COLIN
CONSULENTE LEGALE INFORMATICO

Sviluppare un modello NIS2 in ottica di multi-compliance

Avv. Valentina Frediani
Founder e CEO Colin & Partners

20 Marzo 2025

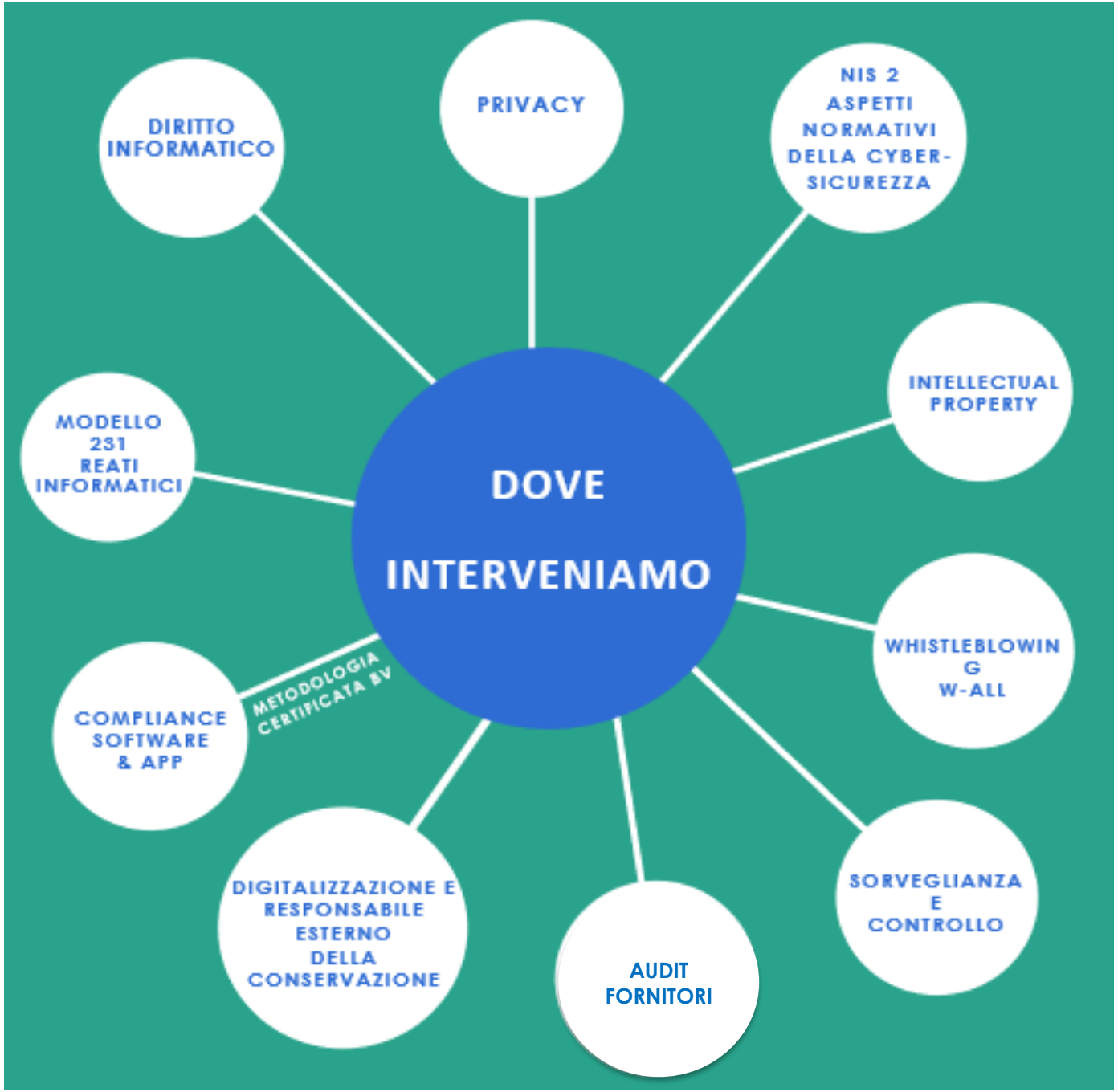
COLIN
CONSULENTE LEGALE INFORMATICO

SOLUZIONI CONTINUATIVE

LAAS
Legal as a Service

ASSISTENZA DATA BREACH
H24

FORMAZIONE



Azioni da intraprendere per l'adeguamento alla NIS2

COLIN
CONSULENTE LEGALE INFORMATICO

Mappatura delle entità coinvolte	• Verifica dell'appartenenza alla categoria di **entità essenziali** o **importanti**. • Identificazione delle **supply chain critiche** che rientrano nell'ambito NIS2.
Valutazione del rischio e piano di cybersecurity	• Implementazione di un **Cyber Risk Assessment Framework**. • Identificazione e mitigazione delle vulnerabilità.
Revisione della governance e responsabilità	• Definizione ruoli (**CISO, DPO e Compliance Officer)**. • Formazione del management sulla **responsabilità diretta**.
Adeguamento delle misure di sicurezza	• Adozione di controlli di sicurezza avanzati. • Integrazione con altre normative (GDPR, D.lgs. 231/2001, AI Act).
Potenziamento della gestione degli incidenti	• Implementazione di un **Incident Response Plan** conforme alle nuove tempistiche di notifica. • Test periodici con **simulazioni di attacchi.**
Monitoraggio e audit	• Implementazione di un **programma di audit periodici** e reportistica per garantire la conformità. • Allineamento con le best practice.
Formazione	• **Formazione e sensibilizzazione sulla cultura della sicurezza** per tutti i dipendenti. • Simulazioni di phishing e attacchi informatici per rafforzare la resilienza.

NIS2 e GDPR

	GDPR	NIS2
Ambito di applicazione	Si applica al trattamento dati personali e coinvolge tutte le organizzazioni.	E' focalizzata sulla cybersecurity di enti ritenuti critici o essenziali per la società e l'economia.
Sicurezza e preservazione da attacchi	Impone misure tecniche e organizzative adeguate per garantire la sicurezza dei dati personali (Art.32).	Introduce obblighi di sicurezza che riguardano l'intero perimetro aziendale.
Obblighi di notifica	Prevede la notifica di data breach all'autorità di controllo entro **72 ore** (art. 33).	Impone la notifica degli incidenti di sicurezza con una tempistica più articolata (prima segnalazione entro 24 ore e notifica dettagliata entro 72 ore).
Sanzioni	GDPR: Fino a **20 milioni di euro o il 4% del fatturato annuo globale.**	Sanzioni fino a **10 milioni di euro o il 2% del fatturato annuo globale** per le entità essenziali e fino a **7 milioni di euro o l'1,4% del fatturato annuo** per le entità importanti.

Ruolo del DPO e del CISO: In aziende soggette a entrambi i regolamenti, il **DPO (Data Protection Officer)** e il **CISO (Chief Information Security Officer)** devono lavorare in stretta collaborazione per garantire sia la protezione dei dati personali che la sicurezza complessiva dei sistemi IT.

Interazione tra NIS2 e D.lgs. 231/2001

COLIN
CONSULENTE LEGALE INFORMATICO

Cybersecurity e Modello 231

La NIS2 impone misure di sicurezza e di governance che potrebbero entrare a far parte dei **modelli organizzativi e di gestione (MOG)** previsti dal D.lgs. 231/2001, specialmente per prevenire reati informatici (art. 24-bis D.lgs. 231).

Ruolo dell'Organismo di Vigilanza (OdV)

L'OdV dovrà monitorare l'adeguatezza delle misure di cybersecurity previste dalla NIS2, per evitare che la mancata attuazione possa configurarsi come colpa organizzativa dell'ente.

Reati informatici e sanzioni

La mancata conformità alla NIS2 potrebbe aumentare il rischio di configurazione della responsabilità ex 231 (es. in caso di attacchi informatici agevolati da carenze nei sistemi di sicurezza).

Doveri del Board

La NIS2 impone agli organi direttivi responsabilità dirette nella gestione della sicurezza, con possibili ripercussioni su profili di colpa grave o negligenza che potrebbero essere rilevanti ai fini della 231.

Interazione tra NIS2 e AI ACT

Cybersecurity e AI: La **NIS2** prescrive misure di sicurezza per la protezione delle infrastrutture critiche e dei sistemi IT, mentre l'**AI Act** impone requisiti stringenti per i sistemi di IA ad alto rischio che devono avere **robuste misure di cybersecurity** per prevenire attacchi o manipolazioni.

Gestione dei rischi: Entrambe le normative richiedono un approccio **basato sul rischio** per l'implementazione delle misure di sicurezza. Nel caso dell'AI Act, questo include la protezione da vulnerabilità che potrebbero essere sfruttate per attacchi informatici.

Obblighi di trasparenza: Le organizzazioni che utilizzano sistemi di IA ad alto rischio devono garantire **audit e documentazione**, così come richiesto dalla NIS2 per garantire la resilienza informatica.

Impatto sulle imprese: Le aziende soggette a **NIS2** potrebbero essere tenute ad adottare misure di sicurezza più stringenti per i sistemi di IA, specialmente se questi vengono utilizzati in infrastrutture critiche o servizi essenziali.

Implicazioni pratiche per le aziende

COLIN
CONSULENTE LEGALE INFORMATICO

Integrazione delle strategie di governance

- Sviluppo di framework unificati per cybersecurity, protezione dati e gestione del rischio.

Sinergia tra funzioni aziendali

- Coordinazione tra IT, Compliance, Legal e Risk Management per prevenire sovrapposizioni o lacune normative.

Aggiornamento delle policy di sicurezza

- Revisione e adeguamento delle misure di sicurezza per incorporare gli obblighi di NIS2 e AI Act, integrandoli con quelli già previsti dal GDPR.

Potenziamento della formazione e della consapevolezza

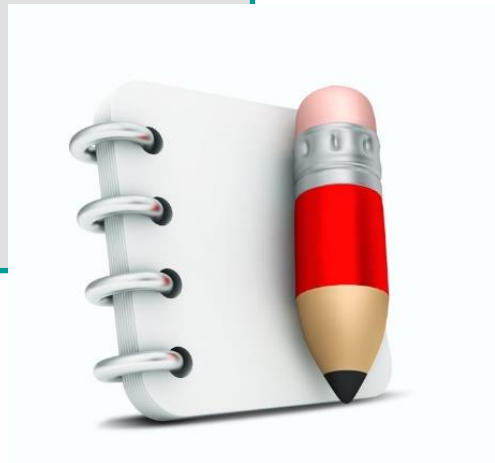
- Coinvolgimento del management e del personale su obblighi e best practice in ambito cybersecurity e protezione dati.

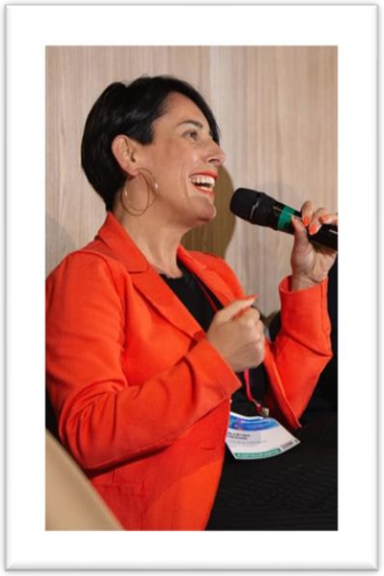
Audit e monitoraggio

- Implementazione di controlli periodici per verificare la conformità a tutte le normative rilevanti.

Consulta le nostre brochure di presentazione dei servizi:

- **NIS2.** Clicca qui.
- **Audit Fornitori**. Clicca qui.
- **Digitalizzare in conformità e tutela**. Clicca qui.
- **W-ALL.** Clicca qui.
- **La gestione del Data Breach.** Clicca qui
- **Compliance applicativi. La metodologia certificata di Colin & Partners.** Clicca qui.
- **Data Protection Officer.** Clicca qui.
- **Catalogo formazione Think Factory.** Per visualizzarlo, clicca qui.
- **Paper Servizi.** Per visualizzarlo, clicca qui





GRAZIE

Avv. Valentina Frediani

vfrediani@consulentelegaleinformatico.it

Linkedin: https://it.linkedin.com/in/vfrediani

Contatti

Sede legale
Via Privata Maria Teresa, 7 – Milano 20123
Tel. +39 0287198390
Sede operativa e amministrativa:
Via Cividale, 51 – Montecatini Terme (PT) 51016
Tel. +39 0572 78166
Fax +39 0572 294540
Sede operativa
Via Del Lavoro, 57 – Casalecchio di Reno (BO) 40033

Partita Iva e Codice Fiscale: 01651060475
Le nostre sedi: Montecatini Terme (PT), Milano
www.consulentelegaleinformatico.it

Per richieste progetti e preventivi:
info@consulentelegaleinformatico.it
Per organizzare eventi:
comunicazione@consulentelegaleinformatico.it
Per organizzare corsi di formazione:
thinkfactory@consulentelegaleinformatico.it

Seguici su: