DPCORE.EU

PRIVACYLAB RIVENDITORE UFFICIALE

RESELLER

FEDERPRIVACY

MEMBRO

PERCHÉ ADEGUARSI ALLA NORMA SULLA SICUREZZA NIS2?

10 Buoni motivi per la compliance alla Direttiva EU NIS2

1	È un **OBBLIGO DI LEGGE** europeo e nazionale ed il mancato adeguamento potrebbe provocare sanzioni ed esclusioni	
2	Rispettare la sicurezza dei dati che si gestiscono rappresenta ormai un **DOVERE PRIMARIO** nei confronti degli interlocutori	
3	I dati raccolti (di vario tipo IT o di fabbrica OT) sono **IL VALORE DELL'AZIENDA** e vanno per prima cosa tutelati e poi valorizzati per applicare nuovi metodi di analisi, per es. con Big Data e l'AI	
4	Chi deve fare la NIS2? "Grandi imprese >250 add. e >€ 50Mil." o "medie <250 add. e tra €10 e 50Mil." dei **settori ESSENZIALI** (es. Sanità, Energia, Finanza, Trasporti, ICT, Infrastr. digitali, Spazio)	
5	Oltre agli essenziali, sono stati aggiunti **MOLTI ALTRI SETTORI "IMPORTANTI"** (Servizi postali, Rifiuti, Chimica, Manifattura, Alimentare, PA), oltre che **AZIENDE** di importanza nazionale*	
6	Sono coinvolte tutte le **aziende della SUPPLY CHAIN**, quindi tutte le aziende che agiscono come fornitori o partner di settori essenziali o di settori importanti (il perimetro diventa ampio)	
7	Sono sempre frequenti le richieste di compilare **QUESTIONARI DI AUDIT** sulla **SICUREZZA** da parte di Clienti, Fornitori, ecc. con il rischio di essere esclusi dall'albo fornitori o da bandi gara	
8	Con la **GESTIONE DEI RISCHI** e la **RESILIENZA OPERATIVA** verranno evidenziate le vulnerabilità dell'area IT/OT e come assicurare continuità anche in caso di attacchi informatici	
9	La NIS2 contribuisce a **PROTEGGERE I DATI PERSONALI** degli utenti, riducendo il rischio di violazioni dei dati personali e delle potenziali frodi informatiche anche basate sull'uso di AI	
10	Con la NIS2 la vostra organizzazione acquisisce **MAGGIOR VALORE** sul mercato per i vostri clienti, per gli azionisti e per l'intero vostro ecosistema	

* Il perimetro effettivo dei settori non è stato ancora definito con estremo dettaglio

DPCORE.EU

PRIVACYLAB RIVENDITORE UFFICIALE
RESELLER

FEDERPRIVACY
MEMBRO

QUALI SONO I PASSI CHE SI DEVONO REALIZZARE?

	**<u>Quali sono gli adempimenti da implementare per Vostra organizzazione?</u>** **a)** Un documento sulla **politica della sicurezza IT** con definizione dei ruoli
	**b)** Una verifica sulla **sicurezza delle risorse umane**, strategie di controllo dell'accesso e **gestione degli attivi e degli archivi** (specie se in cloud)
	**c)** Un'**analisi dei rischi** ed una revisione delle attuali misure di sicurezza adottate
	**d)** Una verifica dei sistemi di sicurezza e delle procedure per la **gestione degli incidenti**
	**e)** Una strategia sulla **Continuità operativa**, come la gestione del **backup** e il ripristino in caso di disastro, DR (**Disaster Recovery)** e gestione delle crisi
	**f)** Pratiche di igiene informatica di base e **formazione** a livello di intera organizzazione **in materia di Cybersicurezza** **g) formazione** a tutta l'organizzazione **sulla Data Protection**
	**h)** Uso di soluzioni di **autenticazione a più fattori** e politiche e procedure relative all'uso della **crittografia** e, se del caso, della **cifratura**
	**i)** Strategie e procedure per **valutare l'efficacia delle misure di gestione** dei rischi di cybersicurezza (es. **penetration test** ed **analisi delle vulnerabilità**)
	**j) Sicurezza dell'acquisizione, dello sviluppo e della manutenzione** dei sistemi informatici e di rete
	**k) Sicurezza della catena di approvvigionamento**, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi
	Le **sanzioni amministrative pecuniarie** previste possono arrivare ad un importo massimo di 7 milioni (settori importanti) o 10 milioni (essenziali) di euro o dall'1,4% (settori importanti) al 2% del fatturato totale annuo lordo