CSI
your digital partner

NIS2

UNA PROVA DA AFFRONTARE INSIEME

PREPARAZIONE, STRATEGIA, RESILIENZA

TUTTO QUELLO CHE SERVE PER APPLICARE LA DIRETTIVA

L'**Italia** ha subìto nel 2024 **il 10% degli attacchi mondiali**

8 incidenti su 10 sono di matrice **cybercrime**

+15% **incidenti** subìti rispetto al 2023

10% incidenti nel **settore pubblico**

1/3 incidenti causati da **malware**

90% incidenti basati su **vulnerabilities**

35% incidenti basati su **phishing e ingegneria sociale**

Rapporto Clusit sulla Cybersecurity in Italia e nel mondo 2025

75% impatto del **fattore umano** sul rischio cyber

73% impatto dell'**obsolescenza** dell'infrastruttura IT

Osservatori.net Politecnico di Milano 2024

LA NUOVA FRONTIERA DELLA SICUREZZA DIGITALE

Un passo importante per garantire una protezione avanzata contro rischi e attacchi cyber sempre più complessi

La **NIS 2** è la **nuova direttiva europea** sulla sicurezza delle reti e dei sistemi informativi, che sostituisce la Direttiva NIS 2016.
L'obiettivo è **creare un ambiente digitale più sicuro, omogeneo e resiliente** nell'Unione Europea.

Molte organizzazioni devono aggiornare le loro politiche e procedure di sicurezza informatica per rispettare i nuovi obblighi, **con sanzioni significative per chi non si adegua.**

LA NUOVA FRONTIERA DELLA SICUREZZA DIGITALE

Cosa cambia

1. Ampliamento dei settori e dei soggetti coinvolti
2. Requisiti di sicurezza più rigorosi
3. Obblighi di segnalazione tempestiva degli incidenti
4. Sanzioni più severe
5. Responsabilità dei soggetti «importanti» ed «essenziali» estesa a tutte le funzioni dell'organizzazione

NIS2, UNA OPPORTUNITÀ PER TUTTI

La NIS2 si applica alle pubbliche amministrazioni e ad altri settori chiave come energia, trasporti, rifiuti, finanza e salute

amministrazioni centrali

amministrazioni locali

Regioni
Province autonome
Città metropolitane
Comuni con popolazione >100.000 abitanti
Comuni capoluogo di Regione
Aziende sanitarie

organizzazioni del settore pubblico

Società di trasporto pubblico
Società "in house" fornitrici di servizi
...

COSA È NECESSARIO FARE?

Adottare misure di sicurezza più rigorose

- Implementare politiche di analisi dei rischi e politiche di sicurezza robuste
- Garantire la protezione delle informazioni e dei sistemi critici
- Creare un piano di risposta agli incidenti
- Garantire la continuità operativa dei servizi
- Assicurarsi che i fornitori e i partner rispettino gli stessi standard di sicurezza

Notificare gli incidenti informatici significativi

24h pre-notifica

72h notifica ufficiale di un incidente

1 mese relazione finale

Promuovere la formazione continua sul rischio cyber

- Organi direttivi
- Dipendenti

Attenzione alle sanzioni

Da 10.000 a 50.000 € per la non registrazione, la mancata comunicazione o l'aggiornamento delle informazioni

Da 25.000 a 125.000 € se si violano gli obblighi relativi alla sicurezza informatica

OBBLIGHI GRADUALI MA SCADENZE RAVVICINATE

OGNI ANNO

Da 1 gennaio 2024 a 28 febbraio 2025
registrazione delle informazioni sulla piattaforma digitale di ACN
https://portale.acn.gov.it/

Entro aprile 2025
comunicazione dell'elenco definitivo dei soggetti interessati da parte di ACN

Tra aprile e maggio 2025
trasmissione e aggiornamento delle informazioni sulla piattaforma digitale

2026

Da gennaio
obbligo di notifica degli incidenti di sicurezza

Da ottobre
implementazione delle misure di sicurezza richieste

TU PREPARATI

NOI TI ACCOMPAGNIAMO

COSA TI OFFRIAMO

Ti accompagniamo passo a passo verso la compliance, offrendo **consulenza, supporto e formazione** per:

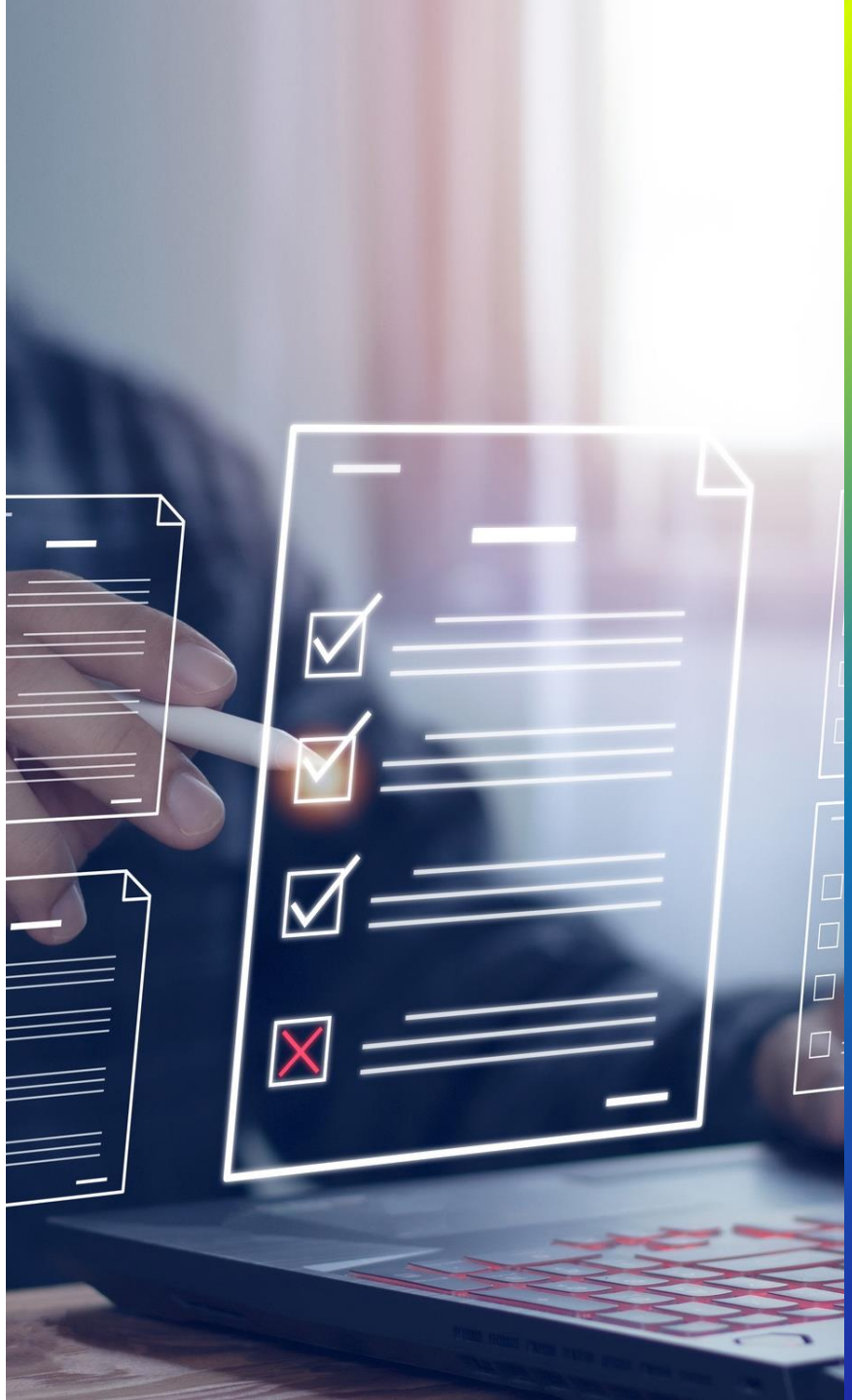
- consulenza preliminare e analisi *as is*
- gestione misure di sicurezza
- gestione del rischio
- continuità operativa
- consapevolezza delle persone

VALUTIAMO LA RESILIENZA DELLE TUE INFRASTRUTTURE E APPLICAZIONI IT

assessment sulla postura di sicurezza e sulla resilienza dei sistemi da parte dai nostri esperti di cybersecurity

supporto nella valutazione del rischio cyber e delle misure di sicurezza idonee

affiancamento per lo sviluppo di un **Remediation Plan**



TI AIUTIAMO A COSTRUIRE LA TUA CONTINUITÀ OPERATIVA

RISK ASSESSMENT

- Individuazione dei principali rischi
- Individuazione degli scenari prioritari per la Continuità Operativa

← Interviste con la Direzione e primi livelli operativi

BUSINESS IMPACT ANALYSIS

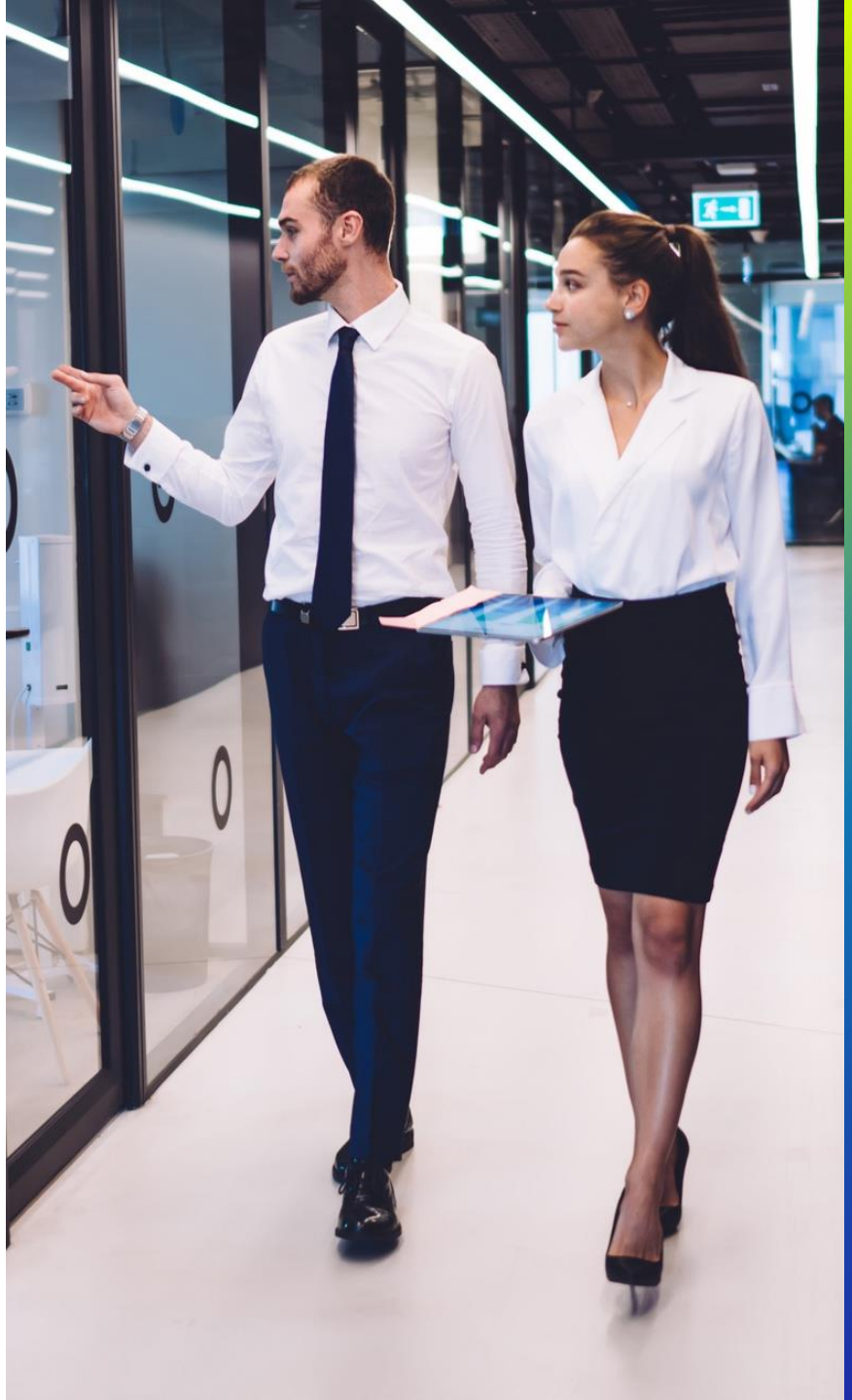
- Identificazione dei processi prioritari per l'erogazione dei prodotti e servizi più urgenti
- Identificazione delle risorse e dei fabbisogni necessari per la continuità e il recupero di tali attività

← Interviste con i livelli operativi influenzati dagli scenari prioritari

BUSINESS CONTINUITY PLAN

- Strategia di continuità operativa
- Procedure di ripristino
- Se sei ospitato nella nostra infrastruttura cloud, possiamo offrirti servizi di **continuità operativa** e **Disaster Ricovery**

← 1. Presentazione alla Direzione
2. Revisione del Piano
3. Approvazione definitiva
4. Test



PER TE, IL NOSTRO DIGITAL CAMPUS

Percorso formativo dedicato alla NIS2
online asincrono, aula virtuale, in presenza

- **Corso base per tutti i dipendenti**
- **Corso avanzato per esperti sicurezza, sistemi IT, responsabili di servizi, referenti privacy**
- **Corso specialistico per dirigenti e top management, organi direttivi, CISO, DPO**

Nuovi corsi, sempre al passo con gli aggiornamenti di ACN

I nostri docenti: l'Academy CSI
Puoi contare su un team di esperti CSI con solide competenze tecniche

Scopri di più sulla nostra offerta formativa su **digitalcampus.csi.it**

NIS2 UNA PROVA DA AFFRONTARE INSIEME

CSI, IL TUO ALLEATO PER LA TRANSIZIONE DIGITALE. PERCHÉ AFFIDARSI A NOI

Il CSI **da quasi 50 anni** è un partner tecnologico di riferimento per la **pubblica amministrazione**, con una lunga tradizione nell'**innovazione digitale**.

I dati di cittadini, imprese e amministrazioni sono un patrimonio di grande valore.
La cultura della sicurezza è alla base del nostro lavoro.

ACCREDITED BY TRUSTED INTRODUCER TI

Il nostro **CSIRT** (Computer Security Incident Response Team) è al servizio dei nostri clienti consorziati per la prevenzione delle minacce e il supporto nella gestione degli incidenti.

NIS2 UNA PROVA DA AFFRONTARE INSIEME

UN PARTNER CERTIFICATO

ISO 20000-1 | Gestione dei servizi

ISO 22301 | Gestione continuità operativa

ISO 27001 | Sicurezza delle informazioni

CSA Star livello 2 | Sicurezza delle informazioni

ISDP 10003:2020 | Conformità al GDPR del Fascicolo Sanitario Elettronico

658
vulnerability assessment nel 2024

18.000
postazioni di lavoro protette

1.800
autenticazione multi fattore
su servizi di accesso remoto

4.500
dipendenti pubblici hanno fatto formazione
su phishing e cybersecurity (2023-24)

CSI
your digital partner

INIZIA LA TRASFORMAZIONE

VUOI MAGGIORI INFORMAZIONI SUI NOSTRI SERVIZI?

clienti@csi.it