Politica NIS2 del Gruppo Diagram

Identificazione:

Tipo	Politica di Gruppo (Classe 2)		
Visibilità	☐ Riservato	☐ Interno	☑ Pubblico
Stato	☐ In lavorazione	☐ Bozza	☑Pubblicato

Approvazioni:

Attività	**Nome**	**Data**
Approvato da	Francesca Gusti	22/07/2026
Pubblicato da	Gloria Ghilardi	22/07/2026

Revisioni:

Rev.	Data	Causale	Redazione RGQ	Approvazione DIR
0	22/07/2026	Prima uscita	22/07/2026	22/07/2026

Sommario

1. Scopo e ambito di applicazione 5
1.1 Obiettivi della politica 5
1.2 Definizioni e terminologia rilevante 5
1.3 Ambito di applicazione 5
1.4 Distinzione tra Soggetti Essenziali e Soggetti Importanti 5
2. Quadro normativo e riferimenti 5
2.1 D.lgs. 138/2024 – recepimento NIS2 5
2.2 Altri riferimenti normativi 5
3. Governance e responsabilità 6
3.1 Organi aziendali e ruoli 6
3.2 Nomina del soggetto responsabile NIS2 7
3.3 Coordinamento interno e responsabilità trasversali 7
3.4 Catena di responsabilità verso fornitori e subfornitori 8
4. Analisi del rischio e gestione del rischio 9
4.1 Metodo di analisi del rischio: identificazione, valutazione e trattamento 9
4.2 Criteri per l'accettazione del rischio residuo 10
4.3 Revisione periodica e aggiornamento del rischio 10
4.4 Valutazione della catena di fornitura – terze parti 10
5. Misure tecniche e organizzative di sicurezza 12
5.1 Controlli di accesso e gestione degli account 12
5.2 Crittografia e protezione dei dati 12
5.3 Monitoraggio, logging e audit dei sistemi 12
5.4 Gestione delle vulnerabilità e patch management 12
5.5 Backup, resilienza e continuità operativa 13
5.1 Segmentazione di rete, difesa perimetrale e Sicurezza fisica e ambientale 13
5.2 Difesa contro malware / attacchi avanzati 14
5.3 Gestione delle modifiche e configurazioni (change management) 14
6. Notifica e gestione degli incidenti di sicurezza 14

6.1 Definizione di incidente significativo (criteri) 15
6.2 Processo interno di rilevazione, risposta e mitigazione 15
6.3 Flussi di notifica verso ACN e autorità competenti 15
6.4 Comunicazioni esterne e reporting 15
6.5 Registro degli incidenti e analisi post evento 16
7. Continuità operativa e ripristino 16
7.1 Piano di continuità / disaster recovery 16
7.2 Procedure di recupero e ripristino 16
7.3 Test periodici e simulazioni 17
7.4 Integrazione con business continuity aziendale 17
8. Formazione, consapevolezza e cultura della sicurezza 17
8.1 Programmi di formazione e sensibilizzazione 17
8.2 Simulazioni ed esercitazioni 18
8.3 Ruoli con obbligo formativo specifico 18
9. Valutazione, audit interno e conformità 18
9.1 Audit interni di conformità NIS2 18
9.2 Verifiche esterne e audit di terza parte 19
9.3 Monitoraggio continuo e indicatori KPI 19
9.4 Reporting interno alla Direzione 19
10. Supervisione, ispezioni e controlli da parte delle autorità 19
10.1 Collaborazione con le autorità competenti 19
10.2 Modalità di ispezione e accertamento 20
10.3 Gestione delle non conformità e piani correttivi 20
10.4 Sanzioni e responsabilità 20
11. Revisione e aggiornamento della politica 20
11.1 Frequenza e modalità di revisione 21
11.2 Circostanze che determinano una revisione straordinaria 21
11.3 Versionamento e approvazione 21
12. Allegati e riferimenti tecnici 21
12.1 Elenco misure e requisiti secondo Allegato 1 / Allegato 2 21

12.2 Documentazione correlata 21

1. Scopo e ambito di applicazione

1.1 Obiettivi della politica

La presente Politica sulla applicazione della normativa NIS2 (di seguito "Politica") stabilisce principi, requisiti e responsabilità volti a garantire un elevato livello di sicurezza informatica e resilienza operativa all'interno delle società del Gruppo Diagram classificate come soggetti importanti ai sensi della Direttiva (UE) 2022/2555 (NIS2) e del D.lgs. 138/2024. Le società del gruppo sono certificate ISO/IEC 27001 e hanno già adottato un Sistema di Gestione della Sicurezza delle Informazioni (ISMS) completo di Policy di Sicurezza ISO/IEC 27001. La Politica integra tali controlli con i requisiti NIS2 relativi alla gestione del rischio, resilienza dei servizi e gestione degli incidenti.

1.2 Definizioni e terminologia rilevante

Incidente: evento che compromette o può compromettere disponibilità, integrità, autenticità o riservatezza di reti, sistemi o dati.
Sistema informativo: infrastrutture hardware e software, reti, dati, applicazioni e procedure aziendali.
Rischio: combinazione di probabilità e impatto di una minaccia su una vulnerabilità.
Misure tecniche e organizzative: controlli di sicurezza adottati in linea con NIS2 e ISO/IEC 27001.

1.3 Ambito di applicazione

La Politica si applica al personale, ai collaboratori, ai consulenti e alle terze parti che accedono ai sistemi delle aziende del Gruppo Diagram ritenute Soggetti Importanti secondo la normativa NIS2.
Include tutte le infrastrutture ICT, on-premises e cloud, e tutti i servizi rilevanti per gli obblighi previsti per i soggetti importanti. La Politica si integra con l'ISMS ISO/IEC 27001 già implementato.
Dall'ambito di applicazione di questa politica è esclusa Agroconsulting Spa e tutte le aziende da essa controllate in quanto non sopposte a direzione e controllo di Diagram Spa.

1.4 Distinzione tra Soggetti Essenziali e Soggetti Importanti

La NIS2 distingue soggetti essenziali e soggetti importanti. Attualmente, all'interno del Gruppo Diagram, le società classificate come soggetti importanti al momento della pubblicazione della presente politica sono: Diagram S.p.A. e Abaco S.p.A., entrambe dotate di un Sistema di Gestione ISO/IEC 27001 certificato.

2. Quadro normativo e riferimenti

2.1 D.lgs. 138/2024 – recepimento NIS2

La Politica è conforme al D.lgs. 138/2024, che recepisce la Direttiva (UE) 2022/2555 e definisce obblighi di gestione del rischio, misure di sicurezza, classificazione e notifica degli incidenti per i soggetti importanti.

2.2 Altri riferimenti normativi

- Regolamento (UE) 2016/679 – GDPR.
- Normative europee e nazionali su resilienza operativa e sicurezza ICT.
- Standard ISO/IEC 27001 e ISO/IEC 27002, adottati dal Gruppo Diagram.
- Policy interne del Sistema di Gestione ISO/IEC 27001.
- Procedure operative relative ad accessi, incidenti, continuità e fornitori.

3. Governance e responsabilità

Il Gruppo Diagram adotta un modello di governance della cybersicurezza fondato sulla chiara attribuzione di ruoli, responsabilità, poteri decisionali e flussi informativi tra gli organi societari, la Direzione aziendale e le funzioni tecniche, legali, di compliance, privacy e di controllo. Il modello è applicato a livello di Gruppo secondo criteri comuni, fermo restando che ciascuna società rientrante nell'ambito di applicazione della normativa NIS2 conserva la responsabilità degli adempimenti a essa direttamente riferibili.
Le nomine e le deleghe in materia di sicurezza delle informazioni e cybersicurezza sono formalizzate dalla Direzione e, quando richiesto dalla normativa, dall'assetto societario o dal contenuto dei poteri attribuiti, sono sottoposte all'approvazione o alla presa d'atto del competente Consiglio di Amministrazione. Le nomine sono riesaminate almeno annualmente e ogniqualvolta intervengano modifiche normative, organizzative, tecnologiche o del perimetro dei servizi rilevanti.

3.1 Organi aziendali e ruoli

Il **Consiglio di Amministrazione** e gli altri organi amministrativi e direttivi competenti approvano le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica, sovrintendono all'attuazione degli obblighi NIS2 e ricevono, periodicamente o tempestivamente in relazione alla gravità dell'evento, informazioni sui rischi, sugli incidenti, sulle vulnerabilità rilevanti e sulle notifiche effettuate alle autorità. Le nomine operative e le deleghe interne non comportano il trasferimento delle responsabilità attribuite dalla normativa agli organi di amministrazione e direttivi.

La **Direzione aziendale** assicura l'attuazione degli indirizzi definiti dagli organi amministrativi, mette a disposizione risorse umane, tecniche ed economiche adeguate, approva procedure e piani operativi e verifica che le funzioni coinvolte dispongano di competenze, autorità e accesso alle informazioni necessari allo svolgimento dei rispettivi incarichi.
La funzione di **gestione dei rischi**, anche quando non attribuita a un autonomo Risk Officer, assicura che il rischio cyber sia identificato, valutato, trattato, monitorato e integrato nel sistema complessivo di gestione dei rischi aziendali. Tale attività è svolta in coordinamento con il Cyber Legal & Compliance Officer, il Responsabile della Sicurezza delle Informazioni/Cyber Security Manager, la Direzione e le funzioni titolari dei processi e dei servizi interessati.
Il **Responsabile della Sicurezza delle Informazioni e Cyber Security Manager**, che ai fini della presente Policy svolge il presidio organizzativo e tecnico normalmente attribuito al CISO, coordina il sistema di gestione della sicurezza delle informazioni, supporta la valutazione dei rischi cyber e sovrintende all'adozione delle misure tecniche, operative e organizzative. In caso di incidente o crisi, valuta l'attivazione e provvede alla convocazione del Comitato di crisi, coordina le attività tecniche di contenimento, ripristino e raccolta delle evidenze e assicura il tempestivo coinvolgimento delle altre funzioni competenti. Il Cyber Security Manager può delegare specifiche attività operative ai Responsabili interni della sicurezza delle informazioni – RISI, ferma restando la propria funzione di coordinamento.
Il Cyber Legal & Compliance Officer, con riporto funzionale all'Organo amministrativo e in raccordo con l'Organismo di Vigilanza, presidia gli aspetti normativi, legali e di conformità relativi alla cybersicurezza e alla sicurezza delle informazioni. Supporta gli organi societari nell'interpretazione degli obblighi applicabili, coordina l'aggiornamento della documentazione NIS2, verifica la coerenza

delle deleghe e dei flussi informativi e collabora alla valutazione delle conseguenze legali, contrattuali e reputazionali degli incidenti.
Il **Data Protection Officer – DPO** svolge i compiti attribuitigli dalla normativa in materia di protezione dei dati personali ed è coinvolto quando un rischio, una vulnerabilità o un incidente di sicurezza possa interessare dati personali. Il **Focal Point Privacy**, designato a livello di Gruppo, facilita il raccordo tra le società del Gruppo e i rispettivi DPO, assicurando la tempestiva circolazione delle informazioni rilevanti. La funzione del DPO rimane distinta dalle responsabilità operative del Cyber Security Manager e dalle responsabilità decisionali degli organi societari.

3.2 Nomina del soggetto responsabile NIS2

Ai fini della presente Policy, l'espressione "**soggetto responsabile NIS2**" identifica il presidio interno di coordinamento degli adempimenti NIS2 e non determina il trasferimento delle responsabilità attribuite dalla legge agli organi di amministrazione e direttivi.
Il coordinamento complessivo della conformità NIS2 è assicurato dal Cyber Legal & Compliance Officer, in stretto raccordo con il Responsabile della Sicurezza delle Informazioni/Cyber Security Manager, il Punto di contatto NIS2, il Referente CSIRT, la Direzione e le altre funzioni competenti. Il coordinatore cura in particolare:

- il monitoraggio degli obblighi e delle scadenze applicabili;
- il raccordo tra governance societaria, compliance e funzioni tecniche;
- la predisposizione dei flussi informativi verso gli organi amministrativi;
- il coordinamento dell'aggiornamento della Policy, delle procedure e delle evidenze di conformità;
- il monitoraggio dei piani di adeguamento e delle eventuali azioni correttive;
- il raccordo con consulenti, auditor, autorità e organismi di controllo.

Per ciascuna società soggetta alla disciplina NIS2 è formalmente designato il **Punto di contatto NIS2**, ai sensi dell'articolo 7 del D.Lgs. 138/2024, nonché il relativo sostituto. Il Punto di contatto garantisce l'interlocuzione ufficiale con l'Agenzia per la cybersicurezza nazionale, cura la registrazione e l'aggiornamento delle informazioni sulla piattaforma ACN e assicura che eventuali variazioni siano comunicate nei termini previsti. L'articolo 7 richiede infatti la designazione del Punto di contatto e del relativo sostituto, oltre alla comunicazione dei soggetti responsabili individuati dalla normativa.
È inoltre designato il **Referente CSIRT**, denominato nella procedura interna "Responsabile Comunicazione CSIRT", incaricato dell'interlocuzione operativa con CSIRT Italia e della gestione delle notifiche di incidente. Il Referente CSIRT opera in coordinamento con il Punto di contatto NIS2, il Cyber Security Manager e il Cyber Legal & Compliance Officer e dispone delle informazioni, delle autorizzazioni e dei canali necessari per effettuare le comunicazioni previste. La disciplina operativa ACN distingue il Punto di contatto dal Referente CSIRT, attribuendo a quest'ultimo il presidio dell'interlocuzione relativa agli incidenti e alle notifiche.

3.3 Coordinamento interno e responsabilità trasversali

La gestione della cybersicurezza è una responsabilità trasversale e coinvolge tutte le funzioni che progettano, sviluppano, acquisiscono, gestiscono o utilizzano sistemi informativi, reti, dati, infrastrutture e servizi digitali.
Il Responsabile della Sicurezza delle Informazioni/Cyber Security Manager assicura il coordinamento tecnico e operativo; il Cyber Legal & Compliance Officer presidia gli aspetti normativi, legali e di compliance; il Punto di contatto NIS2 e il Referente CSIRT gestiscono le interlocuzioni istituzionali di

rispettiva competenza; il DPO e il Focal Point Privacy intervengono per gli aspetti relativi alla protezione dei dati personali. Le funzioni IT, Engineering, Quality & Test, HR, Procurement, Legal, Amministrazione, Comunicazione e i responsabili dei servizi e dei processi collaborano nell'ambito delle rispettive competenze.
In particolare:

- i responsabili di servizio e di processo comunicano tempestivamente rischi, anomalie, vulnerabilità e incidenti relativi agli ambiti di propria competenza;
- le funzioni IT e tecniche attuano le misure di prevenzione, rilevazione, contenimento, ripristino e conservazione delle evidenze;
- HR supporta l'attribuzione delle responsabilità, la gestione delle autorizzazioni, la formazione e i processi di ingresso, variazione e cessazione del personale;
- Procurement e Legal assicurano l'inserimento dei requisiti di cybersicurezza nei contratti con terze parti;
- Comunicazione gestisce, previa autorizzazione della Direzione e in coordinamento con le funzioni competenti, le comunicazioni verso clienti, utenti, stakeholder e mezzi di informazione;
- RGQA supporta la tracciabilità documentale, gli audit, la gestione delle non conformità e il coordinamento con i sistemi di gestione certificati.

Gli incidenti e i rischi rilevanti sono sottoposti a un processo di escalation proporzionato alla gravità, all'impatto operativo, alla possibile compromissione di dati, alla rilevanza normativa e agli effetti sui clienti e sui servizi erogati. Il Consiglio di Amministrazione e la Direzione sono informati periodicamente e, in presenza di eventi significativi, senza ritardo. Le notifiche degli incidenti significativi al CSIRT Italia seguono la sequenza e le tempistiche stabilite dalla normativa, comprese la pre-notifica, la notifica e la relazione finale.

3.4 Catena di responsabilità verso fornitori e subfornitori

Il Gruppo Diagram considera la sicurezza della catena di approvvigionamento parte integrante del proprio sistema di gestione dei rischi cyber. Il ricorso a fornitori, outsourcer, cloud provider, consulenti o subfornitori non esonera la società interessata dagli obblighi e dalle responsabilità derivanti dalla normativa NIS2.
I fornitori sono classificati in base alla criticità dei prodotti e dei servizi erogati, all'accesso a dati e sistemi, alla dipendenza operativa, alla sostituibilità del servizio e al potenziale impatto di un incidente sulla continuità e sulla sicurezza dei servizi del Gruppo. Per i fornitori critici sono effettuate verifiche preventive e periodiche riguardanti, tra l'altro, certificazioni, misure tecniche e organizzative, gestione degli accessi, sviluppo sicuro, vulnerabilità, continuità operativa, gestione degli incidenti e utilizzo di subfornitori.
I contratti con fornitori e subfornitori rilevanti devono prevedere, in misura proporzionata al rischio:

- requisiti minimi di sicurezza e obblighi di conformità alle Policy del Gruppo;
- obblighi di tempestiva segnalazione di incidenti, vulnerabilità e compromissioni;
- tempi di comunicazione compatibili con gli obblighi di notifica NIS2 del Gruppo;
- collaborazione nelle attività di analisi, contenimento, ripristino e notifica;
- disponibilità delle evidenze e dei registri necessari;
- diritto di audit, verifica o acquisizione di attestazioni indipendenti;
- requisiti di business continuity, disaster recovery, backup e ripristino;
- disciplina degli accessi, della restituzione e della cancellazione dei dati;

- autorizzazione preventiva o comunicazione dell'impiego di subfornitori;
- estensione ai subfornitori degli obblighi di sicurezza applicabili al fornitore principale.

Il fornitore principale è responsabile, nei confronti della società del Gruppo contraente, del rispetto degli obblighi attribuiti ai propri subfornitori e deve assicurare che questi ultimi adottino misure coerenti con la criticità dei servizi affidati. Il Gruppo verifica le vulnerabilità specifiche dei fornitori diretti, la qualità delle loro pratiche di sicurezza e l'efficacia delle misure applicate lungo la catena di fornitura. La normativa NIS2 richiede espressamente che la gestione dei rischi comprenda la sicurezza della catena di approvvigionamento e la valutazione delle vulnerabilità e delle pratiche di sicurezza dei fornitori diretti e dei fornitori di servizi.
Per maggiori dettagli sulla classificazione, qualifica e trattamento dei fornitori si veda la procedura interna di gruppo "*GRUPPO_PRO 07.03 Gestione Contratti Passivi e Qualifica dei fornitori*".

4. Analisi del rischio e gestione del rischio

4.1 Metodo di analisi del rischio: identificazione, valutazione e trattamento

Il Gruppo Diagram adotta un processo strutturato e iterativo per la gestione dei rischi relativi alla sicurezza delle informazioni, coerente con i principi delle norme ISO/IEC 27001 e ISO/IEC 27005. Il processo si articola nelle fasi di definizione del contesto, identificazione dei rischi, analisi e valutazione, trattamento, accettazione del rischio residuo, monitoraggio e riesame.
L'identificazione dei rischi è effettuata considerando gli asset informativi, i processi aziendali, le attività, i prodotti e i servizi compresi nel campo di applicazione del Sistema di Gestione per la Sicurezza delle Informazioni. Per ciascun ambito vengono individuati le fonti di rischio, le minacce, le vulnerabilità, le cause, gli eventi potenziali e le relative conseguenze, compresi gli eventuali effetti cumulativi o a cascata. L'analisi tiene conto del contesto interno ed esterno, delle esperienze pregresse, delle prescrizioni legislative, regolamentari e contrattuali, delle procedure esistenti, delle conoscenze disponibili e delle indicazioni contenute nella norma ISO/IEC 27005. Le informazioni possono essere raccolte attraverso interviste, sopralluoghi, analisi documentali, ispezioni e analisi dei processi e dei sistemi aziendali.
La valutazione del rischio prende in considerazione tre parametri:

- l'impatto sul business, valutato su una scala da 1 a 5;
- la probabilità di accadimento, valutata su una scala da 1 a 5;
- il livello di vulnerabilità rispetto alla minaccia, classificato come basso, medio o alto.

L'impatto sul business è determinato considerando, in particolare, la classificazione delle informazioni e degli asset coinvolti, la perdita di riservatezza, integrità o disponibilità, le conseguenze sull'operatività, le perdite economiche o commerciali, il danno reputazionale e la violazione di obblighi contrattuali, legali o regolamentari. Dalla combinazione dei tre parametri, attraverso la matrice aziendale di valutazione, deriva un livello di rischio compreso tra 1 e 11.
In funzione del livello rilevato, il rischio è classificato come inesistente, minimo, medio o inaccettabile. Per i rischi inaccettabili devono essere obbligatoriamente definite e attuate misure di trattamento finalizzate alla riduzione della probabilità di accadimento, della vulnerabilità o dell'impatto. Per ciascuna misura sono individuati l'obiettivo, le attività da realizzare, le risorse necessarie, le responsabilità e i tempi di attuazione. A seguito dell'applicazione dei controlli viene effettuata una nuova valutazione, finalizzata alla determinazione del rischio residuo. Qualora il trattamento non consenta di raggiungere un livello accettabile, il processo di valutazione e trattamento viene ripetuto, eventualmente rivedendo il contesto e i criteri utilizzati.

4.2 Criteri per l'accettazione del rischio residuo

L'accettazione del rischio è effettuata sulla base del livello di rischio residuo risultante dopo l'applicazione delle misure di controllo e del livello di governance associato all'asset, al processo o alla minaccia esaminata.

Il livello di governance esprime la capacità dell'Organizzazione di presidiare il rischio attraverso strategie gestionali, procedure e istruzioni formalizzate, prassi operative, attività di monitoraggio, azioni correttive e valutazione della loro efficacia. Tale livello è classificato come ottimo, buono, sufficiente o scarso e viene utilizzato per determinare il livello di significatività secondo la seguente relazione:

Livello di significatività = Rischio residuo × Governance

Sono considerati accettabili i rischi residui classificati come non significativi, per i quali le misure esistenti risultano adeguate rispetto al contesto, agli obiettivi aziendali e agli obblighi applicabili. I rischi con livello di significatività pari o superiore a 15 sono considerati significativi e richiedono la definizione di specifiche azioni nel Piano di azione e trattamento del rischio, con priorità e tempistiche proporzionate al livello rilevato.

L'accettazione del rischio residuo deve essere esplicita, documentata e approvata dai responsabili competenti dell'Organizzazione. Tale approvazione assume particolare rilevanza quando l'adozione di ulteriori controlli venga omessa, differita o ritenuta non sostenibile in relazione ai costi, alle risorse necessarie o alle esigenze operative. L'accettazione non esclude il successivo monitoraggio del rischio né la possibilità di sottoporlo a nuova valutazione qualora intervengano variazioni significative.

4.3 Revisione periodica e aggiornamento del rischio

L'analisi dei rischi per la sicurezza delle informazioni è riesaminata almeno annualmente, come attività preliminare alla revisione degli obiettivi e dei programmi aziendali e come elemento in ingresso al riesame della Direzione.

La valutazione deve inoltre essere aggiornata ogniqualvolta intervengano variazioni significative riguardanti il contesto interno o esterno, le attività, i processi, i prodotti, i servizi, gli asset informativi, le tecnologie utilizzate o gli obblighi normativi e contrattuali. Il riesame può essere attivato anche in conseguenza di incidenti di sicurezza, non conformità, modifiche organizzative, introduzione di nuovi sistemi o servizi, variazioni delle minacce e delle vulnerabilità o cambiamenti rilevanti nella catena di fornitura.

Le azioni di trattamento definite sono inserite nel Piano di azione e trattamento del rischio e sottoposte a monitoraggio in relazione allo stato di avanzamento, al rispetto delle tempistiche, alle responsabilità attribuite e all'efficacia delle misure implementate. Qualora il monitoraggio evidenzi che i controlli non risultano sufficienti o che il livello di rischio è aumentato, viene effettuata una nuova iterazione del processo di valutazione e vengono individuate ulteriori misure di mitigazione. Gli esiti delle revisioni e le eventuali decisioni di accettazione del rischio sono registrati e conservati quale evidenza del processo svolto.

4.4 Valutazione della catena di fornitura – terze parti

Il Gruppo Diagram valuta e monitora i rischi derivanti dai fornitori e dalle altre terze parti che possono avere accesso alle informazioni, ai sistemi, alle infrastrutture o ai processi aziendali oppure influire sulla continuità operativa, sulla conformità normativa e sulla sicurezza dei servizi erogati.

I fornitori critici devono essere sottoposti a prequalifica prima dell'avvio del rapporto contrattuale. La valutazione prende in considerazione almeno l'idoneità tecnica e professionale, la reputazione commerciale, la capacità economica e organizzativa, la conformità agli standard di sicurezza informatica, il possesso di certificazioni pertinenti, quali ISO/IEC 27001, ISO 9001, ISO 14001 o ISO 45001, nonché la presenza di un Codice Etico e di un Modello organizzativo ai sensi del D.Lgs. 231/2001, ove applicabile.
I fornitori critici sono classificati in:

- **fornitori ad alto rischio**, quando trattano dati personali o informazioni sensibili, gestiscono infrastrutture ICT critiche, operano direttamente sui sistemi aziendali o possono influire in modo rilevante sulla conformità e sulla continuità operativa;
- **fornitori a rischio standard**, quando erogano beni o servizi di uso generale o con un impatto limitato sulla sicurezza e sull'operatività aziendale.

I fornitori ad alto rischio sono sottoposti a qualifica almeno annuale, mentre quelli a rischio standard sono rivalutati almeno ogni tre anni. La rivalutazione può essere anticipata in presenza di inadempienze, incidenti o violazioni di sicurezza, cambiamenti societari, segnalazioni, deterioramento delle prestazioni o altre circostanze che possano modificare il relativo profilo di rischio.
Per i fornitori ICT, cloud, SaaS, IaaS e per gli altri servizi ad elevato impatto cyber, la valutazione comprende anche l'ubicazione dei data center, le misure di protezione dei dati, le certificazioni di sicurezza, gli SLA, i livelli di disponibilità, la gestione degli incidenti, la continuità operativa, l'individuazione dei referenti per la cybersecurity e degli amministratori di sistema, nonché le condizioni di cessazione del servizio, migrazione e restituzione o cancellazione dei dati.
I contratti con le terze parti devono prevedere, in funzione del rischio, requisiti minimi di cybersecurity, obblighi di riservatezza e protezione dei dati, obblighi di notifica e collaborazione in caso di incidente, livelli di servizio, diritti di audit, requisiti di competenza del personale, continuità operativa, gestione del subappalto e clausole risolutive in caso di violazioni gravi.
Le prestazioni dei fornitori sono monitorate considerando la conformità del prodotto o servizio all'ordine e al contratto, la puntualità, la qualità, il rapporto qualità-prezzo, l'assistenza e la capacità di interazione con le funzioni aziendali. In caso di valutazione negativa possono essere richieste azioni correttive e un successivo riesame oppure può essere disposta l'esclusione del fornitore dal Registro dei fornitori qualificati. Le valutazioni, i contratti, le certificazioni e la documentazione di qualifica sono registrati nel sistema aziendale, in modo da assicurare la completa tracciabilità del processo.

5. Misure tecniche e organizzative di sicurezza

5.1 Controlli di accesso e gestione degli account

L'Organizzazione adotta misure volte a garantire che l'accesso ai sistemi, alle applicazioni e alle informazioni aziendali sia consentito esclusivamente a utenti autorizzati, sulla base del ruolo e delle effettive esigenze operative. Gli account sono nominativi e gestiti durante l'intero ciclo di vita, dalla creazione alla modifica o revoca, prevedendo controlli periodici sui privilegi assegnati e l'utilizzo di adeguati meccanismi di autenticazione e protezione delle credenziali. Tutti i dettagli sono riportati in un'unica procedura applicata da tutte le aziende del Gruppo "*GRUPPO_IST 07.05 Procedimento interno per la gestione degli accessi*".

5.2 Crittografia e protezione dei dati

DIAGRAM adotta misure crittografiche volte a garantire la riservatezza, l'integrità e la sicurezza delle informazioni, escludendo l'esposizione di servizi mediante protocolli in chiaro. Le comunicazioni tra gli ambienti aziendali e Internet, gli accessi tramite VPN e i servizi erogati a terzi sono protetti mediante protocolli e algoritmi crittografici adeguati, tra cui AES256 e HTTPS con certificati rilasciati da fornitori accreditati. Le chiavi private e le chiavi di crittografia sono conservate in aree protette del file server, accessibili esclusivamente al personale autorizzato. La crittografia dei dispositivi e dei database viene attivata sulla base della classificazione delle informazioni, dei requisiti di sicurezza del cliente e delle risultanze della valutazione dei rischi, tenendo conto anche degli eventuali impatti sulle prestazioni e sulla continuità operativa dei sistemi.
Tutti i dettagli sono riportati in una procedura "*IST 07.06 Procedimento interno per lo sviluppo dei sistemi informativi*" specifica per ogni azienda del Gruppo.

5.3 Monitoraggio, logging e audit dei sistemi

La gestione e la raccolta dei log degli eventi avviene tramite i servizi standard dei Sistemi Operativi Windows e Linux, rispettivamente Event Viewer e SysLog.
Nel log presente sul server oggetto di eventuale modifica sono presenti le seguenti informazioni:
i tentativi di accesso sia falliti che avvenuti con successo dando evidenza del nome utente, data e ora dell'evento e dell'ip della macchina da cui è stato lanciato l'evento.
Le operazioni principali eseguite sulla macchina
I log registrati sui singoli server sono accessibili solo da parte dell'amministratore di sistema.
Ad inizio 2026 è stata acquisita una piattaforma di gestione integrata dei Log.
Tutti i dettagli sono riportati in un'unica procedura applicata da tutte le aziende del Gruppo "*GRUPPO_IST 07.05 Procedimento interno per la gestione degli accessi*".

5.4 Gestione delle vulnerabilità e patch management

Il Gruppo DIAGRAM adotta un processo strutturato per l'identificazione, la valutazione e la gestione delle vulnerabilità tecniche relative a reti, dispositivi, server, applicazioni web, servizi e infrastrutture aziendali. Il monitoraggio viene svolto periodicamente da un fornitore esterno specializzato in cybersecurity, attraverso vulnerability assessment, web assessment e sistemi proattivi basati su agent, con produzione di report mensili analizzati dalle funzioni Compliance, IT e Produzione. Le vulnerabilità rilevate vengono registrate nel sistema di gestione dei progetti, classificate in base alla criticità e gestite mediante specifiche attività di remediation e, ove necessario, mediante

l'installazione di patch e aggiornamenti correttivi. I tempi previsti per la presa in carico e la risoluzione sono pari a 24 ore per le vulnerabilità critiche, 72 ore per quelle di livello alto, 30 giorni per quelle medie e 90 giorni per quelle basse. Le vulnerabilità particolarmente gravi possono determinare l'attivazione del processo di gestione degli incidenti di sicurezza, mentre eventuali rischi non eliminabili o la cui risoluzione risulti eccessivamente onerosa vengono formalmente valutati e accettati. La chiusura delle attività e l'efficacia delle misure adottate sono oggetto di controlli periodici.
Tutti i dettagli sono riportati in un'unica procedura applicata da tutte le aziende del Gruppo "*GRUPPO_IST 07.09 Gestione delle Vulnerabilità tecniche e protezione contro i malware*".

5.5 Backup, resilienza e continuità operativa

Il Gruppo adotta procedure strutturate e prevalentemente automatizzate per il backup dei dati, dei sistemi, delle applicazioni, dei database e dei repository di codice sorgente, mediante copie conservate sia su infrastrutture interne sia su ambienti cloud. I dati sono protetti attraverso meccanismi di ridondanza, replica, sincronizzazione, versioning, snapshot e, ove previsto, immutabilità delle copie, al fine di garantirne la disponibilità e il recupero in caso di guasti, cancellazioni accidentali, modifiche non autorizzate o indisponibilità dei sistemi.
La frequenza e i periodi di conservazione dei backup sono definiti in funzione della tipologia, della criticità e della classificazione delle informazioni e possono prevedere copie giornaliere, settimanali, incrementali o differenziali. L'esito delle operazioni viene monitorato tramite notifiche automatiche e verificato dal personale tecnico incaricato, che interviene in caso di errore adottando le opportune azioni correttive e valutando l'eventuale ripetizione immediata del backup. L'integrità e l'effettiva recuperabilità delle copie vengono verificate mediante test periodici di ripristino, eseguiti almeno annualmente e formalmente documentati, con particolare attenzione ai sistemi che trattano dati personali e ai servizi considerati essenziali per la continuità operativa.
Tutti i dettagli sono riportati in una procedura "*IST 07.01 procedimento interno per il back up*" specifica per ogni azienda del Gruppo.

5.1 Segmentazione di rete, difesa perimetrale e Sicurezza fisica e ambientale

Il Gruppo adotta un modello di sicurezza multilivello basato sulla segmentazione delle reti, sulla protezione del perimetro informatico e sul controllo fisico e ambientale delle infrastrutture. Le reti aziendali e cloud sono suddivise in ambienti distinti in funzione della tipologia di utenti, dei dispositivi e dei servizi erogati, separando le reti per gli ospiti e i dispositivi personali da quelle dedicate ai dipendenti, ai server, ai sistemi applicativi, ai database e ai servizi esposti verso l'esterno; gli accessi e le comunicazioni tra i diversi segmenti sono regolati secondo il principio del minimo privilegio, mediante specifiche autorizzazioni, regole di rete e collegamenti cifrati. La difesa perimetrale è assicurata da apparati ridondati e costantemente aggiornati, dotati di funzionalità di prevenzione delle intrusioni, filtraggio della navigazione, controllo delle applicazioni e protezione da virus e malware, affiancati da sistemi di autenticazione, monitoraggio, registrazione degli eventi e gestione degli alert; gli attacchi riconducibili a schemi noti vengono contrastati automaticamente, mentre gli eventi anomali sono sottoposti ad analisi e intervento specialistico. La sicurezza fisica e ambientale prevede l'accesso alle sedi e ai locali tecnici esclusivamente da parte di personale autorizzato, attraverso badge o chiavi nominative, la registrazione e l'accompagnamento dei visitatori, la definizione di fasce orarie di accesso e, ove previsto, l'impiego di sistemi di allarme e videosorveglianza. I locali che ospitano le infrastrutture informatiche sono inoltre protetti mediante

climatizzazione continua, sistemi di continuità elettrica, sensori per il rilevamento di temperatura e presenza di acqua, dispositivi antincendio, cablaggi protetti e separati dalle linee elettriche, attività di manutenzione periodica e procedure per la gestione dei guasti e delle emergenze.
Tutti i dettagli sono riportati in una procedura "*IST 07.18 Sicurezza Fisica e Ambientale*" specifica per ogni azienda del Gruppo.

5.2 Difesa contro malware / attacchi avanzati

Il Gruppo adotta misure di protezione multilivello contro malware, tentativi di exploit e altre minacce informatiche avanzate, applicate ai server, alle postazioni di lavoro e alle infrastrutture di rete. I sistemi di sicurezza operano in tempo reale per rilevare e bloccare comportamenti anomali, codice malevolo e tentativi di compromissione, isolando automaticamente i file sospetti in aree di quarantena accessibili esclusivamente al personale autorizzato. Le soluzioni di protezione non possono essere disattivate o rimosse dagli utenti e sono gestite mediante console centralizzate, dalle quali vengono monitorati gli eventi e definite le azioni di eliminazione, autorizzazione o contenimento. Il presidio è completato dal monitoraggio continuo della rete e dei dispositivi, dall'analisi periodica degli eventi registrati dai sistemi perimetrali e da attività di threat intelligence finalizzate a individuare tempestivamente nuove minacce e valutarne il possibile impatto sui servizi aziendali. In presenza di anomalie o minacce rilevanti, il personale tecnico e gli specialisti di sicurezza effettuano le necessarie analisi e attivano le opportune misure di contenimento e remediation.
Tutti i dettagli sono riportati in un'unica procedura applicata da tutte le aziende del Gruppo "*GRUPPO_IST 07.09 Gestione delle Vulnerabilità tecniche e protezione contro i malware*".

5.3 Gestione delle modifiche e configurazioni (change management)

Il Gruppo adotta un processo strutturato per la gestione delle modifiche apportate alle infrastrutture, ai sistemi informativi, alle applicazioni, ai componenti hardware e software e agli ambienti cloud. Ogni cambiamento deve essere preventivamente descritto, valutato e approvato dal responsabile competente, considerando finalità dell'intervento, requisiti tecnici, risorse e licenze necessarie, costi, tempi di realizzazione e modalità di collaudo. La valutazione comprende inoltre l'analisi dei rischi e dei possibili impatti sulla continuità operativa, sulla disponibilità dei servizi, nonché sulla riservatezza e sull'integrità dei dati. Le attività, le responsabilità, le modifiche effettuate e i relativi esiti vengono registrati nel sistema interno di gestione dei progetti, associando a ciascun intervento un livello di priorità commisurato al rischio. Prima dell'introduzione in esercizio, i nuovi componenti e le modifiche ai sistemi esistenti sono sottoposti a test di accettazione, affidabilità, connessione, prestazioni e sicurezza, utilizzando, ove necessario, ambienti temporanei o separati per verificare il corretto funzionamento e ridurre il rischio di interruzioni o anomalie.
Tutti i dettagli sono riportati in una procedura "IST 07.06 Procedimento interno per lo sviluppo dei sistemi informativi" specifica per ogni azienda del Gruppo.

6. Notifica e gestione degli incidenti di sicurezza

l Gruppo adotta un processo formalizzato per la rilevazione, la valutazione, la gestione e la comunicazione degli incidenti che possano compromettere la riservatezza, l'integrità o la disponibilità delle informazioni, dei sistemi informativi, dei servizi cloud e degli asset aziendali. La gestione è coordinata dal Responsabile della Sicurezza delle Informazioni, con il supporto del team tecnico, delle funzioni di compliance e privacy e, per gli eventi più gravi, dell'Incident Response Team. Il processo comprende la segnalazione tempestiva, la classificazione dell'evento, il contenimento,

l'eliminazione della minaccia, il ripristino dei servizi, l'eventuale notifica alle autorità competenti e la successiva analisi delle cause e delle azioni di miglioramento.

6.1 Definizione di incidente significativo (criteri)

La significatività di un incidente viene determinata mediante una valutazione basata su sei criteri: numero di utenti o controparti coinvolti e relativo impatto reputazionale; durata dell'incidente o dell'indisponibilità; estensione geografica; compromissione della riservatezza, integrità o disponibilità dei dati; criticità dei servizi e delle funzioni interessate; impatto economico. A ciascun criterio viene attribuito un punteggio da 1 a 3, corrispondente a un livello basso, medio o alto. Un punteggio complessivo da 6 a 9 identifica un incidente non significativo, da 10 a 13 un incidente significativo da valutare caso per caso e da 14 a 18 un incidente alto o maggiore, soggetto agli obblighi di notifica previsti.

6.2 Processo interno di rilevazione, risposta e mitigazione

Gli incidenti possono essere rilevati tramite segnalazioni del personale oppure attraverso sistemi automatici di monitoraggio, analisi dei log, firewall, antivirus, strumenti di rilevamento delle intrusioni e servizi di controllo delle infrastrutture. Le anomalie devono essere comunicate immediatamente e, comunque, entro un'ora dalla rilevazione, utilizzando i canali aziendali previsti e assicurando successivamente una comunicazione scritta e archiviabile. Il personale tecnico effettua una prima analisi per verificare la natura, la fonte e la criticità dell'evento, correla i log e gli alert disponibili e distingue gli incidenti effettivi dai falsi positivi. Una volta confermato l'incidente, vengono attuate le misure di contenimento, quali l'isolamento dei sistemi, il blocco degli account o la disabilitazione degli accessi a rischio; seguono l'eliminazione della minaccia mediante rimozione del codice malevolo, aggiornamenti, correzioni e modifica delle credenziali compromesse, nonché il ripristino controllato dei sistemi attraverso backup verificati, controlli di integrità, misure di hardening e test finali di validazione.

6.3 Flussi di notifica verso ACN e autorità competenti

Il Responsabile della Sicurezza delle Informazioni valuta, con il supporto dell'Incident Response Team e delle funzioni legali e privacy, la necessità di notificare l'incidente alle autorità competenti. Per gli incidenti classificati come alti o maggiori, il Responsabile CSIRT gestisce la comunicazione operativa verso ACN e CSIRT Italia attraverso il canale ufficiale previsto, trasmettendo una notifica iniziale entro 24 ore, un aggiornamento dettagliato entro 72 ore e una relazione finale entro un mese. Gli incidenti di livello medio sono invece sottoposti a valutazione caso per caso, formalizzata mediante un report dell'Incident Response Team. Qualora l'evento comporti una violazione di dati personali, viene valutato anche l'obbligo di notifica all'autorità garante competente entro 72 ore; per le società estere si applicano i flussi verso i rispettivi organismi nazionali di controllo.

6.4 Comunicazioni esterne e reporting

Le comunicazioni relative agli incidenti sono coordinate dal Responsabile della Sicurezza delle Informazioni e devono essere approvate dalla Direzione quando presentano rilevanza esterna o reputazionale. Le funzioni aziendali coinvolte vengono informate tempestivamente e, per gli incidenti significativi, la comunicazione interna deve avvenire entro due ore dalla classificazione. Le comunicazioni verso clienti, fornitori, partner, assicurazioni o altri stakeholder sono effettuate soltanto previa autorizzazione della Direzione e nel rispetto degli obblighi contrattuali e normativi. Il

reporting deve indicare almeno data e ora dell'incidente, sistemi e servizi interessati, impatti sulla sicurezza e sui dati, misure correttive adottate, tempi stimati di ripristino e riferimenti per i successivi aggiornamenti. Qualora necessario, può essere predisposta una comunicazione pubblica per gestire gli impatti reputazionali e informare correttamente le parti interessate.

6.5 Registro degli incidenti e analisi post evento

Ogni incidente deve essere registrato nel Registro degli incidenti, delle non conformità e dei reclami, documentando la segnalazione, la classificazione, le attività svolte, le decisioni adottate, le notifiche effettuate e l'esito della gestione. I log, le immagini dei sistemi, le tracce di rete e le altre evidenze digitali rilevanti devono essere raccolti, protetti, allegati agli strumenti aziendali di gestione documentale e conservati per almeno cinque anni, salvo differenti obblighi normativi. Al termine dell'evento viene svolta una root cause analysis per individuare la causa principale, le vulnerabilità sfruttate e gli eventuali fattori organizzativi o tecnici che hanno contribuito all'incidente. Le conclusioni e le raccomandazioni vengono riportate in un report finale, utilizzato per verificare l'efficacia della risposta, identificare eventi ricorrenti, aggiornare le misure di sicurezza, le procedure operative e la formazione del personale e condividere con la Direzione le lezioni apprese.

7. Continuità operativa e ripristino

Il Gruppo adotta un modello strutturato di continuità operativa e disaster recovery finalizzato a garantire la prosecuzione dei servizi critici, ridurre al minimo le perdite operative e ripristinare nel più breve tempo possibile sistemi, dati e infrastrutture compromessi da eventi gravi o prolungati. Il modello si applica alle infrastrutture interne, ai servizi cloud, agli archivi, ai sistemi utilizzati dal personale e ai dati aziendali, prevedendo il coinvolgimento di un Comitato di Crisi incaricato di valutare la gravità dell'evento, definire le priorità di intervento, coordinare le attività tecniche e gestire le comunicazioni con le funzioni interne, i clienti, i fornitori e, ove necessario, le autorità competenti.

7.1 Piano di continuità / disaster recovery

Il Disaster Recovery Plan definisce la sequenza delle azioni da attivare in caso di eventi naturali, tecnologici, accidentali o dolosi che compromettano in modo significativo la disponibilità, l'integrità o il funzionamento dei sistemi informativi e dei servizi aziendali. A seguito della dichiarazione di disastro, il Comitato di Crisi valuta l'estensione del danno, attiva le comunicazioni interne e definisce le modalità per mantenere un livello minimo di operatività, anche attraverso il lavoro da remoto. Il piano stabilisce priorità differenziate per il ripristino dei servizi, privilegiando i sistemi necessari allo sviluppo, all'autenticazione, alla gestione dei dati e all'assistenza tecnica, e definisce specifici obiettivi di perdita massima dei dati e tempi di ripristino. Per l'infrastruttura aziendale generale è previsto un RPO di 24 ore e un RTO stimato in 5 giorni lavorativi, mentre per i servizi SaaS critici sono previsti un RPO di 2 ore e un RTO di 2 giorni.

7.2 Procedure di recupero e ripristino

Le procedure di recupero prevedono innanzitutto la verifica della disponibilità delle copie di backup e delle infrastrutture residue, seguita dal ripristino della sede operativa, delle componenti hardware, delle reti aziendali e dei server secondo l'ordine di priorità definito. Il recupero dei sistemi viene effettuato utilizzando backup verificati e, ove necessario, ricostruendo l'infrastruttura su ambienti alternativi. Per gli incidenti che coinvolgono servizi cloud o SaaS, il personale tecnico contatta il

fornitore, valuta congiuntamente l'entità dell'evento e procede al ripristino del servizio; qualora ciò non sia possibile, viene attivata la ricostruzione su una nuova infrastruttura secondo la procedura tecnica dedicata. Le attività comprendono inoltre la verifica dell'integrità dei dati, il ripristino delle connessioni tra le sedi, la riattivazione progressiva dei servizi e la comunicazione ai clienti delle modalità e delle tempistiche di recupero.

7.3 Test periodici e simulazioni

L'efficacia del piano viene verificata attraverso simulazioni di disastro effettuate almeno una volta all'anno, includendo sia le sedi italiane sia, in specifiche esercitazioni, le sedi estere. Le simulazioni hanno lo scopo di verificare la capacità di attivazione del Comitato di Crisi, la corretta applicazione delle procedure di comunicazione, la disponibilità dei backup, la prontezza del personale tecnico e la possibilità di ripristinare i servizi secondo le priorità e i tempi stabiliti. Il personale viene informato preventivamente secondo canali e tempistiche definite, mentre in caso di manutenzioni programmate o indisponibilità pianificate delle infrastrutture vengono adottate misure organizzative alternative, come il ricorso al lavoro da remoto. Gli esiti dei test e delle simulazioni sono documentati e utilizzati per individuare eventuali carenze e aggiornare le procedure.

7.4 Integrazione con business continuity aziendale

Il piano di disaster recovery è integrato con le misure generali di continuità operativa, con le procedure di gestione degli incidenti, di backup, di sicurezza delle informazioni e con gli accordi di servizio stipulati con i fornitori esterni. La gestione dell'emergenza considera non solo il ripristino tecnico dei sistemi, ma anche la continuità delle attività aziendali essenziali, dell'assistenza ai clienti, delle comunicazioni e dell'operatività del personale. Le decisioni assunte dal Comitato di Crisi vengono formalizzate e coordinate con le funzioni aziendali interessate, mentre i servizi esternalizzati sono gestiti in coerenza con i livelli di disponibilità, manutenzione e assistenza previsti contrattualmente. In questo modo il ripristino tecnologico è inserito in un quadro più ampio di gestione della continuità, volto a ridurre gli impatti operativi, economici, contrattuali e reputazionali derivanti da eventi avversi.

8. Formazione, consapevolezza e cultura della sicurezza

L'organizzazione promuove una cultura diffusa della sicurezza attraverso programmi strutturati di formazione, aggiornamento e sensibilizzazione rivolti a tutto il personale. Le iniziative sono definite in funzione dei ruoli e delle responsabilità ricoperte e riguardano, in particolare, la cybersecurity, il Sistema di Gestione per la Qualità, la sicurezza delle informazioni e i principi di sviluppo sicuro. La formazione è integrata da comunicazioni periodiche, simulazioni ed esercitazioni finalizzate a mantenere elevato il livello di attenzione sui rischi informatici e a verificare la capacità di risposta dell'organizzazione.

8.1 Programmi di formazione e sensibilizzazione

Tutti i neoassunti sono inseriti in un percorso formativo obbligatorio erogato tramite una piattaforma dedicata, con contenuti differenziati in base al ruolo e alle attività svolte. Il programma comprende moduli relativi alla cybersecurity, al Sistema di Gestione per la Qualità e la Sicurezza delle Informazioni e, per le figure tecniche interessate, allo sviluppo sicuro del software. Il percorso iniziale è affiancato da attività continuative di sensibilizzazione curate dal Reparto IT, attraverso

aggiornamenti, comunicazioni e approfondimenti sulle principali minacce, sui comportamenti corretti da adottare e sulle modalità di segnalazione di eventi sospetti.

8.2 Simulazioni ed esercitazioni

L'organizzazione effettua con cadenza semestrale simulazioni di incidenti di sicurezza e test di continuità operativa, con l'obiettivo di verificare l'efficacia delle procedure, la capacità di coordinamento delle funzioni coinvolte e la prontezza del personale nella gestione di situazioni critiche. È inoltre prevista la pianificazione di campagne simulate di phishing, finalizzate a misurare il livello di consapevolezza degli utenti, individuare eventuali aree di rischio e definire interventi formativi mirati. Gli esiti delle esercitazioni vengono analizzati per individuare criticità e migliorare progressivamente le misure organizzative e di sicurezza.

8.3 Ruoli con obbligo formativo specifico

Gli amministratori di sistema e il personale del Reparto Ricerca e Sviluppo ricevono una formazione specialistica coerente con le responsabilità e i privilegi associati al proprio ruolo. Per gli amministratori di sistema, la formazione riguarda la gestione sicura delle infrastrutture, degli accessi privilegiati, delle configurazioni, delle vulnerabilità e degli incidenti. Per il personale di Ricerca e Sviluppo, l'aggiornamento è focalizzato sui principi di secure by design, sulle pratiche di sviluppo sicuro, sulla protezione del codice e dei dati e sulla prevenzione delle vulnerabilità applicative. I percorsi sono aggiornati periodicamente in funzione dell'evoluzione tecnologica, normativa e delle minacce rilevate.

9. Valutazione, audit interno e conformità

L'Organizzazione verifica periodicamente l'adeguatezza e l'efficacia delle misure adottate per la gestione dei rischi di cybersicurezza e per l'adempimento degli obblighi applicabili in materia NIS2. Le attività di verifica sono pianificate secondo un approccio basato sul rischio e comprendono audit interni, controlli documentali, verifiche tecniche, monitoraggio degli indicatori e valutazione dello stato di attuazione dei piani di miglioramento. Gli esiti sono documentati, comunicati alle funzioni responsabili e sottoposti agli organi di amministrazione e direttivi, che approvano le modalità di implementazione delle misure di sicurezza, ne supervisionano l'attuazione e vengono informati periodicamente o tempestivamente sugli incidenti e sulle principali criticità.

9.1 Audit interni di conformità NIS2

Gli audit interni sono svolti in concomitanza agli audit interni per la compliance alla normativa ISO27001 sulla base di un programma periodico approvato dalla Direzione e finalizzato a verificare la conformità alle disposizioni normative, alle misure di gestione del rischio, alle politiche aziendali e alle procedure operative. Le verifiche riguardano, in particolare, la governance della cybersicurezza, la gestione degli asset e degli accessi, la sicurezza della catena di fornitura, la gestione delle vulnerabilità e degli incidenti, la continuità operativa, la formazione e gli obblighi di comunicazione e notifica. Gli auditor devono operare con adeguata competenza, indipendenza rispetto alle attività esaminate e accesso alle evidenze necessarie. Ogni audit si conclude con un rapporto che identifica conformità, osservazioni, non conformità, rischi residui e azioni correttive, indicando responsabili e termini di attuazione.

9.2 Verifiche esterne e audit di terza parte

L'Organizzazione può sottoporre i propri sistemi, processi e misure di sicurezza a verifiche indipendenti condotte da soggetti qualificati, anche nell'ambito di certificazioni, obblighi contrattuali, richieste dei clienti o specifiche valutazioni del rischio. Gli audit esterni possono includere verifiche documentali, assessment tecnici, test di sicurezza, scansioni delle vulnerabilità e controlli sui fornitori rilevanti. La documentazione e le evidenze prodotte devono essere conservate e rese disponibili alle autorità competenti quando richiesto. L'Autorità nazionale competente NIS può richiedere rendicontazioni, autovalutazioni, piani di implementazione, audit periodici o mirati e scansioni di sicurezza, in particolare in presenza di incidenti significativi o possibili violazioni degli obblighi normativi.

9.3 Monitoraggio continuo e indicatori KPI

L'Organizzazione definisce e monitora un insieme di indicatori quantitativi e qualitativi per valutare nel tempo l'efficacia del sistema di gestione della cybersicurezza in coordinamento con gli stessi predisposti per la compliance alla normativa ISO27001 ed esposti nel Riesame annuale della Direzione. I KPI possono comprendere il numero e la gravità degli incidenti, i tempi di rilevazione e risposta, il rispetto delle tempistiche di notifica, lo stato di risoluzione delle vulnerabilità, il livello di aggiornamento dei sistemi, l'esito dei backup e dei test di ripristino, il completamento della formazione, i risultati delle simulazioni di phishing, le non conformità aperte e i tempi di chiusura delle azioni correttive. Gli indicatori sono riesaminati periodicamente, confrontati con soglie e obiettivi definiti e utilizzati per individuare anomalie, tendenze e necessità di intervento.

9.4 Reporting interno alla Direzione

Le funzioni responsabili della sicurezza predispongono una rendicontazione periodica destinata alla Direzione e agli organi di amministrazione, contenente lo stato di conformità, l'andamento dei principali indicatori, gli incidenti rilevanti, i rischi residui, gli esiti degli audit e l'avanzamento dei piani correttivi, tutto ciò sintetizzato nel Riesame della Direzione. Le criticità che possono incidere significativamente sulla continuità dei servizi, sulla sicurezza delle informazioni o sull'adempimento degli obblighi normativi devono essere comunicate senza ritardo. La Direzione valuta i risultati, assegna le priorità, approva le risorse necessarie e supervisiona l'attuazione delle misure di miglioramento, in coerenza con le responsabilità attribuite agli organi amministrativi e direttivi dalla disciplina NIS2.

10. Supervisione, ispezioni e controlli da parte delle autorità

L'Organizzazione riconosce i poteri di monitoraggio, vigilanza, verifica, ispezione ed esecuzione attribuiti all'Autorità nazionale competente NIS e si impegna a garantire piena collaborazione nello svolgimento delle relative attività. A tal fine mantiene aggiornate, disponibili e tracciabili le politiche, le procedure, le valutazioni dei rischi, i rapporti di audit, le evidenze tecniche, le notifiche, i registri e i piani di adeguamento necessari a dimostrare l'effettiva attuazione delle misure di sicurezza. L'ACN, in qualità di Autorità nazionale competente NIS, monitora l'adempimento degli obblighi e può richiedere informazioni, autovalutazioni, audit e specifiche attività di verifica.

10.1 Collaborazione con le autorità competenti

Tutte le richieste provenienti dall'Autorità nazionale competente NIS, dal CSIRT Italia o da altre autorità aventi titolo devono essere prese in carico tempestivamente e coordinate dalle funzioni

aziendali designate. L'Organizzazione fornisce informazioni complete, corrette e verificabili, facilita l'accesso alla documentazione e alle evidenze richieste e assicura il supporto del personale tecnico, legale e organizzativo competente. Le comunicazioni sono formalmente registrate e conservate, con indicazione delle richieste ricevute, delle risposte fornite, delle decisioni assunte e degli eventuali impegni di adeguamento. La mancata collaborazione con l'Autorità nazionale competente NIS o con il CSIRT Italia costituisce una violazione sanzionabile.

10.2 Modalità di ispezione e accertamento

L'Autorità competente può effettuare verifiche sulla documentazione e sulle informazioni trasmesse, ispezioni in loco o a distanza, anche casuali, e richieste di accesso a dati, documenti e ulteriori elementi necessari. L'Organizzazione individua preventivamente i referenti incaricati di assistere gli ispettori, coordinare la raccolta delle evidenze e assicurare che ogni attività si svolga nel rispetto delle prescrizioni ricevute e delle esigenze di riservatezza. Le richieste, i verbali, le evidenze consegnate e gli esiti dell'accertamento devono essere tracciati e conservati. Per i soggetti qualificati come importanti, l'esercizio dei poteri ispettivi avviene in presenza di elementi o informazioni che suggeriscano una possibile violazione.

10.3 Gestione delle non conformità e piani correttivi

Le non conformità individuate attraverso audit, verifiche interne o controlli delle autorità sono registrate, analizzate e classificate in funzione della gravità e del rischio associato. Per ciascuna non conformità viene definito un piano correttivo contenente le cause, le misure da adottare, i responsabili, le risorse necessarie, le scadenze e le modalità di verifica dell'efficacia. Le azioni sono monitorate fino alla loro completa chiusura e il relativo stato è comunicato alla Direzione e, quando richiesto, all'Autorità competente. Quest'ultima può impartire istruzioni vincolanti, richiedere la correzione delle carenze, ordinare l'attuazione delle raccomandazioni derivanti dagli audit, imporre la cessazione dei comportamenti non conformi e, in caso di mancato adempimento, adottare una formale diffida.

10.4 Sanzioni e responsabilità

La violazione degli obblighi NIS2 può comportare misure correttive, diffide, sanzioni amministrative pecuniarie e ulteriori provvedimenti previsti dalla normativa. Per i soggetti essenziali privati, le violazioni più rilevanti possono essere sanzionate fino a 10 milioni di euro o, se superiore, fino al 2% del fatturato annuo mondiale; per i soggetti importanti, fino a 7 milioni di euro o, se superiore, fino all'1,4% del fatturato annuo mondiale. Nei casi previsti, l'Autorità può inoltre disporre misure temporanee nei confronti delle persone fisiche che esercitano funzioni dirigenziali. Gli organi di amministrazione e direttivi sono responsabili dell'approvazione e della supervisione delle misure di gestione dei rischi e possono essere chiamati a rispondere delle violazioni secondo le disposizioni applicabili.

11. Revisione e aggiornamento della politica

La presente politica è sottoposta a revisione periodica per garantirne l'adeguatezza rispetto al contesto organizzativo, alle minacce, alle tecnologie utilizzate e agli obblighi normativi applicabili. La revisione considera gli esiti degli audit, gli indicatori di sicurezza, gli incidenti verificatisi, le modifiche ai processi e ai servizi, le risultanze delle valutazioni dei rischi e le indicazioni ricevute dalle autorità competenti. Ogni aggiornamento deve essere formalmente approvato, comunicato alle funzioni

interessate e accompagnato dall'adeguamento delle procedure operative e delle attività formative pertinenti.

11.1 Frequenza e modalità di revisione

La politica è riesaminata almeno annualmente dalle funzioni responsabili della sicurezza, della compliance e dei sistemi informativi, con il coinvolgimento delle ulteriori strutture aziendali interessate. Il riesame verifica la coerenza del documento con la strategia aziendale, la valutazione dei rischi, l'evoluzione del perimetro tecnologico e organizzativo e i requisiti normativi vigenti. Le proposte di modifica sono documentate, sottoposte alla Direzione e approvate dagli organi competenti prima della loro entrata in vigore.

11.2 Circostanze che determinano una revisione straordinaria

Indipendentemente dalla revisione periodica, la politica deve essere aggiornata in occasione di incidenti significativi, nuove minacce o vulnerabilità rilevanti, modifiche normative o indicazioni dell'Autorità competente, introduzione di nuove tecnologie, variazioni sostanziali delle infrastrutture o dei servizi, acquisizioni e riorganizzazioni, cambiamenti nella catena di fornitura o risultati negativi di audit e test. La necessità di revisione viene valutata anche quando gli indicatori evidenziano un peggioramento del livello di sicurezza o l'inefficacia delle misure esistenti.

11.3 Versionamento e approvazione

Ogni versione della politica deve riportare almeno il numero di revisione, la data di emissione, la descrizione sintetica delle modifiche, il responsabile della redazione e i soggetti incaricati della verifica e dell'approvazione. Le versioni superate sono archiviate secondo le regole di conservazione documentale e rese non disponibili per l'utilizzo operativo, mantenendone comunque la tracciabilità. La versione vigente è pubblicata nei canali aziendali autorizzati e comunicata al personale interessato; le modifiche sostanziali devono essere accompagnate, ove necessario, da specifiche attività informative o formative.

12.Allegati e riferimenti tecnici

12.1 Elenco misure e requisiti secondo Allegato 1 / Allegato 2

Sono applicati tutti i requisiti pertinenti dell'Allegato 1. Le modalità tecniche di applicazione sono riportate e aggiornate almeno annualmente nel documento "Misure di sicurezza per i soggetti NIS importanti" correlato al SOA ISO27001.

12.2 Documentazione correlata

Le aziende del gruppo mantengono costantemente aggiornato un registro della documentazione per tutti i sistemi di gestione e la confromità normativa (4.01 MOD EDS Elenco documentazione di sistema).