

Informatica Forense e NIS2

Ordine degli Ingegneri della Provincia di Milano

Un connubio indissolubile ma sottovalutato

Paolo Dal Checco, Consulente Informatico Forense - Forenser Srl



Chi sono

Mi chiamo **Paolo Dal Checco** e mi occupo d'informatica forense e perizie informatiche. In qualità di **Consulente Informatico Forense** e fondatore di **Forenser Srl**, dedico la mia attività a investigare e analizzare incidenti digitali, acquisire in **copia forense** prove informatiche e fornire **consulenza informatica forense** in ambito privato e aziendale.

La mia esperienza spazia dalla gestione di complesse **indagini digitali** alla consulenza per la valutazione di misure di sicurezza e la conformità normativa, oltre che GDPR e D.Lgs 231 anche per quanto riguarda direttive come la NIS2.

Sono qui per condividere come l'**approccio informatico forense** sia cruciale nella prevenzione e risposta agli attacchi cibernetici e incidenti informatici.

Chi sono

Formazione Accademica

Laurea e Dottorato di Ricerca (Ph.D.) in Informatica presso l'Università di Torino, con specializzazione in crittografia e sicurezza di reti ed elaboratori.

Esperienza Professionale

Oltre 10 anni come **Consulente Informatico Forense**, con più di 2.000 casi gestiti in qualità di CTP informatico, CTU informatico, Esperto Forense, Perito del Giudice, CT del PM e Ausiliario di Polizia Giudiziaria.

Attività Didattica

Docente a Contratto per il corso di Sicurezza Informatica presso SUISS (UniTO), collaborazioni con Master UniGE, UniMI e PoliMI oltre che in Corsi di Perfezionamento.

Attività Divulgativa

Collaboro con TV (Le Iene, Rainews 24, etc...), Radio (Radio24, etc...) e riviste per divulgare la conoscenza in ambito digital forensics e sicurezza informatica

Attività in ambito NIS2



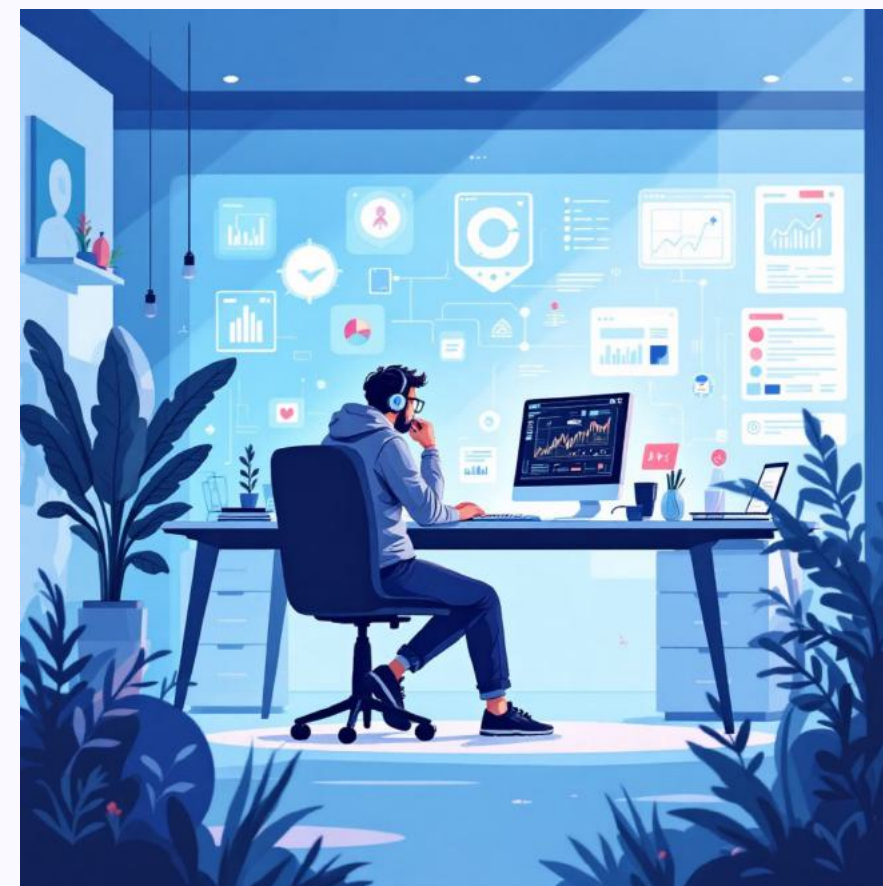
Camera.it

<https://documenti.camera.it> > COM09 > Audizioni PDF

Memoria Scritta sull'Atto del Governo n. 164 cd. NIS2

19 lug 2024 — NIS2 – Paolo Dal Checco (Pag. 1 di 4). Paolo Dal Checco, PhD – Consulente Informatico Forense, Perizie Informatiche e Indagini Digitali.

4 pagine



Ambiti di Specializzazione

- Mobile forensics
- OSINT (Open Source Intelligence)
- Cryptocurrency forensics
- Web forensics
- Analisi forense digitale completa

Il Contesto NIS2: Oltre la Compliance

Cambio di Paradigma

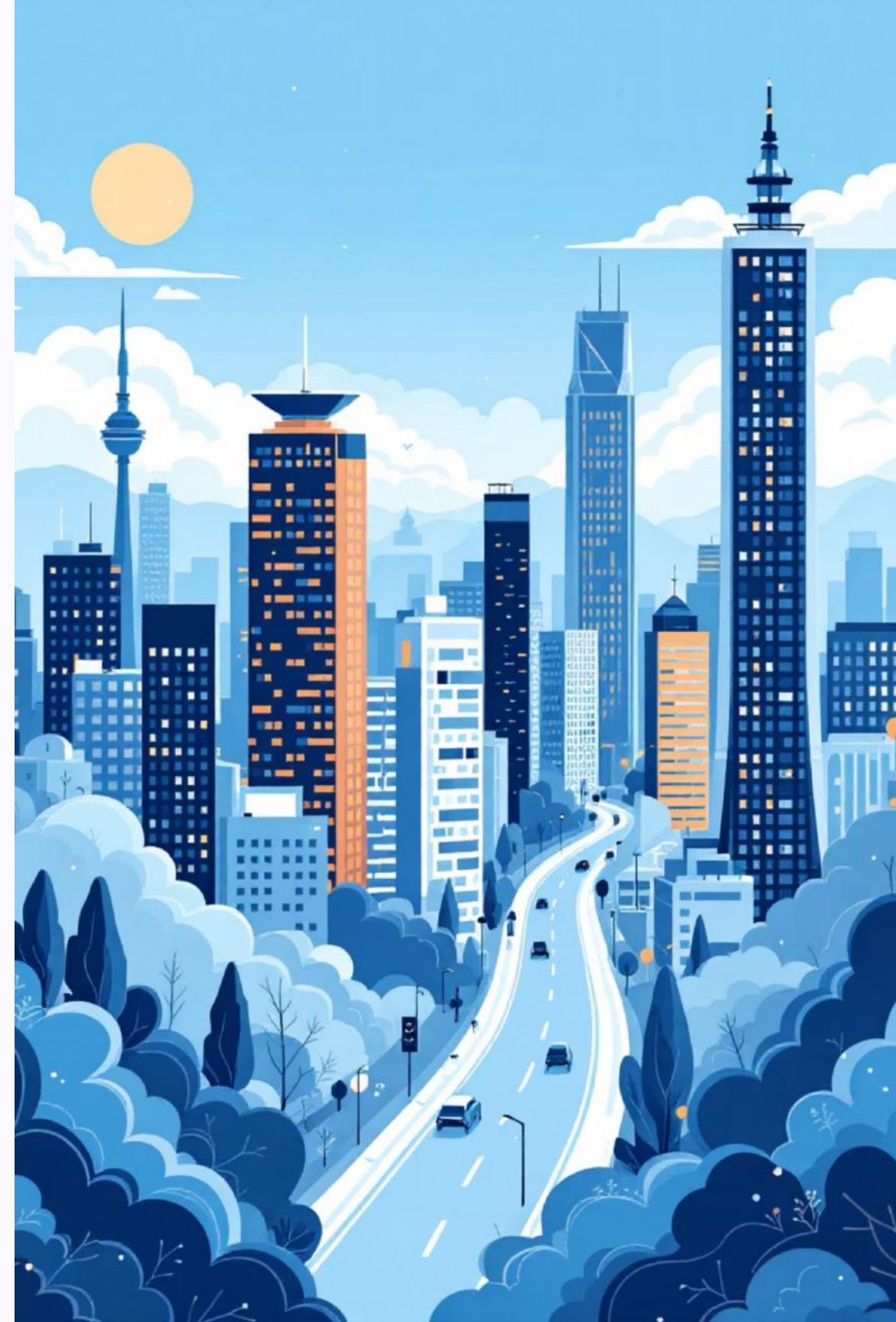
La Direttiva NIS2 rappresenta un'evoluzione significativa: non è più sufficiente "comprare" tecnologie di sicurezza, ma è necessario **dimostrare concretamente** di averle implementate in modo efficace e misurabile.

Approccio Multi-Rischio

La direttiva introduce l'obbligo di implementare **misure di sicurezza** con un approccio **multi-rischio**, proporzionale al rischio identificato attraverso una **valutazione obbligatoria** del sistema informativo e di rete.

Principio di Proporzionalità

Le misure devono essere calibrate in base a tre fattori critici: il **livello di rischio** valutato, le **dimensioni** dell'organizzazione e la **probabilità e gravità** degli incidenti, considerando l'impatto sociale ed economico potenziale.



L'Art. 24: Cosa ci chiede la Legge?

Parte 1 - Le Misure Minime con Prospettiva Forense

1

Analisi dei Rischi e Sicurezza dei Sistemi

Come è possibile valutare accuratamente il rischio senza **analizzare gli incidenti passati**, compresi quelli "mancati" o tentati? L'**informatica forense** è essenziale per questa analisi retrospettiva.

2

Gestione degli Incidenti

Include le **procedure di notifica e risposta**. Questo rappresenta il campo di gioco principale dell'**informatica forense**, dove l'analisi tecnica incontra gli obblighi normativi.

3

Continuità Operativa

Gestione delle crisi, backup e disaster recovery. I backup sono davvero integri? L'attaccante li ha compromessi? Solo un'**analisi forense** approfondita può fornire risposte certe.

4

Sicurezza della Supply Chain

Gestione dei rapporti con fornitori. Se **l'attacco proviene da un vostro fornitore**, come potete dimostrarlo in modo incontrovertibile?

5

Sicurezza nello Sviluppo

Manutenzione continua e gestione proattiva delle **vulnerabilità nei sistemi e nelle applicazioni** critiche.

L'Art. 24: Cosa ci chiede la Legge?

Parte 2 - Il Risolto Investigativo di Ogni Misura

01

Valutazione dell'Efficacia

Politiche per misurare le prestazioni. Le vostre misure (EDR, logging, SIEM) hanno realmente funzionato durante l'incidente? L'analisi post-incidente è l'unica vera metrica di efficacia.

02

Igiene e Formazione

Misure di base come phishing test, awareness training e cultura della sicurezza aziendale.

03

Crittografia

Uso obbligatorio della crittografia e cifratura per proteggere dati sensibili in transito e a riposo.

01

Sicurezza del Personale

Controllo accessi e gestione asset. **Domanda forense fondamentale:** Chi ha fatto cosa, quando e come? L'analisi forense dei log di accesso e delle attività utente è imprescindibile.

02

Autenticazione Forte

Uso di Multi-Factor Authentication (MFA), comunicazioni protette e sistemi di autenticazione robusti per tutti gli accessi privilegiati.



Il "Momento Forense": La Gestione dell'Incidente



Definizione di Incidente Significativo

NIS2 identifica come significativo un incidente che provoca **grave perturbazione operativa** o **perdite finanziarie sostanziali**, con impatto misurabile sui servizi essenziali.



Impatto Sistemico

Include **ripercussioni su altre persone fisiche o giuridiche**, causando perdite materiali o immateriali che si propagano oltre i confini dell'organizzazione colpita.



Distinzione Normativa

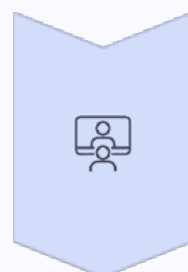
Attenzione critica: Un incidente NIS2 **non coincide necessariamente con un data breach GDPR**. Il focus è sulla **continuità del servizio** e sull'**impatto sistemico**, non solo sulla protezione dei dati personali.

📄 La differenza tra incidente NIS2 e data breach GDPR è fondamentale: mentre il GDPR si concentra sulla violazione di dati personali, NIS2 guarda all'interruzione dei servizi essenziali e all'impatto sulla società nel suo complesso.

Le Misure: Tecniche, Organizzative, Operative

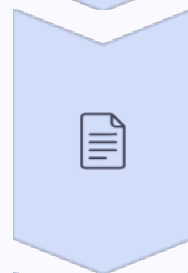
Un Approccio Olistico alla Sicurezza

NIS2 richiede **un'integrazione completa di misure su tre livelli complementari**, ciascuno essenziale per una difesa efficace.



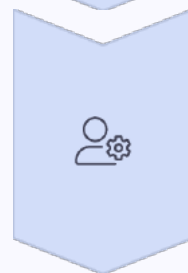
Misure Tecniche

Gli strumenti di protezione: Firewall, antivirus, IDS/IPS, sistemi di autenticazione multifattore (MFA), cifratura end-to-end, EDR/XDR, SIEM e tecnologie di threat detection.



Misure Organizzative

Le regole e la governance: Policy di sicurezza, procedure documentate, regolamenti interni per integrare la cybersecurity nei processi aziendali e nella cultura organizzativa.



Misure Operative

Le azioni quotidiane: Monitoraggio continuo, gestione accessi, backup e ripristino, auditing sistemi, aggiornamenti tempestivi, segregazione dei dati e attribuzione precisa dei ruoli.

Il punto cruciale: I log di sistema, le configurazioni tecniche e le procedure operative (misure operative e tecniche) rappresentano la vostra [prima linea di difesa](#) e la [fonte primaria di prova forense](#) in caso di incidente.

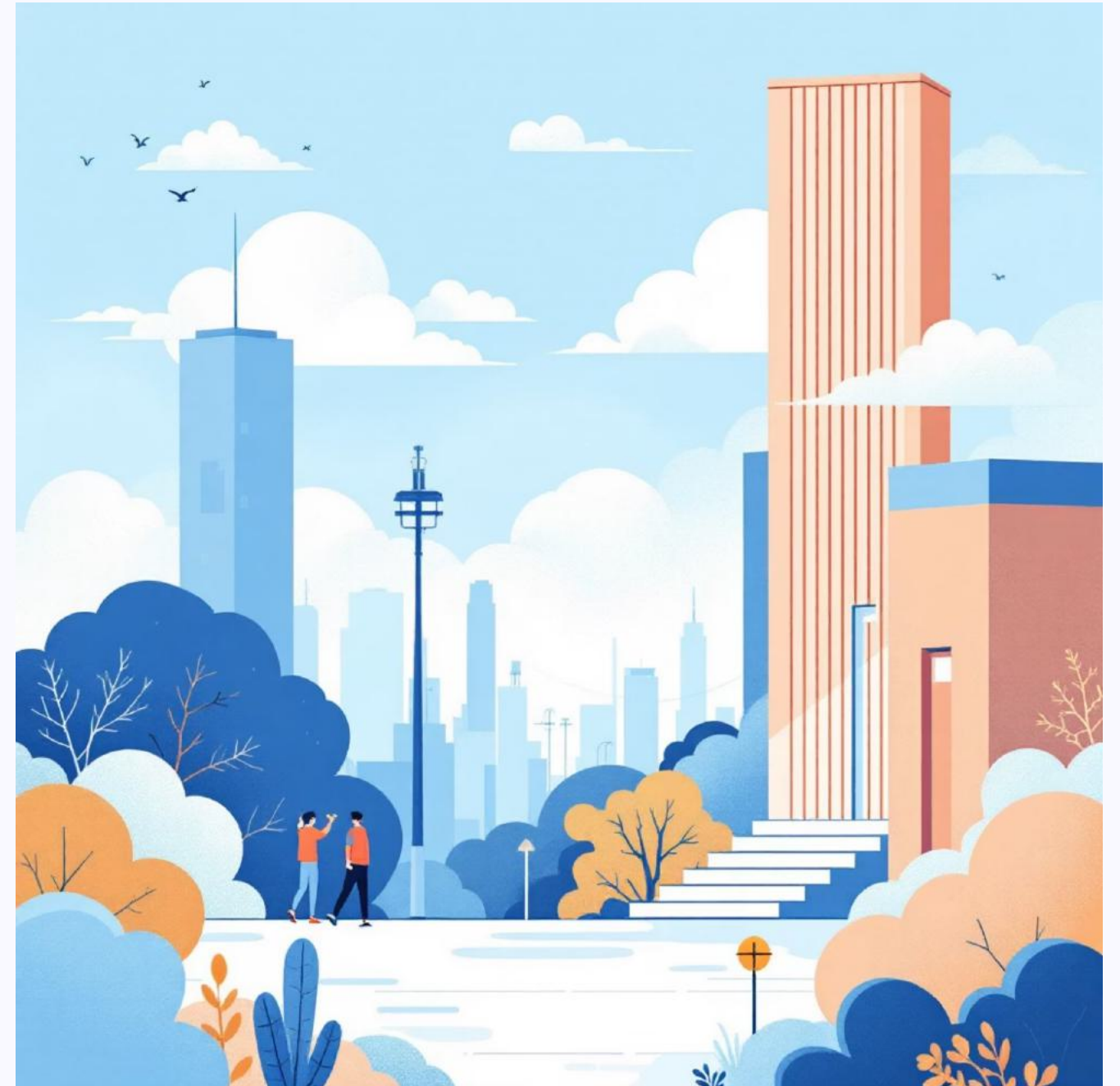
Framework di Riferimento e Standard Applicabili

Normative e Linee Guida Nazionali

- **Art. 24 D.lgs. 138/2024** - Disposizioni italiane NIS2
- **Linee guida ACN** - Alcune già pubblicate, altre in arrivo
- **Framework Nazionale per la Cybersecurity e la Data Protection**
- **GDPR Art. 32** - Obblighi di sicurezza del trattamento

Standard Internazionali

- **ENISA Guidelines** - Agenzia UE per la cybersecurity
- **ISO 27001** - Sicurezza delle informazioni
- **NIST Cybersecurity Framework**
- **ISO 31000** - Gestione del rischio



Integrazione dei Framework

La Questione Temporale: L'Incubo del CISO

Tempistiche Stringenti per la Notifica secondo l'Art. 25

1

Entro 24 Ore

Pre-notifica al CSIRT Italia

Dalla conoscenza dell'incidente: comunicazione iniziale con le informazioni disponibili su cosa è successo, anche se l'analisi è ancora in corso.

2

Su Richiesta

Relazione Intermedia

Il CSIRT può richiedere aggiornamenti progressivi sulla situazione, sull'evoluzione dell'incidente e sulle misure di contenimento adottate.

3

Entro 1 Mese

Relazione Finale Completa

Dalla notifica iniziale: **qui si gioca la partita decisiva**. Deve contenere analisi dettagliata, root cause e misure definitive.

- ❏ **Criticità operativa:** Queste tempistiche rappresentano una sfida significativa per i CISO, richiedendo capacità di analisi forense rapida e accurata, documentazione continua e processi di incident response ben rodati e testati.

Il Nocciolo: La Relazione Finale (Art. 25)

Contenuti Obbligatori e la Domanda da Un Milione di Euro



Descrizione Dettagliata

Analisi completa dell'incidente, specificando con precisione la gravità dell'evento e l'impatto effettivo sui sistemi, sui dati e sulla continuità operativa.



Root Cause Analysis

Identificazione del tipo di minaccia e, soprattutto, della **CAUSA ORIGINALE (ROOT CAUSE)** che ha innescato l'incidente - il vero cuore dell'analisi forense.



Misure di Attenuazione

Descrizione dettagliata delle contromisure già implementate e di quelle ancora in corso di applicazione per prevenire ricorrenze.



Impatto Transfrontaliero

Valutazione e documentazione dell'eventuale impatto su altri Stati membri dell'UE o su organizzazioni internazionali (ove applicabile e noto).

La Domanda da 11 BTC

Come potete identificare con certezza la ROOT CAUSE di un incidente senza condurre un'indagine approfondita di Informatica Forense?

La risposta è semplice: **non potete**. L'informatica forense non è un optional nella compliance NIS2, ma una [necessità tecnica e legale imprescindibile](#) per soddisfare gli obblighi normativi e proteggere efficacemente la vostra organizzazione.