



NIS2 KIT



LA DIRETTIVA EUROPEA CHE MIRA A RAFFORZARE LA SICUREZZA INFORMATICA

NIS2 (Network and Information Security Directive) è la direttiva europea che ha lo scopo di rafforzare i requisiti di sicurezza informatica di istituzioni, enti pubblici e imprese a fronte dei sempre più crescenti attacchi informatici.

L'obiettivo è la protezione di dati, infrastrutture e patrimonio economico e garantire la continuità in caso di attacchi (obbligo comunicazione e creazione sovrastruttura nazionale e internazionale - CSIRT).



GENNAIO 2023

Entrata in vigore



**17 E 18 OTTOBRE
2024**

Termine ultimo recepimento
disposizioni e applicazione delle
stesse



**28 FEBBRAIO 2025
E 10 MARZO 2025**

Registrazione sulla piattaforma
ACN



**ENTRO FINE
MARZO 2025**

Redazione degli elenchi dei
soggetti essenziali e importanti
da parte di ACN.



**ENTRO META'
APRILE 2025**

Notifica dell'inserimento dei
soggetti coinvolti e pubblicazione
obblighi di base da parte di ACN.



**DAL 1° GENNAIO
2026**

Obbligo di comunicazione
annuale delle attività.

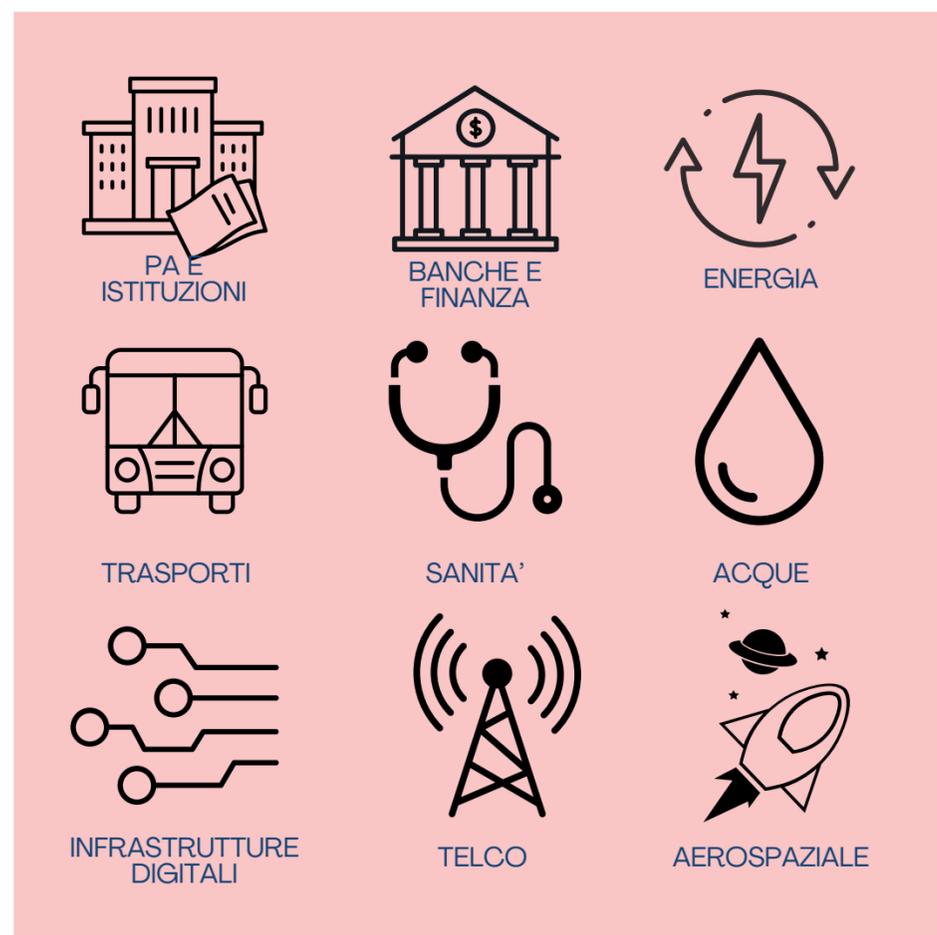
Rispetto alla precedente normativa (NIS1), la NIS2:

- **Identifica le organizzazioni** che hanno un obbligo primario nella messa in opera di misure atte a ridurre i rischi informatici;
- **Stabilisce sanzioni** in caso di mancato adeguamento;
- Impone **obblighi di implementazione, organizzazione e divulgazione** dei principi e comportamenti che possano preservare la sicurezza dell'organizzazione stessa;
- Indica le misure e i riferimenti per la **comunicazione obbligatoria e modalità di gestione degli incidenti.**





ESSENZIALI



PA E ISTITUZIONI

BANCHE E FINANZA

ENERGIA

TRASPORTI

SANITA'

ACQUE

INFRASTRUTTURE DIGITALI

TELCO

AEROSPAZIALE



CRITICI



SERVIZI POSTALI E CORRIERI

RIFIUTI

SOSTANZE CHIMICHE

ALIMENTARI

RICERCA

PRODUZIONE

SERVIZI DIGITALI

Gli **OBBLIGHI** e le **SANZIONI** sono commisurate a **dimensione** aziendale e **criticità** del soggetto, **ma non escludono alcuna impresa**.

Difatti anche le imprese che collaborano con soggetti a cui è diretta la normativa sono coinvolte indipendentemente dalla propria dimensione.

Le modalità di **CONTROLLO** potranno essere di differente natura, tra cui:

- a) **ispezioni** in loco e vigilanza a distanza, compresi controlli casuali, effettuati da professionisti formati;
- b) **audit** sulla sicurezza periodici e mirati effettuati da un organismo indipendente o da un'autorità competente;
- d) **scansioni** di sicurezza basate su criteri di valutazione dei rischi obiettivi;
- e) **richieste di informazioni** necessarie a valutare le misure di gestione dei rischi di cibersecurity adottate dal soggetto interessato;
- g) **richieste di dati** che dimostrino l'attuazione di politiche di cibersecurity.

Le **SANZIONI** previste sono fino a **10.000.000 €** per le inadempienze più gravi, oltre a **possibili interruzioni temporanee dell'attività e conseguenze sugli organi societari.**



NIS: AZIONI INDICATE PER LA GESTIONE DEI RISCHI

1 POLITICHE DI ANALISI DEI RISCHI

Procedure atte a misurare l'impatto dei rischi sull'organizzazione

2 CONTINUITA' OPERATIVA

Adozione di misure tecniche che consentano il ripristino delle informazioni e dei processi (es: backup in cloud).

3 GESTIONE DEGLI INCIDENTI

Obbligo di opportuna gestione degli incidenti, di segnalazione tempestiva e di reportistica.

4 ACQUISTO

Approvvigionamento di soluzione tecniche informatiche certificate da fornitori compilano.

5 FORMAZIONE

Formazione ai dipendenti e collaboratori per prevenire eventuali comportamenti cagionevoli e per una reazione efficace agli incidenti.

6 CIFRATURA

Politiche e procedure relative all'uso della crittografica e della cifratura dei dati.

7 CATENA DI APPROVVIGIONAMENTO

Obbligo di garanzia nei confronti dei fornitori della supply chain, affinché garantiscano misure adeguate.

8 EFFICACIA

Strategie e procedure per il controllo periodico.

9 ALTRE MISURE ORGANIZZATIVE

Controllo degli accessi in azienda, sicurezza dei dati relativi alle risorse umane etc..

10 ALTRE MISURE TECNICHE

Autenticazione a più fattori, protezione delle comunicazioni vocali, video e testuali etc....

I punti elencati sono i requisiti richiesti e sui quali le imprese oggetto della normativa possono essere misurate e controllate dagli organi preposti.



IL GRUPPO ANTELMA



NATI PER CONNETTERE LE IMPRESE AL FUTURO

Antelma è ICT e System Integrator: è partner delle imprese per l'evoluzione dei processi tecnologici da più di 35 anni e accompagna le imprese a connettersi e a sviluppare il proprio business attraverso **soluzioni IT & TLC performanti**.

La **nostra mission** è quella di ascoltare le esigenze e gli obiettivi delle imprese, supportandole e affiancandole nella trasformazione digitale.

Studiamo, attraverso il nostro know-how tecnico, **soluzioni che integrino hardware, software e connettività** che permettano:



Efficienza Operativa

Supportiamo l'efficienza operativa delle imprese, attraverso soluzioni ICT e di Connettività performanti e customizzate.



Business Continuity

Sosteniamo la Business Continuity, progettando soluzioni IT e TLC complete per garantire la continuità operativa in qualsiasi scenario.



Sicurezza Operativa

Forniamo soluzioni per proteggere la rete, i Device e i dati aziendali contro minacce esterne, mantenendo il business sempre sicuro.



Assistenza Continua

Sempre al fianco delle imprese attraverso la nostra consulenza e assistenza tecnica continua, da remoto e on-site, integrandoci con le diverse skills e seniority.



> 35
ANNI DI
ESPERIENZA

3
SOCIETA'
DEL GRUPPO

+ 2.000
AZIENDE CLIENTI

> 60
COLLABORATORI

PARTNER & CERTIFICAZIONI

**Partner
Connettività**



**Partner
Tecnici**



**Partner
Device**



**Partner HW,
SW e Security**



AUTORIZZAZIONE MINISTERIALE PER FORNITURA SERVIZI LEGATE ALLE TELECOMUNICAZIONI



AUTORITÀ PER LE
GARANZIE NELLE
COMUNICAZIONI

CERTIFICATO D'ECCELLENZA CRIBIS

ANTELMA E' PARTNER CERTIFICATO:





RETI E CONNETTIVITA'

Connettività' di alta qualità e **progettazione di reti aziendali**, garantendo efficienza, sicurezza e supporto tecnico continuo.



VOICE & COLLABORATION

Le soluzioni di Voice & Collaboration offrono alle imprese soluzioni avanzate per **comunicazioni vocali e strumenti collaborativi**, migliorando l'efficienza e la produttività.



SECURITY & BUSINESS CONTINUITY

Soluzioni per la **gestione della sicurezza informatica e continuità operativa**, con il fine di preservare il patrimonio aziendale.



ASSISTENZA IT & TLC

Assistenza Tecnica in ambito It e Tlc, da remoto e on-site per garantire la miglior continuità aziendale.



WORKSTATION, DEVICE & CARING

I **migliori device**, personalizzazione dell'offerta e assistenza continua per massimizzare la produttività.



WEB & MARKETING

Soluzioni customizzate per la presenza online e **strategie di marketing** digitale, per aumentare visibilità e crescita del business.



La presente presentazione ha scopo puramente informativo e non costituisce un'offerta vincolante, una consulenza tecnica o legale, né un impegno contrattuale.

Le informazioni contenute sono fornite in buona fede e possono essere soggette a modifiche senza preavviso.

