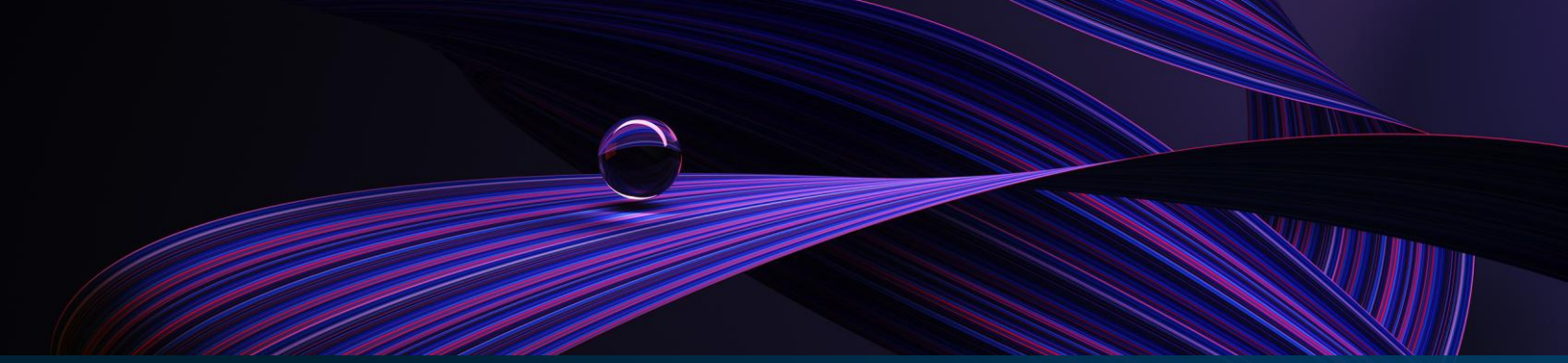


Il Framework Normativo Europeo che eleva il livello di Cybersicurezza e Resilienza

protiviti®
Global Business Consulting

Il panorama normativo europeo si sta evolvendo rapidamente verso un framework sempre più strutturato e integrato per affrontare le sfide della sicurezza digitale. Le principali normative, tra cui il Cybersecurity Act (**CSA**), il Cyber Resilience Act (**CRA**), la Direttiva **NIS2**, il Digital Operational Resilience Act (**DORA**), il Cyber Emergency Response Act (**CER**) e l'Artificial Intelligence Act (**AI Act**), delineano **un approccio completo** e **armonizzato** alla, **protezione delle infrastrutture critiche** alla **sicurezza dei prodotti digitali** e alla **trasparenza dei sistemi di Intelligenza Artificiale.**

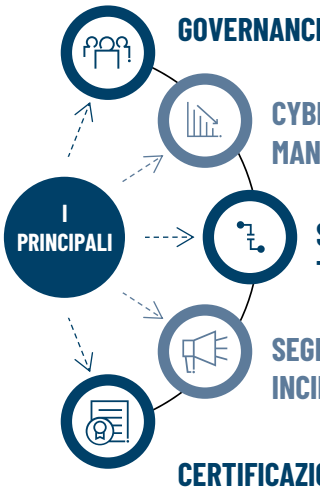
Framework Normativo Europeo

CSA	CRA	AI Act	DORA	CER	NIS2
Certificazione della sicurezza per i prodotti e i servizi ICT, con particolare attenzione alla standardizzazione e all'affidabilità delle soluzioni disponibili sul mercato	Requisiti di cybersicurezza per i dispositivi hardware e software, finalizzati a potenziare la sicurezza dei prodotti digitali connessi a Internet commercializzati nell'UE	Obblighi rivolti a fornitori e utilizzatori di sistemi di Intelligenza Artificiale (AI), con un focus specifico su aspetti di sicurezza e trasparenza	Riguardante esclusivamente i settori finanziario e bancario, prevede garanzie di resilienza operativa e protezione contro le interruzioni operative causate da incidenti cibernetici	Miglioramento della gestione delle crisi e delle risposte agli incidenti informatici a livello europeo, con particolare attenzione alla cooperazione tra le autorità responsabili degli incidenti	Requisiti aggiuntivi di sicurezza per le entità che operano nelle infrastrutture critiche (energia, sanità, trasporti, servizi digitali), includendo obblighi di protezione e segnalazione

Ambito di applicazione

Nel nuovo scenario regolatorio europeo, la resilienza e la sicurezza digitale diventano requisiti imprescindibili per tutti gli operatori del settore. Gli **erogatori di servizi** dovranno assicurare solidi meccanismi di **gestione del rischio** e **risposta agli incidenti**, adottando framework strutturati e architetture moderne. Parallelamente, i **fornitori di prodotti** saranno tenuti a garantire la sicurezza lungo l'intero **ciclo di vita delle soluzioni**, facendo leva su processi **DevSecOps** evoluti e pienamente integrati nelle **pipeline di sviluppo.**

Ambiti di intervento



GOVERNANCE

Approvazione e attuazione da parte degli **organi di gestione delle misure di gestione dei rischi cyber**

CYBER RISK MANAGEMENT

Adozione di **misure tecniche, operative** e **organizzative adeguate a mitigare i rischi** di sicurezza per i sistemi che erogano i servizi critici e per **prevenire o contenere** l'impatto degli incidenti

SICUREZZA TERZE PARTI

Valutazioni coordinate da parte di enti nazionali dei rischi per la sicurezza derivanti da **soggetti coinvolti in catene di approvvigionamento critiche** di servizi, sistemi o prodotti ICT

SEGNALAZIONE INCIDENTI

Notifica al **CSIRT** di **incidenti che hanno un impatto significativo** sulla fornitura di servizi e condivisione degli stessi all'interno del nuovo network di information sharing **EU-Cyclone**

CERTIFICAZIONI

Facoltà da parte degli Stati Membri della UE di imporre ai soggetti in perimetro di utilizzare determinati **prodotti, servizi e processi ICT**, sviluppati da soggetti o acquistati da terze parti **certificati** nell'ambito dei sistemi EU di certificazione

Regime Sanzionatorio

CSA	CRA	AI Act	DORA	CER	NIS2
• Regime sanzionatorio demandato agli Stati	• Fino a 15M€ o 2,5% del fatturato annuo	• Fino a 35M€ o 7% del fatturato per violazioni gravi • 15M€ o 3% per non conformità generali • 7,5M€ o 1,5% per errori di documentazione	• Fino a 10M€ o 5% del fatturato annuo globale	• Da 25k€ fino a 125k€ • Da 10k€ fino a 50k€ per non adempimento entro 30 giorni • Triplicano per reiterazione	• Essenziali: 10M€ o 2% del fatturato • Importanti: 7M€ o 1,4% • Possibile sospensione dei servizi

Il valore di Protiviti

Sulla base della vasta esperienza sviluppata in materia di gestione del rischio e di compliance, con particolare riferimento agli ambiti **Information Technology** e **Cybersecurity**, Protiviti ha definito uno specifico approccio per gestire in maniera efficace e sostenibile l'aderenza al panorama normativo europeo.

Tale approccio è basato su framework metodologici adattati alle specifiche caratteristiche ed esigenze delle singole organizzazioni.

enrico.ferretti@protiviti.com nicola.dallabenetta@protiviti.com raffaele.lambiase@protiviti.com