CMV GROUP

SECURITY & SOFTWARE ENGINEERING

CHECKLIST OPERATIVA
NIS2 FOR BUSINESS

Guida pratica all’adeguamento dell’infrastruttura IT per le PMI

Strumento di autovalutazione e pianificazione tecnica basato sui requisiti della Direttiva (UE) 2022/2555.

Come utilizzare questo documento

La Direttiva NIS2 trasforma la sicurezza informatica da semplice requisito tecnico a pilastro della governance aziendale. Per molte PMI, il percorso di adeguamento rappresenta un passaggio fondamentale per garantire la continuità del business e proteggere il proprio valore di mercato.

Questa checklist è stata strutturata dagli ingegneri di **CMV Group** come strumento operativo interno. Permette di:

01	**Mappare lo stato dell'arte** della tua infrastruttura IT.
02	**Individuare le lacune prioritarie** (Gap Analysis).
03	**Tracciare i progressi** verso la piena conformità.

Il documento è organizzato in **5 aree tecniche** di conformità, ciascuna con requisiti operativi puntuali e la relativa azione richiesta per l’adeguamento.

AREA 1 — GOVERNANCE E ANALISI DEL RISCHIO

	Requisito Operativo	Azione Richiesta
☐	**Valutazione periodica del rischio (Risk Assessment)**	Mappatura completa degli asset aziendali, dei flussi di dati critici e dei potenziali vettori di attacco.
☐	**Coinvolgimento e formazione del Management**	Formalizzazione delle responsabilità del CDA/Direzione e pianificazione di sessioni formative sui rischi cyber.
☐	**Policy di Sicurezza delle Informazioni**	Adozione e diffusione di procedure scritte sulla gestione delle credenziali, dell'hardware e dell'accesso ai dati.

AREA 2 — PROTEZIONE DELL'INFRASTRUTTURA E CONTROLLO ACCESSI

	Requisito Operativo	Azione Richiesta
☐	**Autenticazione a Più Fattori (MFA)**	Abilitazione obbligatoria dell'MFA su tutti gli accessi aziendali (e-mail, VPN, portali interni, gestionale).
☐	**Principio del Minimo Privilegio (RBAC)**	Configurazione degli accessi basata esclusivamente sui ruoli operativi, con revoca immediata dei permessi superflui.
☐	**Crittografia dei dati**	Protezione attiva dei dati archiviati (data at rest) e dei flussi di trasmissione in rete (data in transit).
☐	**Gestione delle Vulnerabilità e Patch Management**	Processo automatizzato e programmato per l'aggiornamento costante dei sistemi operativi e del software applicativo.

AREA 3 — BUSINESS CONTINUITY E DISASTER RECOVERY

	Requisito Operativo	Azione Richiesta
☐	**Backup ridondati e isolati (Air-Gapped / Immutabili)**	Implementazione della regola 3-2-1 per i backup, con almeno una copia isolata e protetta da cifratura o ransomware.
☐	**Piano di Disaster Recovery (DRP)**	Definizione formalizzata dei tempi di ripristino operativi (RTO e RPO) per ogni sistema critico aziendale.
☐	**Test periodici di ripristino**	Esecuzione di simulazioni pratiche di disaster recovery con cadenza almeno semestrale.

AREA 4 — MONITORAGGIO E GESTIONE DEGLI INCIDENTI

	Requisito Operativo	Azione Richiesta
☐	**Log Management e Monitoraggio di Rete**	Centralizzazione e conservazione sicura dei log di sistema per identificare tempestivamente le anomalie.
☐	**Procedura di Incident Response**	Definizione della catena di comando e delle azioni da intraprendere in caso di violazione accertata dei dati.
☐	**Gestione delle notifiche entro 24h**	Predisposizione del flusso per la segnalazione preventiva dell'incidente grave all'autorità competente (ACN).

AREA 5 — SICUREZZA DELLA SUPPLY CHAIN

	Requisito Operativo	Azione Richiesta
☐	**Mappatura dei fornitori IT e terze parti**	Censimento di tutti i software in licenza, servizi cloud e consulenti esterni con accesso alla rete aziendale.
☐	**Valutazione della sicurezza dei fornitori**	Verifica formale delle misure di sicurezza adottate dalla catena di fornitura tecnica e vincoli contrattuali adeguati.

Note Operative e Prossimi Passi

Matrice di priorità dei lavori

Utilizza questo spazio per annotare le criticità emerse dalla checklist e stabilire le priorità di intervento sui tuoi sistemi.

🔴	**Priorità Alta (Bloccante)**	
🟡	**Priorità Media (Da pianificare)**	
🟢	**Priorità Bassa (Ottimizzazione)**	

Piani di azione con CMV Group

Inadeguatezze e vulnerabilità infrastrutturali richiedono un approccio ingegneristico rigoroso. CMV Group affianca le aziende nell'analisi del debito tecnologico, nella protezione dei sistemi esistenti e nello sviluppo di software custom conformi ai principi di *Security by Design*.

Prenota una sessione tecnica di orientamento per la tua infrastruttura IT

Sito Web www.cmvgroup.com
E-mail info@cmvgroup.com
Sede Italia