NIS2

Lista di controllo

Prepararsi strategicamente alla conformità

Acquisti in rete pa

doudlex. powered by uese italia

+39 041 872 3001

uese.eu

Uese Italia SpA

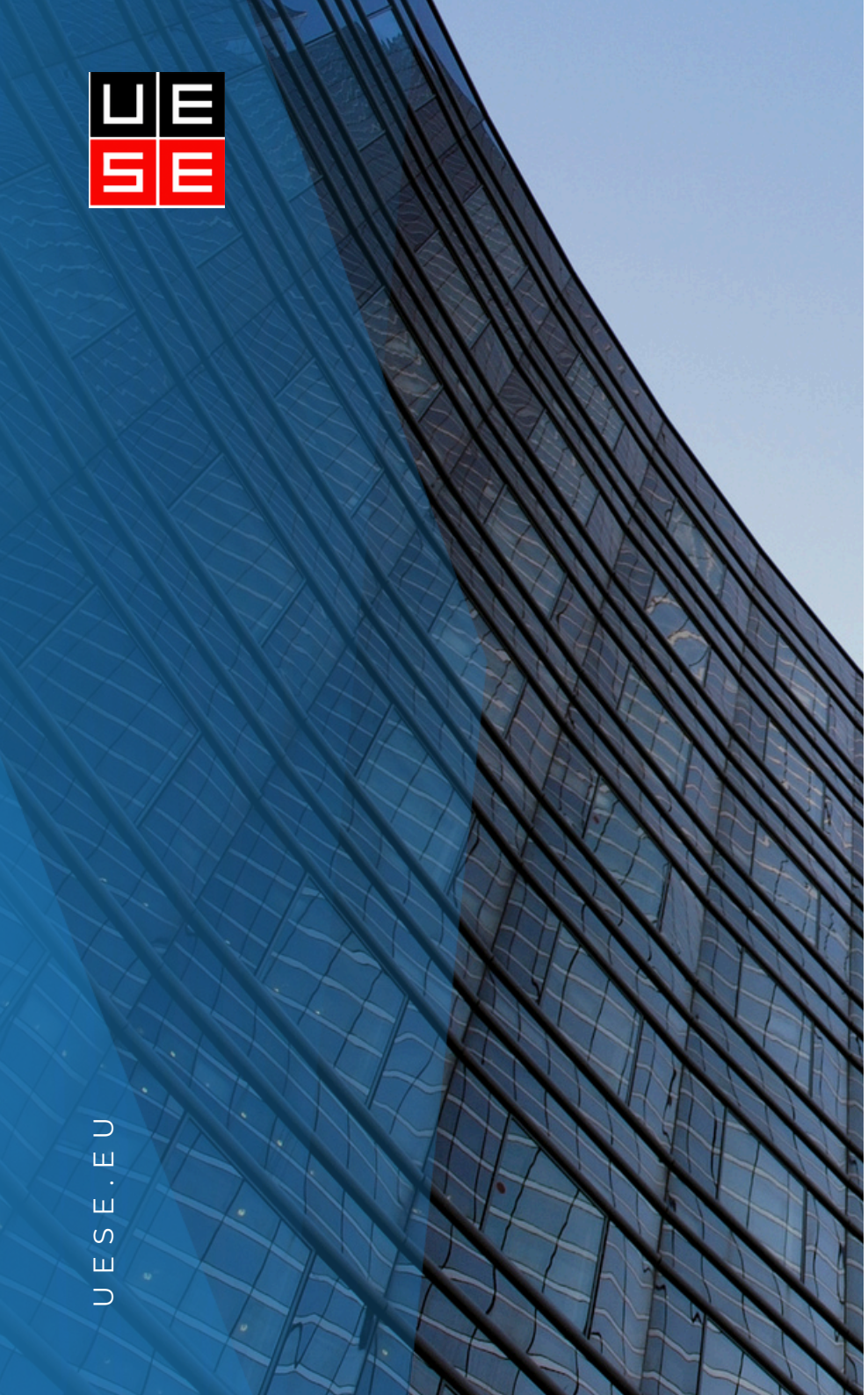
NIS2 Checklist

INTRODUZIONE

L'introduzione della Direttiva sulla sicurezza delle reti e dell'informazione2(NIS2) segna un importante passo avanti negli sforzi dell'Unione Europea per rafforzare la cybersecurity in una più ampia gamma di settori e organizzazioni. Con una scadenza di conformità al17 ottobre 2024, la NIS2 mira a mitigare le minacce informatiche e a migliorare la sicurezza informatica. Estende le misure fondamentali di gestione del rischio di cybersecurity e gli obblighi di segnalazione stabiliti dal suo predecessore, NIS2, con l'obiettivo di migliorare la postura comokessiva della cybersecurity; NIS2 introduce una responsabilità più rigorosa attraverso obblighi di segnalazione più severi e sanzioni più severe, e garantirà una solida sicurezza per le imprese. Si tratta di un'importante pietra miliare per le organizzazioni che si impegnano a mantenere un quadro di cybersecurity.

Preparatevi alla Network and Information System Directive 2 (NIS2) con una lista di controllo completa. È stata progettata per guidarvi attraverso i passi essenziali verso la conformità, evidenziando le opportunità per aumentare la sicurezza informatica, la resilienza operativa e la fiducia degli stakeholder. utilizzate questa lista di controllo per assicurarvi di coprire tutti gli aspetti della NIS2 e usarla come catalizzatore per l'eccellenza nella cybersecurity e la trasformazione digitale.

UESE.EU



UESE.EU

NIS2 Checklist

COMPRENSIONE E PIANIFICAZIONE DELLA DIRETTIVA NIS 2

Conoscere l'ambito di applicazione e il calendario della NIS2 è fondamentale per adeguarsi tempestivamente: la scadenza è fissata al 17 ottobre 2024 e riguarda più di 160.000 aziende in 15 settori. Preparatevi per tempo per evitare sanzioni e garantire una transizione senza intoppi.

Valutare la vostra attuale posizione di sicurezza informatica rispetto ai requisiti NIS2.
La valutazione della vostra posizione di sicurezza informatica rispetto ai requisiti NIS2 identifica le le lacune di difesa e le aree di miglioramento, assicurando che la vostra organizzazione soddisfi un livello base di misure di sicurezza. Il framework di Uese Italia SpA è un complemento naturale ai requisiti di sicurezza NIS2. Fornisce una solida base che integra in modo naturale i requisiti di sicurezza NIS2 e facilità una transizione agevole verso la conformità.

Identificare le aree e i servizi pertinenti all'interno dell'organizzazione. Comprendere quali parti dell'organizzazione rientrano nell'ambito di applicazione esteso della NIS2 per garantire la piena conformità e le misure di sicurezza in tutte le aree applicabili.

PROMUOVERE UNA CULTURA ORIENTATA ALLA SICUREZZA

Formazione sulla sicurezza informatica per tutti i dipendenti :
Fornire ai dipendenti la conoscenza delle migliori pratiche di sicurezza informatica può ridurre al minimo il rischio di attacchi di social engineering e malware, i principali vettori di violazione.

Potenziamento dei team di sicurezza informatica:
Gli strumenti basati sull'intelligenza artificiale possono contribuire a risolvere la carenza di professionisti qualificati della sicurezza informatica,migliorando l'efficienza dei team e consentendo loro di concentrarsi sulle misure di difesa strategiche e sull'innovazione.

NIS2 Checklist

PIANIFICAZIONE: APPROCCIO STRATEGICO ALLA CYBERSECURITY

Valutazione completa del rischio:
Protezione proattiva contro potenziali violazioni attraverso l'identificazione delle vulnerabilità e l'implementazione di misure di salvaguardia, in linea con l'enfasi postada NIS2 sulla gestione preventiva del rischio.

Pianificazione della risposta agli incidenti e del recupero:
La NIS2 richiede piani di mitigazione del rischio e di gestione degli incidenti. È possibile mettere in atto misure per ridurre al minimo l'impatto di una violazione ,garantire la continuità aziendale e mantenere la fiducia dei clienti e l'integrità operativa.

Misure di sicurezza della catena di fornitura:
Proteggere la catena di fornitura dagli attacchi informatici è fondamentale. Infatti, le vulnerabilità nei servizi di terzi possono essere il punto di ingresso per una violazione e mettere a rischio l'intera rete.

PARTNER: FORNIRE COMPETENZE E SOLUZIONI

Collaborare con un partner di sicurezza fidato:
La collaborazione con un fornitore di sicurezza esperto può rafforzare il vostro regime di cybersecurity con soluzioni e approfondimenti avanzati, rendendo la conformità uno sforzo condiviso piuttosto che una sfida solitaria. uese Italia è pronta a fornire intuizioni e soluzioni che sono strettamente allineate con lo spirito di NIS2.

Usare servizi cloud secure-by-design:
La scelta di un servizio cloud progettato con la sicurezza al centro, supporta la conformità con una difesa avanzata, servizi gestiti e una mitigazione predittiva delle minacce in linea con i requisiti NIS2.

NIS2 Checklist

TECNOLOGIA E STRUMENTI:
POTENZIARE CONFORMITÀ E SICUREZZA

Implementazione dell'autenticazione a più fattori (MFA):
L'MFA è la pietra miliare di Zero Trust eNIS2; l'MFA aggiunge un importante livello di sicurezza e progetto dall'accesso non autorizzato a dati e sistemi sensibili.

Utilizzo di tecniche di crittografia avanzate:
La crittografia protegge sia i dati inattivi che quelli in transito, salvaguardando i dati dalle violazioni e garantendo la riservatezza e l'integrità delle informazioni sensibili.

Adozione di analisi di sicurezza basate sull'intelligenza artificiale:
L'intelligenza artificiale e l'apprendimento automatico possono migliorare la velocità e l'efficienza delle operazioni di sicurezza informatica in conformità con i requisiti di rilevamento delle minacce avanzate di NIS2, analizzando rapidamente le minacce e automatizzando le risposte.

NIS2 Checklist

MONITORAGGIO E REPORTING: TRASPARENZA E RESPONSABILITÀ

Monitoraggio e segnalazione regolari della sicurezza informatica:
Il monitoraggio continuo e la segnalazione tempestiva degli incidenti sono imposti dal NIS2 per garantire l'individuazione tempestiva delle minacce e minimizzare l'impatto ,oltre a garantire la conformità normativa.

Documentazione delle attività di conformità:
la conservazione di una documentazione dettagliata delle attività di conformità non solo aiuta a rispettare la NIS2, ma dimostra anche agli stakeholder l'impegno dell'azienda nei confronti della sicurezza informatica, rafforzando la fiducia e la sicurezza.
Questa lista di controllo fornisce un approccio sistematico alla conformità alla norma NIS2 e sottolinea l'importanza di ogni passo verso un ambiente digitale sicuro e resiliente.
Seguendo questa guida, la vostra organizzazione può cogliere l'opportunità non solo di soddisfare i requisiti della direttiva, ma anche di migliorare la vostra strategia di cybersecurity e promuovere la fiducia di clienti e della comunità in generale.
Il nostro impegno è quello di sostenervi nel percorso, sorprendendo sul serio i vostri livelli di sicurezza e utilizzando la nostra esperienza per promuovere un ambiente digitale sicuro, conforme e resiliente.

NIS2 Checklist

Chi sono i soggetti coinvolti nella Direttiva NIS2

A DIRETTIVA NIS2 MIRA A CONSEGUIRE UN LIVELLO DI CYBERSICUREZZA COMUNE ALL'INTERNO DELL'UE

Una delle più importanti novità introdotte a tal fine riguarda il perimetro di applicazione della NIS2, significativamente più esteso rispetto alla precedente NIS, sia in termini di numero di soggetti che di settori coinvolti. Se la NIS si rivolgeva ai soli "Operatori di servizi essenziali" (OSE) e "Fornitori di servizi digitali" (FSD), la nuova Direttiva si applica a tutte le organizzazioni identificate come soggetti "**Essenziali**" o "**Importanti**".
Per stabilire se un'organizzazione rientri in una di queste categorie, viene ridotto il margine di discrezionalità in capo agli Stati Membri, introducendo un duplice criterio basato su dimensione e settore di appartenenza: sono in perimetro le grandi e le medie imprese attive nei settori merceologici e aventi le caratteristiche indicate negli allegati I e II alla Direttiva.

NIS2 Checklist

DIRETTIVA NIS2: I PRINCIPALI OBBLIGHI PER LE ORGANIZZAZIONI

Gli adempimenti richiesti dalla Direttiva NIS2 riguardano i seguenti ambiti:

1. **Governo della cybersecurity**: gli organi di gestione devono approvare le misure per la gestione dei rischi adottate dall'Organizzazione, seguire un'adeguata formazione e garantire una formazione analoga ai propri dipendenti;
2. **Gestione dei rischi**: i soggetti sono tenuti a adottare misure tecniche, operative e organizzative per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che i soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi;
3. **Continuità operativa**: i soggetti devono garantire la continuità dei propri servizi e ridurre al minimo l'impatto di eventuali interruzioni attraverso misure quali la gestione del backup, il ripristino in caso di disastro e la gestione delle crisi;
4. **Sicurezza della catena di approvvigionamento**: i soggetti sono chiamati a proteggere la propria catena di fornitura valutando le vulnerabilità specifiche dei propri fornitori e l'adeguatezza delle loro pratiche di cybersicurezza;
5. **Segnalazione degli incidenti**: i soggetti sono obbligati a segnalare gli incidenti che abbiano un impatto significativo sulla fornitura dei propri serviziai rispettivi CSIRT o autorità nazionali competenti (preallarme entro 24 ore e notifica completa/integrativa entro 72 ore da quando sono venuti a conoscenza dell'incidente significativo).


THANK YOU
uese.eu