Ambito	Categoria	Articolo del dlgs 138	Requisito	Azione/misura	Descrizione	Responsabile	Evidenza/documenti
POLITICA DI SICUREZZA	**Policy di Sicurezza**	Art. 24 co. 2 a	Le misure di sicurezza dei sistemi informativi e di rete devono comprendere una politica di sicurezza.	Definire e approvare una Politica di Sicurezza Informatica	Redigere una Politica di Sicurezza (ambito, principi, ruoli, regole e processo di revisione) e diffonderla internamente.	CISO/IT Security (redazione), CdA/AD (approvazione)	Politica di Sicurezza formalizzata; verbale di approvazione; comunicazione interna; registro revisioni
RESPONSABILITA'	**Organi di Amministrazione e Organi Direttivi**	Art. 23 co. 1 a Art. 23 co. 1 b Art. 23 co. 1 c	Approvano le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica adottate e sovrintendono alla loro implementazione Sovrintendono all'impementazione degli obblighi di registrazione Sono responsabili delle violazioni al decreto NIS2.	Gestire la governance NIS2 e supervisionare conformità	Approvare l'implementazione delle misure di gestione del rischio e vigilare sulla registrazione/adempimenti NIS2; assicurare reporting e accountability.	CdA/AD/Direzione Generale	Verbali CdA/AD; report periodici di conformità; deleghe/nomine; evidenze della supervisione
RISORSE UMANE	**Formazione Top Management**	Art. 23 co. 2a	Gli organi di amministrazione e gli organi direttivi sono tenuti a seguire una formazione in materia di sicurezza informatica.	Formare periodicamente CdA e Alta Direzione	Erogare formazione specifica per organi di amministrazione / direttvi su rischio cyber, obblighi NIS2, decisioni e responsabilità.	CdA/AD (partecipazione), CISO/Compliance (organizzazione)	Agenda e materiale formativo; attestati; registro partecipazione; verbale presa visione
RISORSE UMANE	**Formazione del Personale**	Art. 24 co. 2 g	Le misure di sicurezza dei sistemi informativi e di rete devono comprendere pratiche di formazione in materia di sicurezza informatica.	Istituire un programma di formazione cyber per il personale	Definire e attuare formazione periodica su minacce, policy e comportamenti sicuri per tutto il personale.	CdA/AD (sponsorship), HR (coordinamento), CISO/IT Security (contenuti)	Piano formativo; materiali; registro presenze; test/verifiche; attestati
RISORSE UMANE	**Sicurezza risorse umane**	Art. 24 co. 2 i	Le misure di sicurezza dei sistemi informativi e di rete devono comprendere la sicurezza e affidabilità del personale.	Rafforzare sicurezza e affidabilità del personale	Implementare controlli e procedure HR: onboarding/offboarding, gestione privilegi, accordi di confidenzialità e riservatezza, verifiche di affidabilità per ruoli sensibili.	HR + CISO/IT Security + Legal/Compliance	Procedure HR security; accordi di confidenzialità e riservatezza; checklist onboarding/offboarding; registro autorizzazioni e revoche
IGIENE INFORMATICA DI BASE	**Igiene Informatica di Base**	Art. 24 co. 2 g	Le misure di sicurezza dei sistemi informativi e di rete devono comprendere pratiche di igiene di base in materia di sicurezza informatica.	Applicare pratiche di igiene cyber di base	Implementare e far rispettare misure di base (patching, antivirus/EDR, configurazioni sicure, awareness phishing, gestione password/dispositivi).	IT Operations + CISO/IT Security	Procedure, regoamento utenti, report patch, copertura EDR/AV, campagne phishing; evidenze hardening
ACCESSO AL SISTEMA INFORMATIVO	**Controllo Accessi**	Art. 24 co. 2 i	Le misure di sicurezza dei sistemi informativi e di rete devono comprendere politiche di controllo dell'accesso.	Definire e applicare procedure di controllo accessi	Stabilire regole di accesso (least privilege, segregazione, ecc.), provisioning/deprovisioning e revisioni periodiche delle utenze.	CISO/IT Security + IT Operations (IAM)	Procedure controllo accessi, matrice ruoli, log IAM, report revisione accessi; evidenze revoche
RISK MANAGEMENT	**Analisi dei rischi**	Art. 24 co. 2 a	Le misure di sicurezza dei sistemi informativi e di rete devono comprendere una politica di analisi dei rischi.	Definire politica di analisi dei rischi cyber	Formalizzare metodologia, frequenza e responsabilità per la valutazione dei rischi dei sistemi informativi e di rete.	Risk Manager + CISO/IT Security (redazione), CdA/AD (approvazione)	Politica di analisi dei rischi ; registro rischi; criteri di scoring; verbale approvazione

RISK MANAGEMENT	**Analisi dei rischi**	Art. 24 co. 1 a Art. 24 co. 1 b	Le misure di sicurezza adottate: - Assicurano un livello di Sicurezza adeguato ai rischi esistenti... - Sono proporzionate al grado di esposizione ai rischi del soggetto, alle dimensioni del soggetto e alla probabilità che si verifichino incidenti, nonché alla loro gravità, compreso il loro impatto sociale ed economico....	Adottare misure proporzionate e risk-based	Assicurare che le misure siano adeguate ai rischi e proporzionate a esposizione, dimensioni e impatti (sociali/economici), con prioritizzazione e riesame.	CdA/AD + Risk Management + CISO/IT Security	Risk appetite; piano trattamento rischi; matrice priorità; riesami periodici
RISK MANAGEMENT	**Analisi dei rischi**	Art. 24 co. 2 f	Le misure di sicurezza dei sistemi informativi e di rete devono comprendere politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica.	Valutare efficacia delle misure di sicurezza	Definire KPI/KRI, audit e test (es. vulnerability scan, esercitazioni) per misurare l'efficacia delle misure di gestione del rischio e avviare azioni correttive.	CISO/IT Security + Internal Audit/Compliance	Dashboard KPI; report audit/test; piani di remediation; verbali riesame
INCIDENT MANAGEMENT	**Gestione degli incidenti**	Art. 24 co. 2 b	Le misure di sicurezza dei sistemi informativi e di rete devono comprendere la gestione degli incidenti ivi incluse le procedure e gli strumenti per eseguire le notifiche richieste.	Implementare Incident Management e strumenti di notifica	Definire processo di gestione incidenti (rilevazione, analisi, contenimento, recovery) includendo strumenti e procedure per le notifiche obbligatorie.	CISO/SOC (gestione), PdC e Referente CSIRT (notifiche), IT Ops (supporto)	Incident Response Plan; playbook; ticket/registro incidenti; procedure notifica; evidenze esercitazioni
INCIDENT MANAGEMENT	**Notifica incidenti**	Art. 23 co. 3	Gli organi di amministrazione e gli organi direttivi sono informati su base periodica o, se opportuno, tempestivamente, degli incidenti significativi e delle relative notifiche.	Assicurare reporting al management su incidenti e notifiche	Stabilire flussi di escalation e reporting (periodico e ad evento) verso organi di amministrazione / direttivi su incidenti significativi e notifiche effettuate.	CISO + PdC e Referente CSIRT	Report periodici; verbali; procedura escalation; log comunicazioni
INCIDENT MANAGEMENT	**Notifica incidenti**	Art. 25	Devono essere previste notifiche tempestive al CSIRT per incidenti significativi che impattano la fornitura dei Servizi.	Notificare tempestivamente incidenti significativi al CSIRT	Definire e attuare un processo per notifiche tempestive al CSIRT/ACN degli incidenti significativi che impattano i servizi, con ruoli e tempistiche.	PdC e Referente CSIRT (invio), Incident Manager/CISO (contenuti)	Procedura notifica; template; ricevute portale ACN / CSIRT; registro notifiche
CONTINUITA' OPERATIVA	**Backup/Ripristino**	Art. 24 co. 2 c	Le misure di sicurezza dei sistemi informativi e di rete devono comprendere misure per il backup.	Implementare backup sicuri e test di ripristino	Eseguire backup regolari dei dati/configurazioni, proteggere e segregare i backup e testare periodicamente i ripristini.	IT Operations + BC/DR Manager	Procedura backup; job/log backup; evidenze segregazione/offline; report test di restore
CONTINUITA' OPERATIVA	**DRP**	Art. 24 co. 2 c	Le misure di sicurezza dei sistemi informativi e di rete devono comprendere il ripristino in caso di disastro.	Implementare e testare soluzioni di Disaster Recovery	Predisporre DRP con RTO/RPO, ruoli e procedure; eseguire test periodici e miglioramenti.	BC/DR Manager + IT Operations, CdA/AD (approvazione)	DRP; risultati test DR; RTO/RPO; verbali approvazione e riesame
COMUNICAZIONE	**Sistemi di comunicazione**	Art. 24 co. 2 l	Le misure di sicurezza dei sistemi informativi e di rete devono comprendere l'uso di comunicazioni vocali, video e di testo protette	Adottare comunicazioni protette (voce/video/testo)	Selezionare e configurare strumenti di comunicazione sicuri per scambi operativi e gestione incidenti (cifratura, controllo accessi).	IT Security + IT Operations	Elenco strumenti approvati; configurazioni; procedure uso; evidenze cifratura

COMUNICAZIONE	**Sistemi di comunicazione**	Art. 24 co. 2 l	Devono essere predisposti sistemi di comunicazione di emergenza protetti al proprio interno, ove opportuno	Predisporre comunicazioni di emergenza protette (interno)	Implementare canali di comunicazione di emergenza protetti (out-of-band) per uso interno, ove opportuno, e testarli.	Crisis/BC Manager + IT Security	Piano comunicazioni d'emergenza; liste contatti; evidenze test; procedure attivazione
SICUREZZA DEL SISTEMA INFORMATIVO E DELLE RETI	**Acquisizione, Sviluppo e Manutenzione**	Art. 24 co. 2 e	Le misure di sicurezza dei sistemi informativi e di rete devono comprendere la sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete.	Assicurare sicurezza in acquisizione/sviluppo/manutenzione	Integrare requisiti di sicurezza in procurement, sviluppo e manutenzione (secure-by-design, change management, patching, code review).	IT Engineering/Development + CISO + Procurement	Secure Development Life Cycle SDLC; requisiti di gara/contratto; change log; evidenze code review
SICUREZZA DEL SISTEMA INFORMATIVO E DELLE RETI	**Sicurezza delle reti**	Art. 24 co. 2 e	Le misure di sicurezza dei sistemi informativi e di rete devono comprendere la sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete.	Rafforzare sicurezza delle reti e manutenzione	Applicare controlli di sicurezza di rete (segmentazione, hardening, firewalling, monitoraggio) e manutenzione sicura delle componenti di rete.	IT Operations + IT Security	Schema architettura rete; regole firewall; configurazioni hardening; report monitoraggio/scansioni
SICUREZZA DEL SISTEMA INFORMATIVO E DELLE RETI	**Gestione Asset**	Art. 24 co. 2 i	Le misure di sicurezza dei sistemi informativi e di rete devono comprendere politiche di gestione dei beni e degli assetti	Gestire beni e asset (asset management)	Definire procedure e processi di inventario, classificazione e ciclo di vita degli asset (HW/SW/dati) rilevanti per i servizi IT.	IT Manager + CISO/IT Security	Inventario; classificazione asset; procedure lifecycle; report aggiornamenti
SICUREZZA DEL SISTEMA INFORMATIVO E DELLE RETI	**Gestione delle Vulnerabilità**	Art. 24 co. 2 e	Le misure di sicurezza dei sistemi informativi e di rete devono comprendere la gestione e la divulgazione delle vulnerabilità.	Gestire e divulgare le vulnerabilità	Istituire processo di vulnerability management end-to-end (identificazione, valutazione, remediation, disclosure coordinata) e tracciamento delle azioni.	CISO	Procedura di vulnerability management; report scansioni; priano di remediation; SLA patching
CRITTOGRAFIA	**Crittografia e cifratura**	Art. 24 co. 2 h	Le misure di sicurezza dei sistemi informativi e di rete devono comprendere politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura.	Definire politica di crittografia e cifratura	Stabilire algoritmi/standard, gestione chiavi, cifratura in transito e a riposo dove opportuno, e controlli di conformità.	CISO/IT Security + DPO (per dati personali) + IT Ops	Procedura crittografia e cifratura; inventario chiavi; configurazioni; evidenze key management
FORNITORI IT	**Catena di approvvigionamento**	Art. 24 co. 2 d	Le misure di sicurezza dei sistemi informativi e di rete devono comprendere la sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti con i diretti fornitori o i fornitori di servizi.	Gestire sicurezza della supply chain	Valutare e trattare i rischi dei fornitori (diretti e di servizi), includere requisiti di sicurezza e obblighi di notifica/audit nei contratti, monitorare nel tempo.	Procurement + CISO/IT Security + Legal/Compliance	Registro fornitori critici; valutazioni rischio; clausole contrattuali; report audit/monitoraggio; registro incidenti fornitori