ACN Agenzia per la  
cybersicurezza  
nazionale

DIS Dipartimento  
informazioni per  
la sicurezza

AISI Agenzia  
informazioni e  
sicurezza interna  
AISE  
Agenzia

Introduzione sull’architettura di cybersicurezza  
nazionale e ACN  
• La legge n. 90/2024  
- soggetti rilevanti  
- gli adempimenti in capo ai soggetti rilevanti  
- le sanzioni in caso di inottemperanza  
- le modifiche alla normativa penalistica  
- le novità in materia di contratti pubblici in materia di beni  
e servizi informatici  
- preclusioni per il personale che abbia ricoperto ruoli  
specifici presso altre PP.AA

La Direttiva NIS 2 – 2022/2555

• 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)

Estensione ambiti di applicazione

• 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

Processo di identificazione dei soggetti

• 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)

Rafforzamento degli obblighi

• 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

Approccio al principio di

proporzionalità degli obblighi

Attività e Servizi

Altamente

critici Rilascio documenti /

autorizzazioni

Critici

Documentale

Servizi ancillari

Ordinari

Risorse umane

Intranet

Sistemi informativi e di rete

Altamente critici

Critici

Ordinari

Obblighi

ELEVATI

INTERMEDI

DI BASE

ESEMPIO SU 3 LIVELLI

Fasi del recepimento e

dell’attuazione

• Avvio informale di alcuni tavoli settoriali

• Adozione definitiva in CDM (7 agosto)

• Pubblicazione in Gazzetta Ufficiale (~fine settembre)

• Entrata in vigore (entro 17 ottobre)

Recepimento (febbraio 23 - metà ottobre 24)

• 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)

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

• 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

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

• Categorizzazione delle attività e dei servizi

• Implementazione degli obblighi a lungo termine

LEGGE 90

Pubbliche amministrazioni centrali

Regioni e Province autonome di Trento e

di Bolzano

Città metropolitane

Comuni con popolazione superiore a

100.000 ab.

Comuni capoluoghi di regione

TPL urbano con utenza ≥ 100.000 ab. e extra

urbano operanti nelle città metropolitane

ASL

Società in house (informatica, trasporto pubblico,

acque reflue, rifiuti)

DECRETO NIS

Pubbliche amministrazioni centrali

Regioni e Province autonome di Trento e di Bolzano

Città metropolitane

Comuni con popolazione superiore a 100.000 ab.

Comuni capoluoghi di regione

Società di trasporto pubblico ritenute critiche dall’Autorità di

settore (MIT)

ASL

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.

Impianto documentale (1)

Impianto documentale: insieme dei documenti necessari ai fini dell’attuazione delle misure

di sicurezza e dell’attestazione dell’effettiva implementazione delle stesse

• Per ciascuna misura le linee guida indicano i contenuti minimi che il relativo impianto

documentale deve trattare

• In base al proprio contesto, ciascun soggetto può decidere come organizzare il proprio

impianto documentale, ad esempio raggruppando i contenuti in un unico documento o

distribuendoli tra più documenti

• L’impianto documentale può essere reso disponibile in formato cartaceo o digitale,

purché facilmente fruibile da chi ha la necessità di conoscerlo e consultarlo

Il soggetto deve segnalare e notificare

qualunque incidente:

• avente impatto su reti, sistemi informativi e

servizi informatici;

• riconducibile a una delle tipologie individuate

nella tassonomia (c.d. ICP-C) di cui all’art. 1,

comma 3-bis, del decreto legge 21 settembre

2019 n.105, convertito con modificazioni dalla

legge 18 novembre 2019, n.133.

Obblighi e facoltà – art. 14,

comma 2, della Legge 90/2024

Criterio Offerta Economicamente più vantaggiosa (O.E.P.V)

FACOLTÀ

a) le S.A. (stazioni appaltanti),

comprese le centrali di committenza,

possono decidere di non aggiudicare

l’appalto all’offerente che ha presentato

l’O.E.P.V. se hanno accertato che la

stessa non tiene in considerazione gli

elementi essenziali di cybersicurezza

individuati con D.P.C.M. (Decreto del

Presidente del consiglio dei ministri)

OBBLIGHI

b) le S.A. (stazioni appaltanti),

comprese le centrali di committenza,

tengono in considerazione gli elementi

di cyberbersicurezza nella valutazione

dell’elemento qualitativo per

l’aggiudicazione;

d) Punteggio economico: 10

Punteggio tecnico: 90

Cosa prevede la normativa:

• lett. e) prevedere – nei casi individuati nel futuro Decreto del Presidente del

Consiglio dei Ministri – criteri di premialità per le proposte o le offerte che

contemplino l’uso di tecnologie di cybersicurezza italiane o di Paesi

appartenenti all’Unione europea o di Paesi aderenti all’Alleanza atlantica (NATO)

o di Paesi terzi tra quelli che hanno accordi di collaborazione con l’Unione

europea o con la NATO in materia di cybersicurezza, protezione delle

informazioni classificate, ricerca e innovazione. Ciò, al fine di tutelare la

sicurezza nazionale e di conseguire l’autonomia tecnologica e strategica

dell’Italia nell’ambito della cybersicurezza.