

White Paper

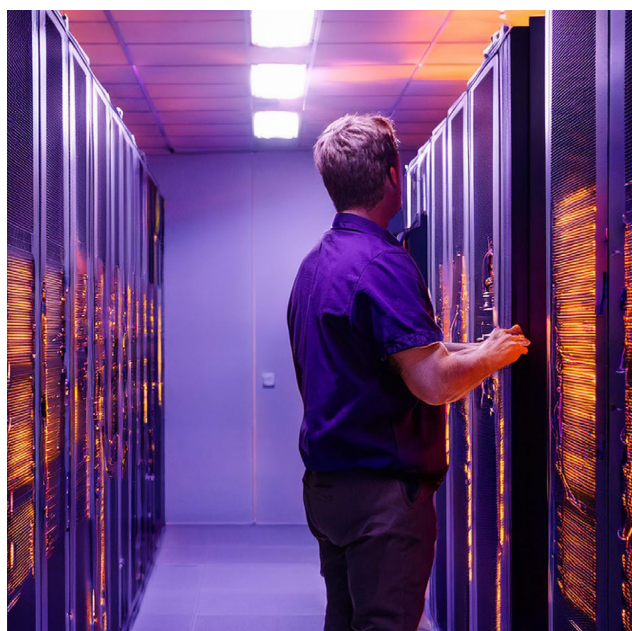
# Nuova direttiva NIS2

## Dati essenziali e conformità

## Introduzione a NIS2

Con l'aumento della frequenza delle minacce digitali e l'evoluzione della sofisticatezza degli aggressori informatici, governi e agenzie internazionali stanno proponendo normative nuove e aggiornate per aumentare la resilienza. Quando viene introdotta una nuova normativa, può essere difficile apprenderla, analizzarla e implementarla prima della data di entrata in vigore.

Se lavori nel settore informatico nell'Unione europea (UE), saprai già che nel tuo futuro dovrai scoprire i dettagli della Direttiva sulla sicurezza delle reti e dell'informazione 2 (NIS2). Abbiamo pensato che potrebbe essere utile fornirti una rapida introduzione a NIS2 per dare il via al tuo percorso di implementazione, in modo da restare al passo con le normative e, soprattutto, un passo avanti agli aggressori.



# Cos'è NIS2?

La direttiva sulla sicurezza delle reti e dell'informazione 2 (NIS2) mira a rafforzare la sicurezza informatica negli Stati membri dell'UE e in tutte le entità che intrattengono rapporti commerciali con essi. Risponde alle crescenti minacce legate alla digitalizzazione e all'aumento degli attacchi informatici.

NIS2 amplia il campo di applicazione della direttiva NIS originaria con più settori e tipologie di entità che rientrano nella sua giurisdizione, compresi quelli ritenuti aventi un ruolo "essenziale" e "importante" nel mercato interno dell'UE. Introduce requisiti più significativi, tra cui la segnalazione completa degli incidenti, pratiche di gestione del rischio, misure di responsabilità aziendale e strategie di continuità aziendale.

## Rischi di non conformità

La direttiva NIS2 prevede sanzioni sostanziali in caso di non conformità, nonché la possibilità di avviare contenziosi. NIS2 impone agli Stati membri di recepire tali requisiti nella legislazione nazionale entro il 17 ottobre 2024. Anche se l'implementazione potrebbe variare leggermente, è essenziale una preparazione approfondita per tale scadenza.

È necessario comprendere proattivamente la direttiva, identificare gli impatti sulla propria organizzazione e stabilire un piano per raggiungere la conformità.

A questo punto, probabilmente ti starai chiedendo: "Qual è l'impatto su di me?", ma prima devi capire chi sei "tu" e se NIS2 ha un impatto sulla tua organizzazione.

# Sono essenziale o importante?

NIS2 classifica le organizzazioni aziendali in due gruppi: "essenziali" e "importanti". La tua posizione in questo gruppo ti aiuterà a capire in che modo NIS2 avrà un impatto futuro sulla tua organizzazione.

## Entità essenziali

NIS2 individua settori cruciali quali i trasporti, i servizi finanziari, l'assistenza sanitaria e le aziende di servizi pubblici (inclusi i fornitori di energia) come "entità essenziali", sottolineandone l'importanza per il benessere sociale ed economico. Rafforza gli obblighi di conformità, in particolare imponendo la segnalazione degli incidenti entro 24 ore, il che rappresenta un inasprimento significativo dei requisiti previsti dalla direttiva precedente. Inoltre, prevede pesanti sanzioni e gravi conseguenze in caso di non conformità, sottolineando la posta in gioco più elevata e il quadro normativo più severo che queste entità devono ora affrontare.

Sei un'entità essenziale se la tua azienda ha più di 250 dipendenti e un fatturato annuo di 50 milioni di euro e rientra in una di queste categorie:

- Infrastruttura digitale
- Energia
- Finanza
- Salute
- Pubblica amministrazione
- Spazio
- Trasporto
- Approvvigionamento idrico (potabile e acque reflue)

## Entità importanti

NIS2 introduce una nuova classificazione per le entità "importanti", ampliando per la prima volta l'ambito di applicazione della direttiva per comprendere settori quali i servizi postali, la gestione dei rifiuti e la produzione manifatturiera. Questa espansione implica che questi settori debbano valutare e migliorare rapidamente le proprie misure di sicurezza informatica per conformarsi allo standard NIS2. Sebbene le entità "importanti" siano soggette a obblighi e sanzioni meno severi in caso di non conformità rispetto alle loro controparti "essenziali", non bisogna sottovalutare la sfida di soddisfare tali requisiti in tempi relativamente brevi.

Sei un'entità "importante" se la tua azienda ha più di 50 dipendenti e un fatturato annuo di 10 milioni di euro e rientra in una di queste categorie (ciò include anche le categorie elencate come essenziali):

- Prodotti chimici
- Alimenti
- Produzione
- Servizi postali
- Ricerca
- Gestione dei rifiuti

## Impatto di NIS2

Se la tua attività rientra nelle categorie "essenziali" o "importanti" elencate, il passo successivo è capire cosa significa NIS2 per la tua organizzazione e quale impatto può avere su di te.

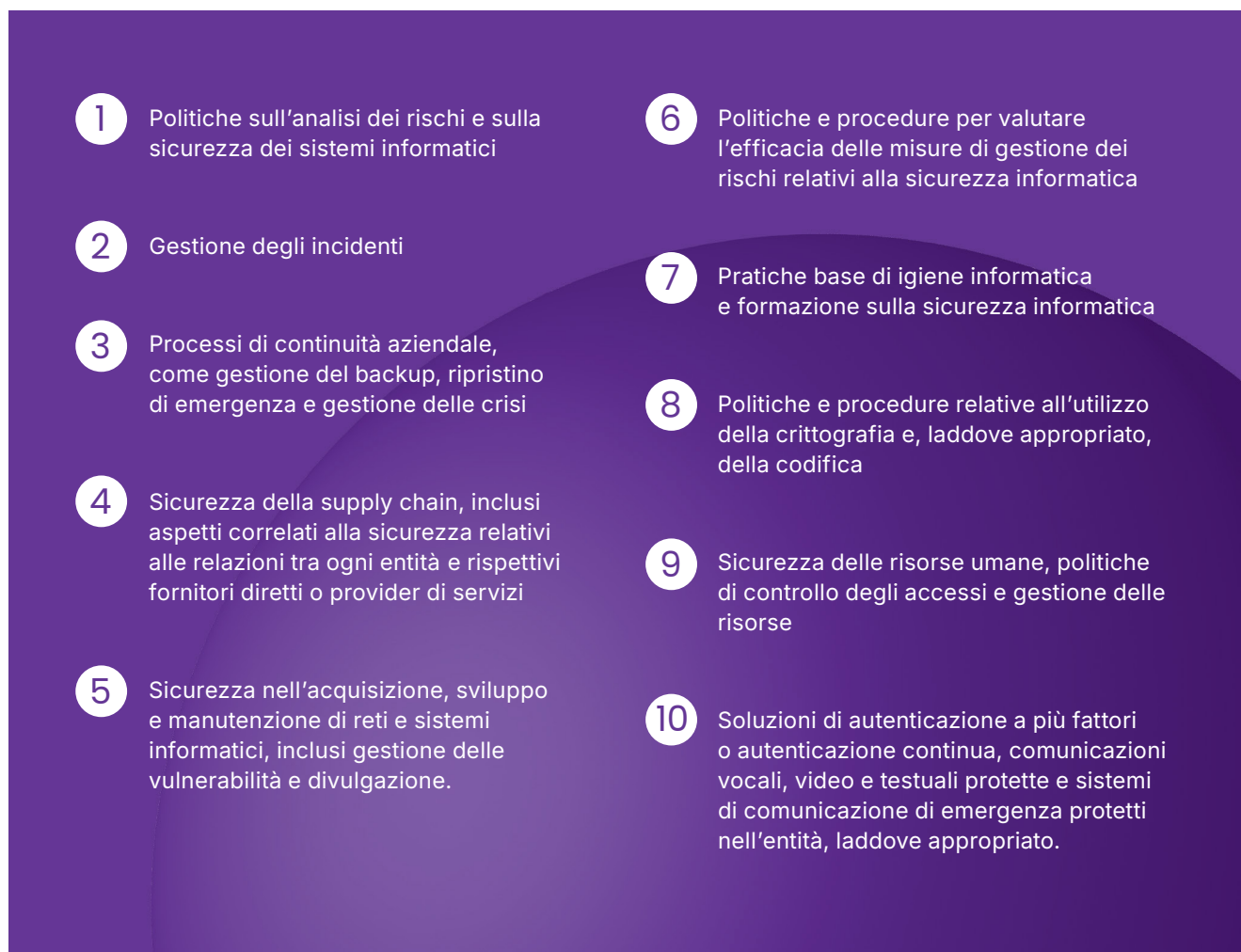
### Introduzione

La direttiva NIS2 sottolinea l'importanza di una strategia approfondita per la sicurezza informatica all'interno delle organizzazioni. Sebbene si tratti di un quadro normativo molto dettagliato e raccomandiamo alle organizzazioni interessate all'interno di uno Stato membro di prendersi il tempo di leggere autonomamente gli articoli, abbiamo creato alcuni punti salienti per aiutarti a iniziare la tua valutazione, a partire dalle dieci misure minime di sicurezza informatica evidenziate nella direttiva.

# Le dieci misure di gestione del rischio per la sicurezza informatica

Una delle sezioni più critiche della direttiva è l'articolo 21, che elenca dieci misure di gestione dei rischi per la sicurezza informatica. Gli Stati membri devono garantire che le entità "essenziali" e "importanti" attuino misure tecniche, operative e organizzative idonee a gestire i rischi per la sicurezza delle loro reti e dei loro sistemi informativi utilizzati nelle loro operazioni o nei loro servizi. Tali misure dovrebbero prevenire o ridurre al minimo l'impatto degli incidenti sui destinatari dei servizi. Devono tenere conto delle tecnologie più recenti, degli standard pertinenti e dei costi, nonché garantire che il livello di sicurezza sia adeguato al livello di rischio. Nel valutare la proporzionalità delle misure di sicurezza, le organizzazioni devono considerare la loro esposizione al rischio, le loro dimensioni e il potenziale impatto degli incidenti. Ciò include la valutazione della gravità e della probabilità degli incidenti, nonché dei loro effetti sociali ed economici.

La direttiva NIS2 elenca dieci misure di sicurezza informatica che tutte le entità qualificate devono implementare:

- 
- 1 Politiche sull'analisi dei rischi e sulla sicurezza dei sistemi informatici
  - 2 Gestione degli incidenti
  - 3 Processi di continuità aziendale, come gestione del backup, ripristino di emergenza e gestione delle crisi
  - 4 Sicurezza della supply chain, inclusi aspetti correlati alla sicurezza relativi alle relazioni tra ogni entità e rispettivi fornitori diretti o provider di servizi
  - 5 Sicurezza nell'acquisizione, sviluppo e manutenzione di reti e sistemi informatici, inclusi gestione delle vulnerabilità e divulgazione.
  - 6 Politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi relativi alla sicurezza informatica
  - 7 Pratiche base di igiene informatica e formazione sulla sicurezza informatica
  - 8 Politiche e procedure relative all'utilizzo della crittografia e, laddove appropriato, della codifica
  - 9 Sicurezza delle risorse umane, politiche di controllo degli accessi e gestione delle risorse
  - 10 Soluzioni di autenticazione a più fattori o autenticazione continua, comunicazioni vocali, video e testuali protette e sistemi di comunicazione di emergenza protetti nell'entità, laddove appropriato.

## Obbligo di segnalazione

Un tema ricorrente nell'intera direttiva NIS2 è l'importanza della rendicontazione. Le entità "essenziali" sono tenute a predisporre procedure per segnalare rapidamente incidenti significativi di sicurezza informatica, con scadenze specifiche per la segnalazione, incluso un sistema preliminare di "allerta precoce" attivo 24 ore su 24.

NIS2 sottolinea inoltre l'importanza della responsabilità aziendale, richiedendo che il management si impegni attivamente e comprenda gli sforzi dell'organizzazione in materia di sicurezza informatica. I manager potrebbero essere penalizzati per violazioni della sicurezza, potenzialmente

esponendosi a responsabilità e anche divieti temporanei da posizioni dirigenziali.

## Penali

Le nuove norme della direttiva NIS2 sono molto più severe di prima e in alcuni casi introducono sanzioni più elevate o addirittura del tutto nuove.

Tuttavia, i paesi dell'Unione possono decidere di imporre sanzioni ancora più elevate, se lo desiderano. Le aziende considerate "essenziali" dovranno essere preparate a incorrere in sanzioni fino a 10 milioni di euro o al 2% dei loro ricavi annui globali dell'ultimo anno, a seconda di quale importo sia più elevato. Le aziende considerate "importanti" potrebbero incorrere in multe fino a 7 milioni di euro o all'1,4% dei loro profitti globali dell'anno precedente, a seconda di quale importo sia più alto.

## Ma aspetta, c'è di più

Queste tre sezioni illustrano un'ampia gamma di aspettative nella direttiva NIS2; tuttavia, non sono esaustive. Invitiamo tutte le aziende che operano nell'Unione europea a esaminare l'intera direttiva e i relativi requisiti con i propri team e a comprendere appieno le aspettative e le implicazioni di questa imponente legislazione.



# Come Object First può essere di aiuto

NIS2 rappresenta un'evoluzione estremamente importante nella regolamentazione della sicurezza e potrebbe rappresentare un notevole passo avanti per garantire la conformità nei data center di entità "importanti" ed "essenziali". Oltre a scrivere questa guida introduttiva, abbiamo pensato di ampliare alcuni dei nostri consigli per aiutarti a raggiungere in modo efficiente i tuoi obiettivi NIS2.

## Resilienza dei dati Zero Trust

La sezione 89 dell'introduzione della direttiva NIS2 menziona le organizzazioni che adottano Zero Trust per migliorare il loro livello di sicurezza complessivo. Zero Trust è un insieme di principi essenziali per garantire la sicurezza delle app e delle infrastrutture di produzione. Tuttavia, non considera il software di backup e l'archiviazione di backup come parte del suo modello di maturità complessivo.

L'anno scorso, Veeam e Numberline hanno pubblicato la loro ricerca su [Zero Trust Data Resilience \(ZTDR\)](#). Si tratta di un approccio completo alla protezione dei dati che estende i principi di sicurezza Zero Trust all'ambiente di backup di un'organizzazione. Introduce elementi critici quali la separazione tra software di backup e archiviazione di backup, più zone di resilienza e archiviazione di backup immutabile e crittografata. Questo approccio riduce al minimo i rischi, rafforza la protezione dei dati e aumenta il livello di sicurezza di un'organizzazione. Comprendere ZTDR è fondamentale per le organizzazioni poiché fornisce un quadro solido per proteggere i propri dati dalle minacce informatiche, in particolare dagli attacchi ransomware e di esfiltrazione dei dati. Offre un'alternativa più sicura ai modelli di sicurezza tradizionali per quanto riguarda la protezione dei dati e dovrebbe essere parte della checklist di ogni amministratore per quanto riguarda la preparazione al NIS2. Per maggiori informazioni su ZTDR, leggi il nostro whitepaper.

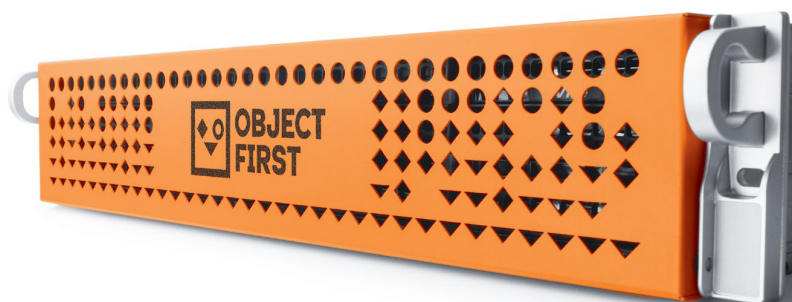
## Archiviazione dati di backup immutabile

Sorprendentemente, il termine immutabilità non è menzionato nella direttiva NIS2. L'aspetto più importante della protezione dei dati è la capacità di recupero; con l'archiviazione immutabile, la probabilità di recupero è molto più alta. Oggi la maggior parte degli attacchi prende di mira innanzitutto l'infrastruttura di backup per eliminare la possibilità di ripristino e garantire il pagamento del riscatto. Le misure di sicurezza informatica dell'articolo 21 accennate in precedenza menzionano direttamente i requisiti di protezione dei dati, l'igiene della sicurezza informatica e la crittografia. Tuttavia, tutti questi elementi possono essere violati e distrutti. Al contrario, un target di archiviazione immutabile conforme alle best practice ZTDR, come l'accesso zero alla root, un'architettura intrinsecamente segmentata dal software di backup e un'archiviazione che sfrutta il blocco degli oggetti S3 in modalità di conformità, contribuirà ad aumentare la resilienza di fronte a un attacco.

# Raggiungimento degli obiettivi di tempo di recupero

La direttiva contiene numerose affermazioni sull'importanza di una strategia di ripristino, tra cui un piano di ripristino reattivo e simulazioni di ripristino di prova prima che si verifichi un attacco informatico. Consigliamo a tutte le organizzazioni interessate dalla normativa NIS2 di prendersi il tempo necessario per valutare i propri attuali ambienti di protezione dei dati e di eseguire scenari di ripristino di prova per valutare meglio i propri reali obiettivi di punto di ripristino (RPO) e obiettivi di tempo di ripristino (RTO). Comprendere quanto indietro si dovrà andare per il ripristino, insieme al tempo necessario per recuperare i dati, è un aspetto fondamentale della reattività richiesta da NIS2.

## Scopri Ootbi (Immutabilità immediata)



Object First si propone di aiutare tutti i clienti Veeam nell'UE a garantire che la loro archiviazione di backup superi gli standard NIS2. Ecco perché Object First ha creato Ootbi, l'archiviazione migliore per Veeam. A prova di ransomware e immutabile fin da subito, Ootbi di Object First offre un'archiviazione di backup sicura, semplice e potente, progettata appositamente per Veeam. Il dispositivo può essere installato in rack, impilato e alimentato in 15 minuti.

Ootbi aiuta gli amministratori Veeam a implementare un'architettura Zero Trust Data Resilience per backup e ripristini indistruttibili. Grazie alla sua architettura "secure by design", Ootbi garantisce che i dati di backup di Veeam rimangano immutabili e non richiede alcuna competenza aggiuntiva in materia di sicurezza da parte dell'utente finale.

## Conclusione

La direttiva NIS2 sarà presto disponibile: il 17 ottobre 2024 sarà recepita dagli Stati membri. Come per qualsiasi mandato importante, ciò richiederà uno sforzo notevole da parte di molti individui all'interno di organizzazioni "importanti" ed "essenziali" per garantire che non vengano multati per non conformità. L'istruzione sarà sempre un primo passo fondamentale per soddisfare le richieste di legislazioni come queste. Se sei interessato dalla [direttiva NIS2](#), prenditi il tempo necessario per leggerla integralmente e assicurarti che la tua organizzazione sia consapevole delle implicazioni. Anche se inizialmente questa iniziativa potrebbe rivelarsi destabilizzante, ne varrà sicuramente la pena, in quanto contribuirà a ridurre le attività criminali dannose.

