# Softway e lo Studio Legale Bernardini insieme per supportare le Organizzazioni appartenenti al Perimetro di Sicurezza Nazionale Cibernetica


*Roma e Milano, 18 ottobre 2021*

**Softway Srl** e lo **Studio Legale Avv. Paolo Bernardini** annunciano la partnership finalizzata ad offrire alle organizzazioni inserite nel Perimetro di Sicurezza Nazionale Cibernetica un supporto consulenziale completo, per garantire la conformità a quanto richiesto in merito dalla normativa, sia per gli aspetti tecnologici che per quelli organizzativi richiesti dal D. Lgs.231/01.

Sulla base di questa sinergia siamo in grado di supportare l'Organizzazione, dal momento dello studio architetturale necessario a definire il quadro di attività necessarie, fino alla predisposizione delle misure tecniche, procedurali ed organizzative che saranno state individuate e definite.

**Sommario**

## Il quadro normativo

Il Decreto Legge n.105 del 21.9.2019, convertito con modifiche nella Legge 18.11.2019, n.133 ha istituito il "Perimetro di Sicurezza Nazionale Cibernetica", che prevede una serie di adempimenti da porre in essere al fine di assicurare la sicurezza di reti, sistemi informativi e servizi informatici.

Rientrano nel Perimetro operatori pubblici e privati da cui dipende l'esercizio di una funzione essenziale dello Stato, dal cui malfunzionamento, interruzione, anche parziale, ovvero utilizzo improprio dei sistemi informativi ed informatici, possa derivare un pregiudizio per la sicurezza nazionale.

L'elenco dei soggetti appartenenti al Perimetro è aggiornato con specifico Decreto dal Governo, che non dà pubblicazione dell'atto, ma fornisce comunicazione ai soggetti interessati.

## Gli obblighi

Dal momento in cui il soggetto riceve la comunicazione scattano una serie di obblighi:

- **predisposizione e trasmissione dell'elenco beni ICT critici**;
- **revisione della gestione fornitori e di terze parti;**
- **comunicazione degli incidenti**, entro tempi predefiniti, al Computer Security Incident Response Team (CSIRT);
- **applicazione delle misure di Cyber Security entro 6 mesi.**

Il soggetto che ostacola o condiziona l'espletamento (i) dei procedimenti di predisposizione ed aggiornamento degli elenchi di reti, sistemi informativi e servizi informatici o (ii) della comunicazione al CVCN dell'affidamento di forniture di beni, sistemi e servizi ICT, ovvero ancora delle attività ispettive e di vigilanza da parte della Presidenza del Consiglio dei ministri e del Ministero dello sviluppo economico per quanto di rispettiva competenza è passibile di pesanti sanzioni previste dal D. Lgs. 231/01.

## Le attività

1) **Resilienza**
   - censire gli asset
   - definire una tassonomia degli incidenti
   - individuare i processi critici
   - definirne la priorità
   - analizzare le minacce
   - misurare il livello di rischio
   - analizzare i potenziali impatti
   - predisporre le misure di contenimento
     - organizzative
     - procedurali
     - tecniche

2) **Controllo**
   - revisione della gestione fornitori e di terze parti
   - criteri di definizione della criticità
   - monitoraggio proattivo
   - monitoraggio reattivo
   - segnalazioni degli incidenti al CSIRT nazionale
   - interazione con gli altri soggetti nel perimetro

3) **Capacità di reazione**
   - Approntamento delle procedure per la gestione degli incidenti
   - definizione dell'Incident Response Team
   - definizione della matrice delle responsabilità in caso di incidenti
   - tassonomia degli incidenti
   - analisi delle interdipendenze
   - approntamento del piano di continuità
   - collaborazione col CSIRT nazionale per il contenimento e l'analisi ex post
   - simulazioni periodiche per testare l'efficienza dei piani di continuità.

Allo scopo di evitare di incorrere in responsabilità e di subire le sanzioni previste dal D. Lgs.231/01 è necessario che il soggetto incluso nel perimetro predisponga o, nel caso sia già stato adottato, aggiorni il c.d. "modello di organizzazione, gestione e controllo".

## Le buone pratiche

Il Perimetro Nazionale di Sicurezza Cibernetica definisce le regole per proteggere le infrastrutture ed i servizi critici, ma non introduce metodologie innovative: si muove nel solco delle buone pratiche della Cybersecurity.

Una gran parte delle indicazioni della normativa può essere soddisfatta applicando gli standard più consolidati a livello internazionale quali:

- **ISO 22301** (security and resilience)
- **ISO 31000** (risk management)
- **ISO 27001** (information security)
- **COBIT** (control objectives for information technologies)
- **ITIL** (information technology infrastructure library)

**SOFTWAY Srl**

Softway è un'azienda qualificata nella consulenza, progettazione e realizzazione di progetti informatici legati all'infrastruttura tecnologica e all'integrazione di sistemi e tecnologie. La nostra missione è creare progetti e infrastrutture ad alta tecnologia per consentire alle persone di lavorare al meglio, avere accesso a dati e applicazioni in modo sicuro. La nostra Security and Privacy Business Unit ha una esperienza pluridecennale sulle tematiche di Security Governance e di Policy Compliance.

**Studio Legale Avv. Paolo Bernardini**

Lo Studio Legale dell'Avv. Paolo Bernardini vanta una pluriennale esperienza nella redazione di modelli organizzativi, in applicazione della normativa sulla responsabilità delle società derivante da reato.