dracmaservice
software house and web solutions

2024 NIS 2 COMPLIANCE

LINEE GUIDA ALL'ADEGUAMENTO

PROPOSED BY :
Dracma Service s.r.l.

dracmaservice
software house and web solutions

DIRETTIVA NIS 2
CENNI GENERALI

La pubblicazione in **Gazzetta Ufficiale del D.lgs. 138 del 2024 di recepimento della NIS 2** ha definitivamente chiarito gli adempimenti in carico alle organizzazioni.

Il 17 ottobre 2024 entra in vigore la **Direttiva Europea NIS2** con lo scopo di rafforzare il livello di sicurezza in tutti gli Stati membri, tra cui l'Italia la quale stabilirà all'interno del suo ordinamento le modalità di adeguamento per i soggetti coinvolti.

La Direttiva NIS2 rappresenta **un'evoluzione della precedente NIS1**, con un'implementazione più estesa e complessa.

Il suo obiettivo principale, in risposta ai conflitti globali in atto e alla crescente sofisticazione delle minacce informatiche, è tutelare le **organizzazioni essenziali**, così come il **contesto sociale** ed **economico europeo**, dai rischi legati alla sicurezza informatica.

Rispetto alla **NIS** (la Direttiva 2016/1148 precedentemente in vigore, recepita in Italia dal D.lgs. 65 del 2018 e ora abrogata dai nuovi dispositivi) la **NIS 2**:

- **E' applicabile a più soggetti**;
- **Richiede un'analisi dei rischi**;
- **Richiede che le misure di sicurezza siano adeguate al contesto, considerando quindi anche la capacità di spesa**.

Nell'articolo si fa riferimento ad **ACN come l'autorità italiana per la NIS 2**, come previsto dall'Articolo 10.

dracmaservice
software house and web solutions

DIRETTIVA NIS 2
CENNI GENERALI

Di conseguenza, i settori coinvolti vengono ampliati e aumentano anche i controlli e gli obblighi per garantire la conformità.

Le principali novità rispetto alle versioni precedenti includono:

- Gli **amministratori aziendali vengono considerati direttamente responsabili** delle violazioni e devono ricevere una formazione adeguata.

- La **sicurezza della catena di fornitura diventa obbligatoria**, coinvolgendo tutte le aziende che forniscono servizi o prodotti alle organizzazioni critiche, inclusi i fornitori esterni all'UE.

- **Obbligo di notificare** tempestivamente gli attacchi informatici.

- Necessità di adottare misure tecniche, operative e organizzative idonee per **assicurare un determinato livello di sicurezza**.

- Le **sanzioni in caso di mancata conformità** sono stabilite in: fino a 10 milioni di euro o il 2% del fatturato annuo globale per gli enti essenziali, e fino a 7 milioni di euro o l'1,4% del fatturato annuo globale per le entità importanti.

dracmaservice
software house and web solutions

DIRETTIVA NIS 2

LE MISURE DI SICUREZZA

Il D.lgs. 138 identifica le misure di gestione del rischio , ossia:

- **Politiche di analisi dei rischi e di sicurezza** dei sistemi informativi e di rete;
- **Gestione degli incidenti**, ivi incluse le procedure e gli strumenti per eseguire le notifiche di cui agli articoli 25 e 26;
- **Continuità operativa**, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove applicabile, e gestione delle crisi;
- **Sicurezza** dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità;
- Politiche e procedure per **valutare l'efficacia delle misure di gestione dei rischi** per la sicurezza informatica;
- **Pratiche di igiene di base e di formazione in materia di sicurezza informatica** (notare che **l'articolo 23**, correttamente, impone agli organi di amministrazione e gli organi direttivi dei soggetti NIS 2 una formazione in materia di sicurezza informatica);
- **Politiche e procedure relative all'uso della crittografia** e, ove opportuno, della **cifratura** (notare che non è chiara la differenza tra crittografia (cryptography) e cifratura (encryption), presente peraltro anche nella Direttiva);
- **Uso di soluzioni di autenticazione a più fattori** o di **autenticazione continua**, di comunicazioni vocali, video e testuali protette, e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, ove opportuno.

dracmaservice
software house and web solutions

DIRETTIVA NIS 2
CATENA DI APPROVVIGIONAMENTO

La NIS 2 descrive più approfonditamente le necessità di controllo della **catena di approvvigionamento**:

"*i soggetti tengono conto delle vulnerabilità specifiche per ogni diretto fornitore e fornitore di servizi e della qualità complessiva dei prodotti e delle pratiche di sicurezza informatica dei propri fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro. Per la medesima finalità i soggetti tengono altresì conto dei risultati delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche effettuate dal Gruppo di cooperazione NIS*"

Per questo sarà sicuramente necessario **migliorare le pratiche di selezione, valutazione e rivalutazione dei fornitori e delle forniture**.

dracmaservice
software house and web solutions

DIRETTIVA NIS 2
SOCIETA' COINVOLTE

La tua organizzazione è soggetta alla nuova normativa NIS2 ?

Verifica se rientri in uno dei **18 settori critici** identificati dalla direttiva, di cui **11 sono considerati essenziali e 7 importanti**.

Sono coinvolte tutte le aziende che impiegano almeno 50 dipendenti, con un fatturato annuo o un bilancio totale superiore ai 10 milioni di euro, e che appartengono a uno dei seguenti settori critici:

Settori ad alta criticità

Trasporti	Sanità
Settore bancario	Energia
Acqua potabile	Acque reflue
Infrastrutture del mercato finanziario	
Spazio	Infrastrutture digitali
Pubblica amministrazione	
Gestione dei servizi TIC B2B	

Altri settori critici

Gestione dei rifiuti
Filiera alimentare
Filiera delle sostanze chimiche
Ricerca
Fabbricazione di particolari prodotti
Servizi postali e di corriere
Fornitori di servizi digitali

Anche i fornitori di essi sono inclusi. Una delle principali novità introdotte rispetto alla versione precedente riguarda la sicurezza della catena di fornitura. Pertanto anche chiunque fornisca loro beni o servizi è coinvolto indirettamente.

Via Achille Papa, 1/a 25128 Brescia - +39 030 51 050 59 - commerciale@dracmaservice.com

dracmaservice
software house and web solutions

DIRETTIVA NIS 2

GESTIONE DEGLI INCIDENTI

E' previsto **l'obbligo di notifica al CSIRT** e alle **autorità competenti** (oltre che ai destinatari stessi del servizio) degli **incidenti significativi** (incidenti informatici capaci di impattare in modo significativo sulla fornitura del servizio).

- **Entro 24 ore** dalla conoscenza dell'incidente con una notifica di preallarme (questo per attenuare la potenziale diffusione di incidenti e per consentire di chiedere assistenza);
  - deve riportare i dati strettamente necessari se l'incidente significativo è sospettato di essere il risultato di atti illegittimi o malevoli o se potrebbe avere (ossia se è probabile che abbia) un impatto transfrontaliero;
  - deve contenere una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione.

- **Entro 72 ore** dalla conoscenza dell'incidente con aggiornamenti rispetto alle informazioni fornite con il preallarme

- **Entro 1 mese** dalla conoscenza dell'incidente con una relazione finale a completamento del processo di segnalazione (questo per poter trarre insegnamenti preziosi dai singoli incidenti);
  - la relazione deve essere comprensiva della sua gravità e del suo impatto, il tipo di minaccia o la causa di fondo che ha probabilmente innescato l'incidente, le misure di mitigazione adottate e in corso e, se opportuno, l'impatto transfrontaliero dell'incidente.

- Se l'incidente **non è ancora risolto**, la normativa fornisce indicazioni su come procedere.

- Sono indicate eccezioni per i **prestatori di servizi fiduciari**, oltre che, all'articolo 33, per chi è compreso nel **PNSC**.

dracmaservice
software house and web solutions

DIRETTIVA NIS 2

SOLUZIONI DRACMA SERVICE

ANALISI TECNICA

VALUTAZIONE DELLO STATO ATTUALE DI SICUREZZA

SOLUZIONI E SERVIZI PER L'ADEGUAMENTO

COSTANTE GESTIONE E MONITORAGGIO

Via Achille Papa, 1/a 25128 Brescia - +39 030 51 050 59 - commerciale@dracmaservice.com

dracmaservice
software house and web solutions

DIRETTIVA NIS 2
LE SCADENZE

7 ottobre 2024: Gli Stati membri dovranno pubblicare e adottare entro questa data le misure necessarie per conformarsi alla nuova Direttiva europea.

18 ottobre 2024: Le misure adottate dagli Stati membri diverranno applicabili e verranno messe in atto dagli organi nazionali.

17 gennaio 2025: Prima revisione tra pari dell'Istituzione da parte del gruppo di cooperazione, composto dalla Commissione Europea, ENISA e CSIRT, per valutare la metodologia e gli aspetti organizzativi.

17 aprile 2025: Sarà definito l'elenco degli enti essenziali e importanti soggetti alla NIS2, con successiva revisione biennale.

17 ottobre 2027: Entro questa data, e successivamente ogni tre anni, la Commissione Europea effettuerà una revisione della Direttiva NIS2 e del suo funzionamento, con un report al Parlamento europeo.

Via Achille Papa, 1/a 25128 Brescia - +39 030 51 050 59 - commerciale@dracmaservice.com

NIS2
DIRECTIVE

Acronis nethesis syneto

Via Achille Papa, 1/a 25128 Brescia - +39 030 51 050 59 - commerciale@dracmaservice.com