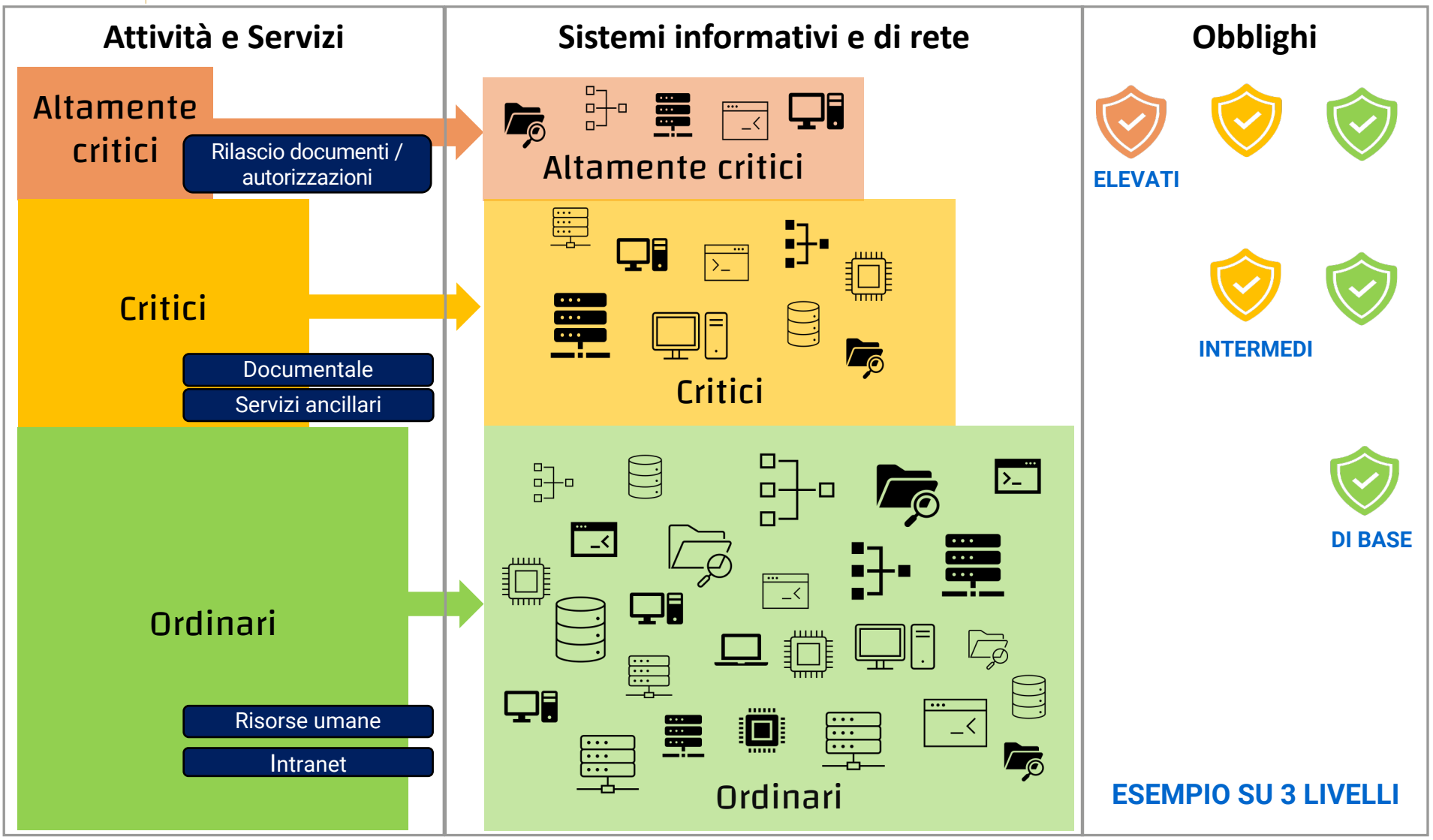
Decreto Legislativo NIS 2

Ambito di applicazione

[1] Possibile identificazione governativa come essenziali
[2] Possibile identificazione governativa 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	2 tipologie di soggetto			
ULTERIORI TIPOLOGIE DI SOGGETTI				
Pubblica Amministrazione centrale				
Pubblica Amministrazione regionale e locale	11 categorie di PA			
Ulteriori tipologie di soggetti	5 tipologie e 2 criteri aggiuntivi	**Identificazione governativa**		

Approccio al principio di proporzionalità degli obblighi



Fasi del recepimento e dell'attuazione

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

Finanziato dall'Unione europea NextGenerationEU

Recepimento (febbraio 23 - metà ottobre 24)

- Avvio informale di alcuni tavoli settoriali
- Adozione definitiva in CDM (7 agosto)
- Pubblicazione in Gazzetta Ufficiale (~fine settembre)
- Entrata in vigore (entro 17 ottobre)

Prima fase attuativa (metà ottobre 24 - metà aprile 25)

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

Seconda fase attuativa (metà aprile 25 - metà aprile 26)

- Implementazione degli obblighi di base (notifica Q1 2026, misure di sicurezza Q3 2026)
- Monitoraggio e supporto dell'implementazione obblighi di base
- Elaborazione e adozione del modello di categorizzazione delle attività e dei servizi
- Elaborazione e adozione degli obblighi a lungo termine

Terza fase attuativa (metà aprile 26 -)

- Categorizzazione delle attività e dei servizi
- Implementazione degli obblighi a lungo termine

Comparativa

Ambito di applicazione Legge 90 del 2024 e NIS

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

anci

Finanziato dall'Unione europea NextGenerationEU

LEGGE 90	DECRETO NIS
Pubbliche amministrazioni centrali	Pubbliche amministrazioni centrali
Regioni e Province autonome di Trento e di Bolzano	Regioni e Province autonome di Trento e di Bolzano
Città metropolitane	Città metropolitane
Comuni con popolazione superiore a 100.000 ab.	Comuni con popolazione superiore a 100.000 ab.
Comuni capoluoghi di regione	Comuni capoluoghi di regione
TPL urbano con utenza ≥ 100.000 ab. e extra urbano operanti nelle città metropolitane	Società di trasporto pubblico ritenute critiche dall'Autorità di settore (MIT)
ASL	ASL
Società in house (informatica, trasporto pubblico, acque reflue, rifiuti)	Società in house, società partecipate o a controllo pubblico ritenute critiche dall'Autorità di settore (PCM)
	Soggetti pubblici (e privati) dei settori elencati negli allegati I e II del decreto, inclusi i settori delle infrastrutture digitali, servizi digitali, MSP, gestione dei rifiuti e delle acque reflue riconducibili a media o grande impresa.

Obblighi Legge 90/2024 e NIS

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

Finanziato dall'Unione europea NextGenerationEU

Legge 90/2024

- Referente
- Misure di sicurezza
- Notifica di incidente
- Indicazioni ACN

Decreto NIS

- Punto di contatto
- Misure di sicurezza
- Notifica di incidente
- Poteri di esecuzione
- Responsabilità dirigenziale

Ambiti delle misure di sicurezza L. 90 E NIS

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

Finanziato dall'Unione europea NextGenerationEU

LEGGE 90/2024

1. Sviluppo delle politiche e delle procedure di sicurezza delle informazioni
2. Produzione e aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico
3. Produzione e aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione
4. Produzione e aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione
5. Pianificazione e attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici […]
6. Pianificazione e attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale
7. Monitoraggio e valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza

DECRETO NIS

1. Politiche di analisi dei rischi e di sicurezza dei sistemi informatici
2. Gestione degli incidenti
3. Continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi
4. Sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza […] dei rapporti […] con i suoi fornitori […]
5. Sicurezza dell'acquisizione, dello sviluppo e della manutenzione […], compresa la gestione e la divulgazione delle vulnerabilità
6. Strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza
7. Pratiche di igiene informatica di base e formazione in materia di cybersicurezza
8. Politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura
9. Sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli assetti
10. Uso di soluzioni di autenticazione a più fattori o di autenticazione continua […]

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE
anci
Finanziato dall'Unione europea NextGenerationEU

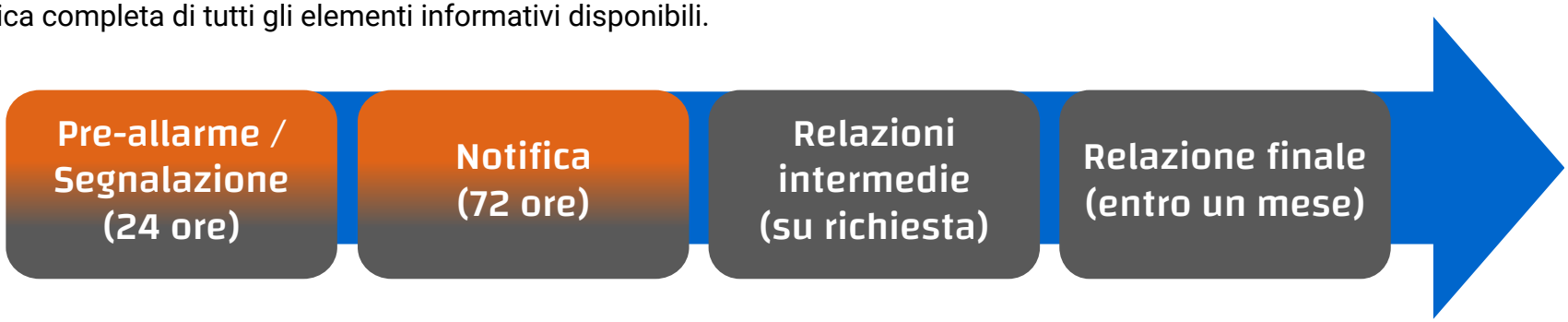
Obblighi di segnalazione

L90/2024 – Articolo 1

2. I soggetti […] segnalano, senza ritardo e comunque entro il termine massimo di ventiquattro ore […] qualunque incidente riconducibile a una delle tipologie individuate nella tassonomia di cui al comma 1 ed effettuano, entro settantadue ore […], la notifica completa di tutti gli elementi informativi disponibili.

D.LGS NIS – Articolo 25

5. Ai fini della notifica [di incidenti significativi] i soggetti interessati trasmettono al CSIRT Italia:
a) senza ingiustificato ritardo, e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo, una pre-notifica […];
b) senza ingiustificato ritardo, e comunque entro 72 ore da quando sono venuti a conoscenza dell'incidente significativo, una notifica dell'incidente […];



DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

Finanziato dall'Unione europea NextGenerationEU

Grazie

per la vostra attenzione

Il Sistema Anci a supporto della digitalizzazione dei Comuni