In questa scheda:

NIS 2

Decreto Legislativo 4 settembre 2024 n. 138

Il primo ottobre 2024 è stato pubblicato nella Gazzetta Ufficiale il Decreto Legislativo 138 che recepisce la direttiva UE 2022/2555, nota come NIS 2. Il decreto affronta aspetti fondamentali della sicurezza informatica, dalle definizioni operative fino alle sanzioni in caso di inadempimento. Di seguito un estratto di alcuni aspetti normati e le soluzioni per l'adeguamento proposte da Gruppo L&T.

L&T

06 565 69307
info@gruppoLT.com
www.gruppoLT.com

Estensione degli Ambiti di applicazione

Il decreto si applica ai soggetti pubblici e privati identificati negli allegati I, II, III e IV. Gli allegati I e II specificano i settori considerati altamente critici e critici, inclusi i relativi sottosettori e tipologie di soggetti. Gli allegati III e IV descrivono le categorie di Pubbliche Amministrazioni e altre tipologie di soggetti a cui si applica il decreto.

Il decreto si applica ai soggetti delle tipologie indicate negli allegati I e II che superano i massimali previsti per le **piccole imprese** secondo l'articolo 2, paragrafo 2, dell'allegato alla raccomandazione 2003/361/CE. Semplificando, vengono definite piccole imprese quelle con meno di 50 dipendenti (unità lavorative-anno) e fatturato minore o uguale a 10.000.000 di euro (o totale di bilancio minore o uguale a 10.000.000 di euro), da valutare comunque caso per caso, ad esempio in presenza di collegamenti con altre imprese.

Ai fini del decreto, sono da considerarsi soggetti **essenziali e importanti** anche tutte le Società che esercitano un'influenza dominante o che possono, in altro modo, influire sulle decisioni relative alla gestione della sicurezza informatica di un soggetto essenziale o importante o che ne gestiscano a vario titolo i sistemi informatici.

Tra gli enti così identificati, la normativa prevede altresì una suddivisione tra soggetti essenziali ed importanti a seconda delle dimensioni e dei servizi erogati.

L'Allegato I individua i settori ad alta criticità

- Energia
- Trasporti
- Settore bancario
- Settore sanitario
- Acqua potabile
- Acque reflue
- Infrastrutture digitali
- Gestione dei servizi TIC
- Spazio.

L'Allegato II individua ulteriori settori critici

- Servizi postali e di corriere
- Gestione dei rifiuti
- Fabbricazione, produzione e distribuzione di sostanze chimiche
- Produzione, trasformazione e distribuzione di alimenti
- Fabbricazione
- Ricerca Fornitori di servizi digitali
- Ricerca

L'Allegato III individua le Pubbliche amministrazioni

- Amministrazioni centrali
- Amministrazioni regionali
- Amministrazioni locali particolari
- Altri soggetti pubblici

L'Allegato IV, infine, contiene ulteriori tipologie di soggetti quali

- Soggetti che forniscono servizi di trasporto pubblico locale
- Istituti di istruzione che svolgono attività di ricerca
- Soggetti che svolgono attività di interesse culturale
- Società in house, società partecipate e società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175

Adempimenti

Quali sono i reali termini degli obblighi discendenti dal decreto di recepimento della Direttiva NIS2?
E' opportuno sintetizzare i principali adempimenti derivanti dal decreto, ordinandoli per data. In particolare:

- **entro il 31 dicembre 2024**, aziende e pubbliche amministrazioni dovranno svolgere un assessment per comprendere se siano o meno soggette agli obblighi della Direttiva NIS2, seguendo il dettato degli artt. 6 e 7, degli Allegati I, II, III e IV, nonché di ogni altro atto che verrà emanato;

- **tra il 1° gennaio e il 28 febbraio 2025**, i soggetti privati e pubblici – che a seguito dell'assessment ritengano di rientrare nell'ambito di applicazione del decreto – dovranno registrarsi sulla piattaforma digitale resa disponibile da ACN fornendo le informazioni richieste dalla normativa;

- **entro il 17 gennaio 2025**, dovranno registrarsi sulla piattaforma i fornitori di servizi di sistema dei nomi di dominio, i gestori di registri dei nomi di dominio di primo livello, i fornitori di servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network;

- **entro il 31 marzo 2025**, l'ACN redigerà l'elenco dei soggetti essenziali e dei soggetti importanti sulla base delle registrazioni ricevute attraverso la piattaforma;

- **tra il 1° aprile 2025 e il 15 aprile 2025**, attraverso la piattaforma, l'ACN comunicherà ai soggetti registrati l'inserimento nell'elenco dei soggetti essenziali o importanti;

- **entro il 15 aprile 2025**, i soggetti che avranno ricevuto la comunicazione dovranno nominare con un apposito atto un soggetto che abbia la responsabilità dell'adempimento degli obblighi del decreto;

- **tra il 15 aprile e il 31 maggio 2025**, i soggetti che avranno ricevuto la comunicazione attraverso la piattaforma dovranno fornire le ulteriori informazioni richieste dalla normativa.

Chiusa questa fase preliminare, le aziende e le Pubbliche Amministrazioni che avranno ricevuto la comunicazione di inclusione da parte dell'ACN dovranno procedere con gli ulteriori adempimenti previsti nel decreto. A tal proposito, a titolo esemplificativo:

• **a partire dal 1° gennaio 2026**, si dovrà adempiere all'obbligo di notifica degli incidenti;
• **entro il 1° ottobre 2026**, si dovrà adempiere:
- agli obblighi degli organi di amministrazione e direttivi;
- agli obblighi in materia di misure di sicurezza;
- all'obbligo di raccolta e mantenimento di una banca dei dati di registrazione dei nomi di dominio, laddove applicabile.

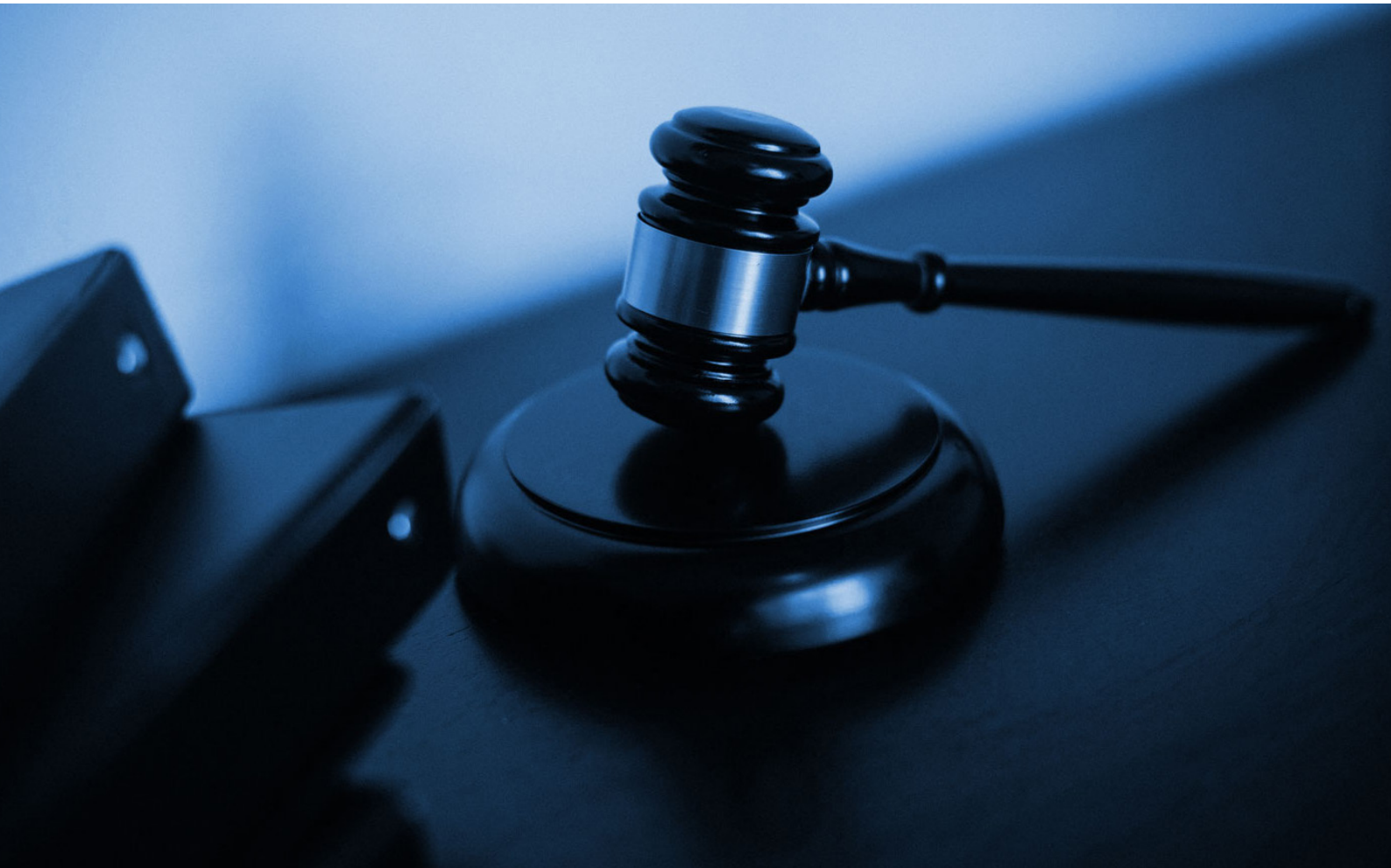
Sanzioni

Sanzioni differenziate in base al tipo di violazione e alla qualifica del soggetto.

Il trattamento sanzionatorio viene differenziato in base al tipo di violazione e alla qualifica del soggetto. In particolare, la violazione dei seguenti obblighi è sanzionata, in caso di soggetti essenziali, **fino a 10 milioni di euro o fino al 2%** del totale del fatturato annuo su scala mondiale per l'esercizio precedente del soggetto, o, in caso di soggetti importanti, **fino a 7 milioni o fino al 1,4% del totale del fatturato mondiale.**
È prevista una sanzione fino al 0,1% o fino allo 0,07% del fatturato mondiale annuo per le violazioni considerate meno gravi, la mancata collaborazione con l'ACN nello svolgimento dei suoi compiti e nell'esercizio dei suoi poteri.

Le sanzioni accessorie.

In aggiunta a quanto sopra, sono previste anche delle sanzioni che potremmo definire "accessorie" come la sospensione temporaneamente di un certificato o un'autorizzazione relativi ai servizi erogati dal soggetto. Inoltre, nella medesima ipotesi, le conseguenze possono ripercuotersi anche sul management, che non potrà svolgere funzioni dirigenziali nell'ente.



Adeguamento

Capo IV "Obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente"

- L'**articolo 23** stabilisce il ruolo degli **organi di amministrazione e direttivi.**

- L'**articolo 24** determina **gli obblighi in materia di misure di gestione dei rischi per la sicurezza informatica.**

  Il primo comma prevede che vengano adottate misure tecniche, operative e organizzative adeguate e proporzionate, alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché' per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi.

  Il secondo comma stabilisce che tali misure siano basate su un approccio multi-rischio, volto a proteggere i sistemi informativi e di rete nonché il loro ambiente fisico da incidenti, e comprendono almeno i seguenti elementi:

  a) *politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete;*
  b) *gestione degli incidenti, ivi incluse le procedure e gli strumenti per eseguire le notifiche di cui agli articoli 25 e 26;*
  c) *continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove applicabile, e gestione delle crisi;*
  d) *sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;*
  e) *sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità;*
  f) *politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica;*
  g) *pratiche di igiene di base e di formazione in materia di sicurezza informatica;*
  h) *politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura;*
  i) *sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli assett;*
  l) *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.*

  Il terzo comma specifica che nel valutare quali misure di cui al comma 2, lettera d), siano adeguate, 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.

  Il quarto comma stabilisce che, qualora un soggetto rilevi di non essere conforme alle misure di cui al comma 2, esso adotta, senza indebito ritardo, tutte le misure appropriate e proporzionate correttive necessarie.

- L'**articolo 25** sancisce **gli obblighi in materia di notifica di incidente.**

- L'**articolo 27** introduce **l'uso di schemi di certificazione della cybersicurezza.**

SOLUZIONI PROPOSTE DA GRUPPO L&T PER L'ADEGUAMENTO

Il panorama della cybersecurity in Italia sta subendo una profonda trasformazione, guidata da una serie di normative europee che innalzano significativamente gli standard di protezione dei dati e delle infrastrutture critiche. Tra queste, Il Regolamento Generale sulla Protezione dei Dati (GDPR), a livello europeo, e il Codice in materia di protezione dei dati personali a livello nazionale, impongono a tutte le organizzazioni di adottare misure tecniche e organizzative adeguate a garantire la sicurezza dei dati. Le sanzioni per le violazioni di questi regolamenti possono essere estremamente elevate e danneggiare gravemente la reputazione di un'organizzazione.

Oltre a ciò, le misure minime di sicurezza emanate da ACN, la Direttiva NIS2 (Network and Information Systems) e il Regolamento DORA (Digital Operational Resilience Act) rappresentano indicazioni importanti sull'importanza dell'adozione di misure adeguate in termini di sicurezza informatica.

Gruppo L&T propone un'ampia gamma di servizi e soluzioni finalizzate all'adozione di tali misure.

1. Analisi e gestione dei rischi

Piattaforma per l'analisi e la gestione dei rischi dell'organizzazione

2. Soluzione per gestione incidenti

Piattaforma per la gestione degli incidenti.

3. Piano di continuità operativa

Piattaforma per la gestione del piano di continuità operativa e piano di disaster recovery.

4. Servizio di Disaster Recovery

Servizio di DR che consente la produzione di copie di backup con adeguata frequenza, conservazione in Datacenter cloud ridondato con elevate garanzie di sicurezza (Tier 3) e test periodici di integrità delle copie di sicurezza. Regolarmente, vengono create copie di tutti i dati, archiviate in un luogo sicuro, datacenter cloud a sua volta coperto da sistema di replica in diverso datacenter. Viene verificato periodicamente che i backup vengano eseguiti correttamente e che sia possibile ripristinare i dati in caso di bisogno. In caso di disastro, le procedure per ripristinare i dati e riavviare le attività sono già definite e, ove possibile, automatizzate.

Un sistema di disaster recovery (DR) è essenziale per qualsiasi organizzazione che voglia proteggere i propri dati. In caso di calamità naturali, guasti hardware, attacchi informatici o qualsiasi altro evento in grado di compromettere le operazioni, il DR permette di ripristinare rapidamente sistemi e dati.

5. Servizio di protezione dalle minacce alla sicurezza informatica (SOC)

Servizio SOC, basato su applicativo di protezione dedicato e gestito da personale specializzato con servizio di risposta e intervento 24/7 in italiano e inglese. Personale qualificato, con l'ausilio di software dedicati, monitora costantemente lo stato della struttura informatica alla ricerca di potenziali minacce alla struttura informatica dell'organizzazione. Il personale dedicato può intervenire o allertare l'organizzazione per una risposta tempestiva a minacce ed anomalie. In caso di disastro, le procedure per ripristinare i dati e riavviare le attività sono già definite e, ove possibile, automatizzate.

La sicurezza informatica (o Cybersecurity) è fondamentale e mira a proteggere sistemi informatici, reti e dati da accessi non autorizzati, uso improprio, divulgazione e distruzione. In un mondo sempre più digitalizzato, dove le informazioni sono diventate una risorsa preziosa, la necessità di tutelare questi asset è divenuta cruciale.

6. Formazione in materia di sicurezza informatica (FAD Cybersecurity)

Servizio di formazione tramite piattaforma online automatizzata con videocorsi strutturati in microlezioni.
La formazione viene erogata tramite percorsi formativi strutturati suddivisi in lezioni e con quiz di verifica dell'acquisizione delle nozioni presentate e attestato di completamento finale.
Tramite una struttura a microlezioni è possibile seguire il piano formativo a diversi ritmi e l'accesso online permette di adeguare la fruizione dei contenuti in base alle necessità del personale dell'organizzazione. La piattaforma non necessita di complesse configurazioni e provvede a fornire promemoria automatici ai discenti e report sull'andamento dell'avanzamento dei percorsi formatici di ogni utente. I percorsi formativi forniscono anche esempi reali e soluzioni pratiche alle problematiche e dubbi più comuni, fornendo un approccio più pratico alla materia.

La formazione in materia di sicurezza informatica è un investimento a lungo termine per la protezione dei dati e delle risorse informatiche dell'organizzazione.

7. Servizio di Vulnerability Assessment Interno, Esterno e per Applicazioni Web

Servizi di vulnerability assessment per:

- reti interne (VA Interna)
- dispositivi pubblicati su internet (VA Esterna)
- applicazioni web (VA WebApp)

Tali servizi consentono di individuare le potenziali vulnerabilità note e configurazioni rischiose, che passano al vaglio di un team di analisti. Tutte le potenziali vulnerabilità individuate vengono classificate, con assegnazione di un indice di gravità. Per ogni vulnerabilità vengono fornite indicazioni sulla risoluzione o mitigazione. Tutte le informazioni vengono trasmesse all'organizzazione corredate da un report completo ed esaustivo.

Un vulnerability assessment (valutazione delle vulnerabilità) è un processo fondamentale per qualsiasi organizzazione che desideri proteggere i propri sistemi informatici e i dati sensibili. È come una radiografia per la sicurezza informatica: permette di individuare le potenziali debolezze e le falle presenti nei sistemi, prima che possano essere sfruttate da cybercriminali.

8. Servizio OSINT

Servizio di formazione tramite piattaforma online automatizzata con Il servizio OSINT identifica eventuali attacchi informatici passati, fughe di dati o altre attività dannose di cui l'organizzazione potrebbe essere stata vittima. Verifica se dati dell'organizzazione sono stati rubati e venduti sul dark web. Verifica se credenziali di accesso dell'organizzazione sono state rubate e venduti sul dark web. Verifica se esistono domini con nomenclature similari a quelli dell'organizzazione, che potrebbero essere stati creati con scopi ingannevoli. Viene prodotto un report finale con eventuali indicazioni su quali punti attenzionare maggiormente e quali potrebbero meritare ulteriori approfondimenti specifici.

L'OSINT è una disciplina dell'intelligence che si occupa di raccogliere e analizzare informazioni disponibili pubblicamente per ottenere una comprensione più profonda di un determinato argomento, persona, organizzazione o evento e, applicato alla sicurezza informatica, permette di raccogliere e analizzare informazioni disponibili pubblicamente per identificare potenziali minacce, vulnerabilità e rischi.

9. Sistema Asset Inventory

La soluzione di Asset Inventory consiste in un sistema di analisi della rete aziendale tramite sonda dedicata, disponibile sia hardware che software (virtual appliance). Il sistema rileva tutti i dispositivi connessi alla rete sia Hardware che Software. Permette inoltre di definire la frequenza delle analisi senza limiti o con programmazione per strutture molto ampie o complesse. La soluzione rileva le potenziali vulnerabilità note del parco software analizzato, fornendo indicazioni su possibili modalità di risoluzione.

L'inventario hardware e software è uno strumento essenziale per garantire la sicurezza, l'efficienza e la conformità della struttura informatica. È un'attività che richiede un impegno continuo, poiché l'ambiente IT è in costante evoluzione.

10. Autenticazione a due fattori

Soluzione di autenticazione a due fattori per i sistemi informativi.

11. Cifratura dei dati importanti

Soluzione per cifratura dei dati sensibili/importanti dell'organizzazione.

12. Politiche di controllo dell'accesso e gestione dei beni e degli asset

Soluzione per la gestione e monitoraggio degli asset dell'organizzazione.

13. Sicurezza della catena di approvvigionamento.

Piattaforma per la gestione della sicurezza nella catena di approvvigionamento.

Richiedi INFORMAZIONI

ENTRA IN CONTATTO CON LA NOSTRA REALTÀ

Richiedi subito una consulenza

06 565 69307

info@gruppoLT.com

Lazio

- Via della Conciliazione, 10
00193 Roma

Lombardia

- Via Achille Grandi, 8
25125 Brescia

- Viale Sabotino, 22
20135 Milano

Sicilia

- Piazza Paola Frassinetti, 1
95040 Mirabella Imbaccari (CT)