LA SICUREZZA DELLE INFORMAZIONI NELLE AZIENDE:

- **NORMATIVE**
- **ADEMPIMENTI OBBLIGATORI**
- **PROSSIME SCADENZE**

→ ERGON AMBIENTE E LAVORO SRL - 091 340837 - www.ergon.palermo.it

PREPARATI PER LA DIRETTIVA NIS2

L'attuale incertezza e la crescente minaccia degli **attacchi informatici** hanno motivato l'elaborazione di una **Direttiva europea** volta a standardizzare l'approccio alla gestione delle attività legate alla **Cybersecurity** in settori ritenuti critici e strategici.

Nel 2016, il Parlamento Europeo aveva introdotto la **Direttiva NIS – Network and Information Security**, con l'obiettivo di potenziare le difese dei Paesi membri contro potenziali **attacchi informatici**. Tale direttiva prevedeva una serie di misure legislative finalizzate a armonizzare l'implementazione e l'applicazione dei **sistemi di sicurezza** delle reti e dei sistemi informativi nei **paesi dell'Unione Europea**.

A fine dicembre 2022, la **Direttiva NIS2** è stata ufficialmente pubblicata sulla Gazzetta Ufficiale dell'UE, abrogando e sostituendo la precedente del 2016. Questo aggiornamento mira a modernizzare il quadro normativo europeo in materia di **Cybersecurity**, correggendo imprecisioni identificate nel tempo e ampliando il campo di applicazione della direttiva stessa.

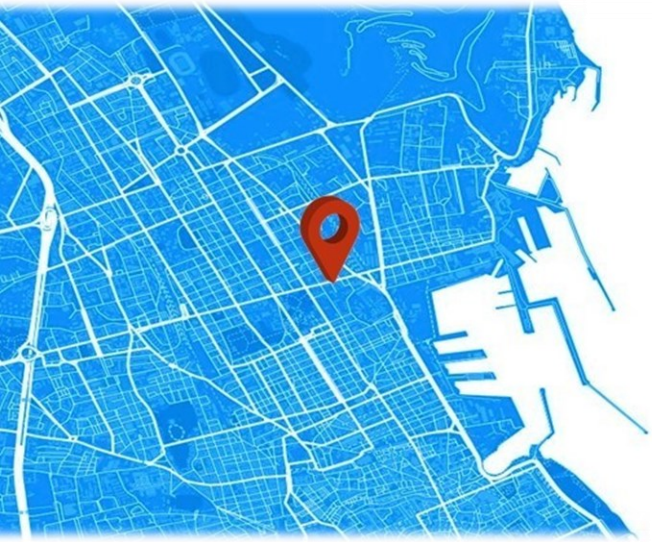
Con l'entrata in vigore, nel gennaio 2023, della Direttiva NIS2 - che i 27 Stati membri dell'Unione Europea devono recepire in una legge nazionale entro la fine del 2024 - le organizzazioni che forniscono servizi essenziali in UE dovranno affrontare un regolamento di cybersicurezza più severo che mai.

Da questo momento in avanti, le imprese saranno tenute a implementare una politica e una metodologia specifiche e dovranno valutare regolarmente la sicurezza delle informazioni. In altre parole, i requisiti imposti alle aziende dalla **NIS2** mirano a istituire, di fatto, un sistema di gestione della sicurezza informatica.

Perché creare un proprio sistema di gestione quando l'articolo 20 della Direttiva suggerisce di adottare gli standard esistenti?

Certificazioni come la **ISO/IEC 27001:2022**, intitolata "Sicurezza delle informazioni, cybersicurezza e protezione della privacy - Requisiti per i sistemi di gestione della sicurezza delle informazioni," e la **ISO 22301:2019**, denominata "Sicurezza e resilienza - Requisiti per i sistemi di gestione della continuità aziendale," già focalizzano gli aspetti affrontati dalla **Direttiva NIS2**, che le imprese nei **settori** interessati devono esaminare, mappare e gestire.

Ciò implica che **l'adozione di un sistema ISO/IEC 27001 e/o ISO 22301 efficace può fornire un supporto significativo** per le aziende che stanno affrontando l'adeguamento alla Direttiva. L'utilizzo di questi standard implica la conformità alla legislazione, compresa la NIS2. Pertanto, esistono tutte le motivazioni per iniziare. Se la **Direttiva NIS2** ha un impatto diretto sulla vostra attività, l'invito è a iniziare immediatamente l'implementazione di un sistema di gestione conforme alla ISO/IEC 27001 e/o alla ISO 22301. Evitare di affrontare le **scadenze** imminenti o già passate è sempre più oneroso, complicato e prolungato, e la scadenza per l'implementazione della **NIS2** si avvicina rapidamente.



Il team di Ergon è pronto ad assistervi nell'assicurare che siate preparati e tranquilli quando la normativa NIS2 entrerà in vigore.

→ ERGON AMBIENTE E LAVORO SRL - 091 340837 - www.ergon.palermo.it

DIRETTIVA NIS2
COSA SIGNIFICA PER TE E IL TUO BUSINESS?

La Direttiva NIS2 diventerà efficace in Italia entro la fine del 2024, introducendo requisiti più rigorosi e ampliando la sua portata rispetto alla versione originale del 2016, che è stata implementata nelle normative nazionali a partire dal 2018. Le imprese che non si conformano a tali requisiti rischiano sanzioni significative e persino la revoca della licenza.

La **NIS2** non solo estende la sua copertura a **nuovi settori** non contemplati dalla Direttiva precedente (Vedi Allegati), ma impone anche requisiti più dettagliati in materia di **sicurezza informatica** e gestione delle informazioni per le imprese di grandi e medie dimensioni. L'obiettivo principale è armonizzare e semplificare i livelli di sicurezza tra gli Stati membri. Inoltre, la NIS2 rafforza i requisiti per la valutazione del rischio informatico da parte delle importanti realtà nei settori interessati, includendo la gestione dei rischi legati alle catene di fornitura e alle relazioni con i fornitori.

Ergon stima che le organizzazioni dovranno iniziare ad adeguarsi alle leggi nazionali che recepiscono la **Direttiva NIS2** già **nella prima metà del 2024**. Il tempo è quindi limitato per affrontare la complessa sfida di valutazione dei rischi, gestione e formazione, specialmente per le medie e grandi organizzazioni coinvolte nell'ambito della NIS2.

La preparazione per la conformità richiederà molti mesi e sarà particolarmente complessa per le organizzazioni operanti in più Stati membri.

Molte aziende con attività industriali dovrebbero già aver avviato la pianificazione fin dall'inizio del 2023.

→ ERGON AMBIENTE E LAVORO SRL - 091 340837 - www.ergon.palermo.it

I SETTORI IMPATTATI DALLA DIRETTIVA NIS2

L'UE prevede che la Direttiva NIS2 coinvolgerà oltre 10.000 organizzazioni europee

Servizi essenziali e fornitori di servizi digitali

- Energia - elettricità, petrolio, gas naturale
- Approvvigionamento e distribuzione di acqua potabile Trasporti – aerei, ferroviari, marittimi, stradali
- Banche
- Infrastrutture del mercato finanziario
- Sanità - strutture sanitarie inclusi ospedali e cliniche private
- Infrastrutture Digitali – Internet Exchange Point (IXP), provider DNS, registri di nomi TLD
- Pubbliche amministrazioni individuate come operatori di servizi essenziali

Servizi importanti

- Servizi postali e corrieri
- Gestione dei rifiuti
- Sostanze chimiche – fabbricazione, produzione, distribuzione
- Cibo – produzione, trasformazione, distribuzione
- Fabbricazione di dispositivi medici (possono essere ridefiniti come servizi essenziali durante un'emergenza di salute pubblica)
- Fabbricazione di computer, prodotti elettronici e ottici, apparecchiature elettriche, macchinari e attrezzature, veicoli a motore e altri mezzi di trasporto
- Fornitori digitali: marketplace online, motori di ricerca online e piattaforme per servizi di social network

Servizi essenziali

- Energia – elettricità, teleriscaldamento e teleraffrescamento, petrolio, gas naturale, idrogeno
- Produzione di prodotti farmaceutici, compresi i vaccini
- Acqua potabile e acque reflue
- Trasporti – aerei, ferroviari, marittimi, stradali
- Banche (ad eccezione delle banche centrali)
- Infrastrutture del mercato finanziario
- Sanità
- Infrastruttura digitale – Internet Exchange Point (IXP), provider DNS, registri di nomi TLD, fornitori di servizi di cloud computing, fornitori di servizi di data center, reti di consegna di contenuti, fornitori di servizi fiduciari, reti di comunicazione elettronica pubbliche, servizi di comunicazione elettronici
- Gestione dei servizi ICT (business- to-business)
- Industria spaziale
- Amministrazioni pubbliche centrali e regionali o, a scelta degli Stati membri possono, regolamentazione delle autorità nazionali di sicurezza informatica

DOMANDE SULLA DIRETTIVA NIS2

Per quale motivo sono stati ampliati i requisiti della NIS2 in questo momento?
L'espansione del campo di applicazione delle norme **NIS2** mira a contribuire a elevare nel tempo il livello di sicurezza informatica in Europa. La sicurezza delle informazioni riveste un'importanza cruciale per tutte le imprese e rappresenta un elemento essenziale per la maggior parte di esse. Di conseguenza, l'obiettivo della NIS2 è anche quello di inviare un messaggio inequivocabile a coloro che non rientrano attualmente nei requisiti, indicando che devono affrontare la questione della sicurezza informatica con maggiore serietà rispetto al passato. Questa è una delle ragioni per cui le aziende sono obbligate a esaminare le vulnerabilità presenti nella loro catena di approvvigionamento.

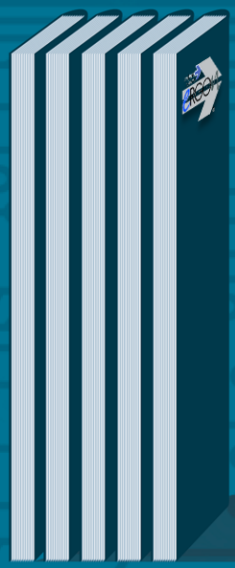
Entro quale periodo le organizzazioni devono adempiere ai recenti requisiti della NIS2?
La **Direttiva** è stata adottata nel **gennaio 2023** e diventerà operativa **dopo 21 mesi**, momento a partire dal quale le imprese rischiano **sanzioni finanziarie**. Ciò implica che le organizzazioni coinvolte devono essere pronte a conformarsi ai nuovi requisiti **entro la fine del 2024**. Le imprese che non si adeguano **ai requisiti della NIS2** possono essere soggette a **multe fino a 10 milioni di euro**. Considerando l'esperienza con l'entrata in vigore dei requisiti del GDPR, molte organizzazioni si sono ritrovate impreparate, arrivando troppo tardi e affrontando una carenza di risorse che ha reso proibitivo il costo dell'adeguamento nell'ultimo anno prima della scadenza.

DOMANDE SULLA DIRETTIVA NIS2

Quali sono gli aggiornamenti richiesti?
I nuovi criteri della **NIS2** comprendono l'integrazione della gestione del rischio nel processo gestionale, l'adozione di misure organizzative e tecniche, e la segnalazione pronta e condivisa degli incidenti di cybersicurezza. Con la NIS2, la **responsabilità** della conformità viene attribuita direttamente al **management**.

Come è possibile impiegare standard come la ISO/IEC 27001 o la ISO 22301 per soddisfare i requisiti della NIS2?
È del tutto logico seguire le linee guida dei sistemi di gestione per la sicurezza delle informazioni o per la **business continuity**, poiché la stessa **NIS2** incoraggia l'adozione di standard già esistenti. Non c'è alcuna necessità di creare un sistema di gestione "da zero" quando esiste un **quadro di riferimento** già adottato da numerose altre imprese, e che può anche essere certificato per attestare la **conformità ai requisiti**. Se si lavora conformemente alla **ISO/IEC 27001** e/o alla **ISO 22301**, ci si adatta alla normativa risultando **conformi alla legislazione**. Inoltre, se si dispone già di un altro sistema di gestione, come ad esempio la ISO 9001, si è già avanti nel percorso. Pertanto, ciò ha perfettamente senso.

È fattibile mettere a confronto i requisiti della NIS2 con quelli di un sistema di gestione?
Certamente! La presenza di una politica di sicurezza delle informazioni, insieme a valutazioni dei rischi e delle prestazioni, rappresentano elementi fondamentali di un sistema di gestione. In sostanza, quanto attualmente richiesto può essere considerato un sistema di gestione de facto. Ciò che la NIS2 richiede alle aziende è in linea con un sistema di gestione.



PREPARATI ALLA DIRETTIVA NIS2 CON ERGON

Se siete soggetti alla **Direttiva NIS2**, vi consigliamo di iniziare tempestivamente l'implementazione dei nuovi requisiti normativi. Ergon, con la sua specifica esperienza nella sicurezza delle informazioni e nella continuità aziendale, è accreditata per verificare la conformità agli standard indicati.

Ricevete supporto e competenza nella certificazione

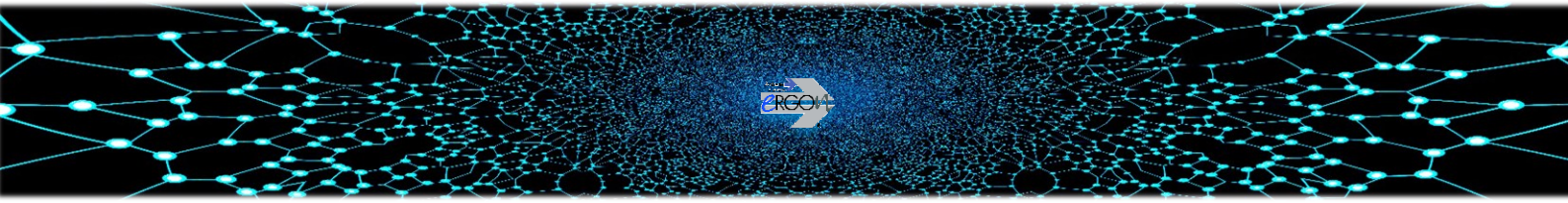
L'utilizzo di standard di gestione può risultare confusionario per chi non vi ha mai lavorato in precedenza. Al contempo, è essenziale comprendere cosa apporti valore all'azienda. In prospettiva, la sicurezza delle informazioni e la continuità aziendale non saranno più ostacoli per l'attività, ma diventeranno un catalizzatore per lo sviluppo aziendale.
Ergon può guidarvi nella realizzazione e nell'adozione di un sistema di gestione adatto alla vostra organizzazione, favorendo il vostro business.

Formazione su Sicurezza delle Informazioni e Business Continuity

Il progresso continuo di un'organizzazione è facilitato dall'implementazione di un sistema di gestione per la sicurezza delle informazioni, in grado di identificare i potenziali rischi legati alla sicurezza delle informazioni e di proteggere gli asset aziendali correlati. La **norma ISO/IEC 27001** sovrintende a un'implementazione efficace di tale sistema di gestione. Ogni interruzione dei servizi erogati può causare danni gravi e perdite di profitto, e qui entra in gioco la **Business Continuity**, descritta nei requisiti della ISO 22301. Questa viene definita come il processo di individuazione delle potenziali minacce per un'azienda e di avvio delle strategie e operazioni necessarie per garantire la resilienza della struttura in caso di situazioni avverse. Attraverso il **programma di formazione offerto da Ergon**, aumentate il vostro valore sul mercato in quanto avete la possibilità di evidenziare la vostra competenza nel generare e comprovare risultati mediante il vostro sistema di gestione della sicurezza delle informazioni.

GAP Analysis & Resolution

L'effettuazione di analisi delle lacune e del grado di conformità per ottenere una panoramica della vostra posizione in relazione ai nuovi requisiti. Durante questa valutazione, esaminiamo la vostra organizzazione e determiniamo se rientrerete **nell'ambito di applicazione della Direttiva**, identificando eventuali non conformità rispetto ai suoi requisiti e supportandovi nella previsione e nell'adozione delle idonee contromisure tecnologico-organizzative.



TI AIUTIAMO SULLA CONFORMITÀ ALLA DIRETTIVA NIS2

Con **oltre 1.000 aziende seguite** nei settori della Sicurezza, **Ergon Ambiente e Lavoro** è da anni il **partner** di consulenza preferito da molte organizzazioni, piccole-medie-grandi imprese.
La presenza locale di Ergon, l'**esperienza nazionale** e la riconosciuta competenza professionale **in tutti i settori che impattano sulla sicurezza a 360°** contribuiscono a creare un buon rapporto di lavoro con i nostri clienti. Collaboriamo con i nostri clienti per aiutarli a creare **valore** e a soddisfare le **esigenze** e le sfide economiche, sociali e ambientali, indipendentemente dall'industria, dal settore o dalle dimensioni dell'organizzazione.
Attraverso i **nostri servizi** di consulenza, verifica, valutazione e formazione, rafforziamo le organizzazioni, i prodotti, le persone, le strutture e le catene di fornitura dei nostri clienti.

→ ERGON AMBIENTE E LAVORO SRL - 091 340837 - www.ergon.palermo.it