CONFINDUSTRIA
VENETO EST
Area Metropolitana
Venezia Padova Rovigo Treviso

Appuntamenti con l'InnovAzione 2025

NIS2:
le 10 misure chiave di sicurezza tradotte in tecnologie e applicazioni concrete.

09/06/2025

IL RELATORE

Lorenzo Celussi
CISO e Resp. ISO 27001

Tinet®
DIGITAL SOLUTIONS

Azienda certificata ISO 27001
CSQA
GESTIONE SICUREZZA delle INFORMAZIONI

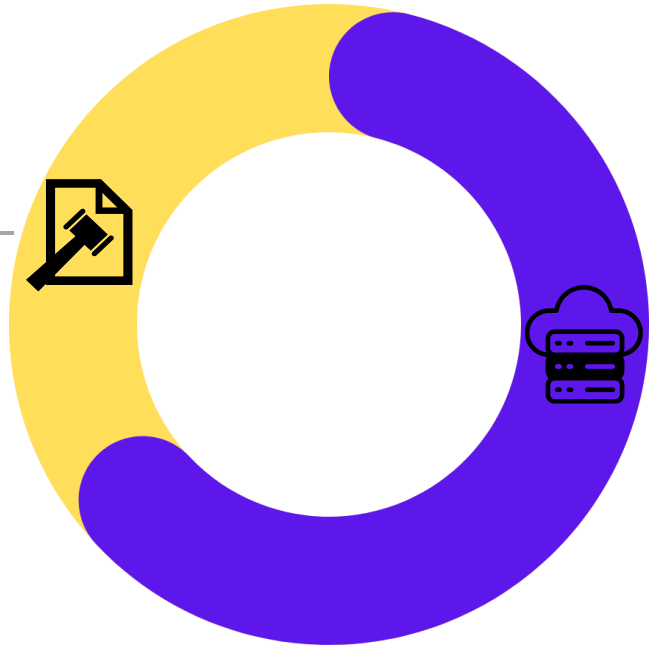
TINET srl è un System Integrator IT con sede principale in provincia di Treviso: offriamo soluzioni e servizi IT evoluti, con un forte focus sulla cybersecurity.

COMPONENTI DELLA DIRETTIVA NIS2

La Direttiva NIS2 ***Legge*** *in vigore da* ***Ottobre 2024*** *che definisce l'****obbligatorietà dei requisiti minimi*** *di* ***CyberSecurity*** *per* ***determinate aziende*** *di* ***tutta Europa****, si articola in* ***due aree principali*** *di adempimento per le organizzazioni*:

Requisiti Organizzativi & Implicazioni Legali

Requisiti normativi, processi interni e responsabilità legali che le organizzazioni devono rispettare



Infrastruttura Tecnologica

Soluzioni tecniche e misure di sicurezza per proteggere sistemi e dati

Agenzia per la cybersicurezza nazionale

https://www.acn.gov.it/portale/nis

La **NIS2** oltre a riguardare i soggetti obbligati per legge, rappresenta un **modello di riferimento** utile anche per tutte le altre imprese.

LE 10 MISURE DI SICUREZZA NIS2

1. **Politiche di Analisi dei Rischi e Sicurezza Informatica**
   Definizione di politiche per valutare e gestire i rischi informatici.

2. **Gestione degli Incidenti**
   Procedura per gestire e rispondere agli incidenti di sicurezza.

3. **Continuità Operativa**
   Pianificazione per garantire il ripristino delle attività in caso di disastro.

4. **Sicurezza della Catena di Approvvigionamento**
   Protezione dei rapporti con fornitori per garantire la sicurezza.

5. **Sicurezza e manutenzione Sistemi Informativi e di Rete**
   Sicurezza Sistemi Informativi e di rete, e gestione e divulgazione vulnerabilità

6. **Valutazione dell'Efficacia delle Misure**
   Verifica dell'efficacia delle misure di gestione dei rischi informatici.

7. **Pratiche di Igiene Informatica e Formazione**
   Adozione di pratiche di base per mantenere la sicurezza informatica.

8. **Utilizzo della Crittografia**
   Implementazione di politiche e procedure per l'uso corretto della crittografia.

9. **Sicurezza delle Risorse Umane**
   Strategie di Controllo dell'accesso e gestione degli assetti.

10. **Soluzioni di Autenticazione, MFA e Comunicazione Protette**
    Implementazione di sistemi di autenticazione avanzati e comunicazioni sicure.

MODELLO DI APPROCCIO ALLA CYBERSECURITY

CONOSCI LA TUA AZIENDA → **IDENTIFICA**

PROTEGGI I TUOI ASSETS → **PROTEGGI**

VIOLAZIONE → **RILEVA**

MINIMIZZA L'IMPATTO → **RISPONDI**

RIPRENDI LE TUE ATTIVITÀ → **RIPRISTINA**

PREVENZIONE

- Risk & Security Assessment
- Vulnerability Assessment
- Penetration Testing
- Mappatura degli Asset/ Monitoraggio IT
- Dark Web Monitoring
- Security Awareness
- Test Phishing

- Firewall
- Antivirus
- Protezione della Posta
- MFA
- Cifratura
- Password Manager
- Backup
- Log Management
- Segmentazione di Rete

- XDR
- MDR SOC 24x7

GESTIONE DEI DANNI

- XDR
- MDR SOC 24x7
- Piano di risposta all'incidente

- Restore da Backup
- Business Continuity (B.C.)
- Disaster Recovery (D.R.)
- Piano B.C. & D.R.

NIST
Cyber Security Framework

Misure di sicurezza tradotte in soluzioni concrete

Attenzione: la stessa soluzione può garantire l’adempimento a più misure di sicurezza.

POLITICHE DI ANALISI DEI RISCHI E SICUREZZA INFORMATICA

RISK & SECURITY ASSESSMENT

Adozione di **politiche strutturate per la gestione dei rischi** legati alla **sicurezza delle informazioni**, definendo come l'organizzazione:

- Identifica, valuta e gestisce i rischi informatici.
- Pianifica e attua misure di protezione proporzionate a tali rischi.
- Integra la gestione del rischio nei processi decisionali e operativi.

Implementazione delle tecnologie specifiche per raggiungere il livello di sicurezza desiderato.

POLITICHE DI ANALISI DEI RISCHI E SICUREZZA INFORMATICA

SECURITY ASSESSMENT

Mappatura e Analisi della **postura di Sicurezza Informatica**, svolta utilizzando Framework internazionali

VULNERABILITY ASSESSMENT

Processo fondamentale per identificare, analizzare e classificare le **vulnerabilità tecniche presenti nei sistemi informatici.**
Attraverso strumenti avanzati e tecniche di scansione, questo servizio permette di **individuare punti deboli che potrebbero essere sfruttati da attacchi informatici**, garantendo una maggiore sicurezza e protezione dei dati aziendali.

PENETRATION TESTING

Simulazione controllata di attacchi per testare la resistenza dei sistemi e identificare falle di sicurezza.

1 **Politiche di Analisi dei Rischi e Sicurezza Informatica**
Definizione di politiche per valutare e gestire i rischi informatici.

TECNOLOGIA

Gestione degli Incidenti

CARATTERISTICA	XDR	MDR – SOC 24x7
Tipo di soluzione	Extended Detection and Response multipiattaforma	Servizio gestito di rilevamento e risposta alle minacce (MDR)
Obiettivo principale	Analisi, correlazione e risposta su dati provenienti da più fonti	Monitoraggio continuo, threat hunting e risposta gestita da esperti 24/7
Funzionalità chiave	- XDR multi-dominio - Correlazione eventi - Threat hunting - Automazione investigativa	- Monitoraggio H24 - Investigazione proattiva - Risposta agli incidenti - Root Cause Analysis
Origine dei dati analizzati	Endpoint, firewall, email, cloud, identità	Tutte le fonti XDR + threat intelligence e AI
Modalità di gestione	Interna, con strumenti per analisi avanzata	Esterna: gestita da esperti in collaborazione con il cliente
Automazione e risposta	Automatizzata con policy e playbook configurabili	Completamente gestita: il team MDR interviene direttamente sugli incidenti
Destinatari ideali	Organizzazioni che desiderano visibilità e controllo su più superfici di attacco	Aziende che vogliono delegare la sicurezza a esperti, senza gestire team interni dedicati
Valore aggiunto	Correlazione multi-layer e investigazione approfondita automatizzata	Protezione completa e continua con risposte rapide anche contro minacce avanzate

COMPLIANCE

PIANO DI **RISPOSTA ALL'INCIDENTE**

Procedure e ruoli per gestire efficacemente incidenti informatici.

TECNOLOGIA

CONTINUITÀ OPERATIVA

RESTORE DA BACKUP

Ripristino dei dati da copie di sicurezza per garantire la continuità operativa dopo una perdita o compromissione.

BUSINESS CONTINUITY

Strategie e strumenti per mantenere attivi i servizi critici anche durante eventi imprevisti.

DISASTER RECOVERY

Piano tecnico per il recupero rapido di sistemi IT e dati aziendali dopo un evento critico.

COMPLIANCE

SICUREZZA DELLA CATENA DI FORNITURA

Valutazioni fornitori
Verifiche di sicurezza approfondite

Connessioni sicure
Protezione dei dati condivisi

Gestione rischi
Monitoraggio continuo

La NIS2 richiede una gestione rigorosa dei rischi legati ai fornitori.
È necessario implementare verifiche di sicurezza, clausole contrattuali specifiche e monitoraggio continuo.

Sicurezza della Catena di Approvvigionamento

4 Protezione dei rapporti con fornitori per garantire la sicurezza.

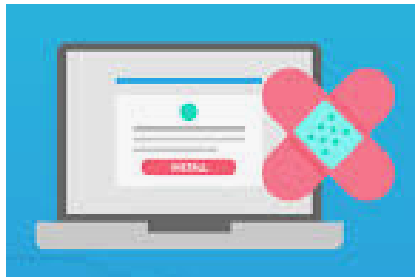
SICUREZZA E MANUTENZIONE SISTEMI INFORMATIVI E DI RETE
VALUTAZIONE DELL'EFFICACIA DELLE MISURE

LOG MANAGEMENT

Soluzione che consente di tracciare e registrare gli accessi ai sistemi, fondamentale per rilevare comportamenti anomali o malevoli. La registrazione dei log non è solo un obbligo normativo ma è anche un alleato in caso di incidenti o verifiche.

PATCH MANAGEMENT

Aggiornamento regolare di software e sistemi operativi per correggere le vulnerabilità



VULNERABILITY ASSESSMENT

Vedi slide n. 8
Questa soluzione è trasversale a più misure di sicurezza.

Sicurezza e manutenzione Sistemi Informativi e di Rete

5 Sicurezza Sistemi Informativi e di rete, e gestione e divulgazione vulnerabilità

Valutazione della Efficacia delle Misure

6 Verifica dell'efficacia delle misure di gestione dei rischi informatici.

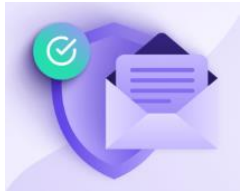
PRATICHE DI CYBER HYGIENE E CRITTOGRAFIA

BACKUP PERIODICO DEI DATI

Backup periodico dei dati per evitare perdite in caso di incidenti

USO DI PASSWORD SICURE

Loro gestione tramite strumenti come **Password Manager**



PROTEZIONE POSTA ELETTRONICA

Filtri avanzati per proteggere la posta elettronica da spam, malware, phishing e allegati pericolosi.

CIFRATURA

Tecnica che rende i dati illeggibili a chi non possiede la chiave di decrittazione, proteggendo la riservatezza.

Pratiche di Igienizzazione Informatica

7 Adozione di pratiche di base per mantenere la sicurezza informatica.

Utilizzo della Crittografia

8 Implementazione di politiche e procedure per l'uso corretto della crittografia.

SICUREZZA DELLE RISORSE UMANE

FORMAZIONE DEL PERSONALE

Formazione continua, in modalità in presenza o e-learning, per aumentare la **consapevolezza dei dipendenti sulle minacce informatiche e le migliori pratiche di sicurezza**. L'obiettivo principale di questo programma formativo è quello di sviluppare la conoscenza delle minacce cyber.

TEST PHISHING

Simulazione di attacchi mail Phishing, tramite l'invio programmato di un mail finte (ma credibili) per osservare se gli utenti aziendali reagiscono cliccando su link, fornendo informazioni sensibili o compiendo altre azioni pericolose.

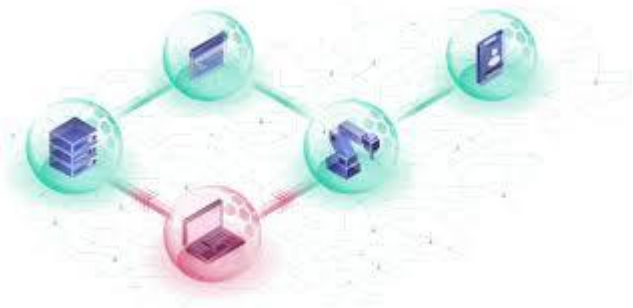
SOLUZIONI DI AUTENTICAZIONE E COMUNICAZIONE PROTETTE

MFA (Multi-Factor Authentication)

È semplice, ma potentissimo.

SEGMENTAZIONE DI RETE

La segmentazione isola i sistemi critici: se un attaccante entra, non può muoversi liberamente nella rete.



Grazie per l'attenzione

Lorenzo Celussi – Tinet srl

Per informazioni:
ricercainnovazione@confindustriavenest.it