CONSIGLIO REGIONALE DEL PIEMONTE - Deliberazione dell'Ufficio di Presidenza

Deliberazione 28 ottobre 2026, n. 352

PIANO GENERALE DI ATTUAZIONE DELLA DIRETTIVA (UE) 2022/2555 "NIS 2" E DEL D.LGS. 138/2024 IN CONSIGLIO REGIONALE DEL PIEMONTE. AGGIORNAMENTO (V02). APPROVAZIONE. (CG/FCA/ASC)

Documento allegato

CONSIGLIO REGIONALE DEL PIEMONTE

Ufficio di Presidenza

Delibera n. 352/2026 - Cl. 6.6.4

Oggetto PIANO GENERALE DI ATTUAZIONE DELLA DIRETTIVA (UE) 2022/2555 "NIS 2" E DEL D.LGS. 138/2024 IN CONSIGLIO REGIONALE DEL PIEMONTE. AGGIORNAMENTO (V02). APPROVAZIONE. (CG/FCA/ASC)

Seduta n. 44

L'anno 2026, il giorno 28 ottobre alle ore 13.47 - presso la sede di Palazzo Lascaris, via Alfieri n. 15, Torino - si è riunito l'Ufficio di Presidenza del Consiglio Regionale.

Sono presenti: il Presidente NICCO, il Vice Presidente GRAGLIA, il Vice Presidente RAVETTI, il Consigliere Segretario CASTELLO.

Non sono presenti: i Consiglieri Segretari CAROSSO, CERA.

A relazione del Consigliere Segretario CASTELLO

PIANO GENERALE DI ATTUAZIONE DELLA DIRETTIVA (UE) 2022/2555 "NIS 2" E DEL D.LGS. 138/2024 IN CONSIGLIO REGIONALE DEL PIEMONTE. AGGIORNAMENTO (V02). APPROVAZIONE. (CG/FCA/ASC)

Premesso che:

in data 17 gennaio 2023 è entrata in vigore la direttiva (UE) 2022/2555 (NIS 2) del Parlamento Europeo e del Consiglio relativa a misure per un livello comune elevato di cybersicurezza

nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (NIS), da recepire da parte di tutti gli stati membri dell'Unione europea entro il 17 ottobre 2024;
tale direttiva stabilisce misure volte a garantire un livello elevato di cybersicurezza nell'Unione, in modo da migliorare il funzionamento del mercato interno, definendo una serie di obblighi e misure da adottare da parte degli Stati membri;
in Italia la suddetta direttiva è stata recepita con il decreto legislativo 4 settembre 2024, n. 138 recante "Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148", pubblicato in G.U. il 1° ottobre 2024 (di seguito anche solo "Decreto NIS 2");
con legge 28 giugno 2024, n. 90 recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici", pubblicata in G.U. Serie Generale n. 153 del 02 luglio 2024, sono altresì state introdotte disposizioni in materia di rafforzamento della cybersicurezza nazionale, di resilienza delle pubbliche amministrazioni e del settore finanziario, di personale e funzionamento dell'Agenzia per la cybersicurezza nazionale e degli organismi di informazione per la sicurezza nonché di contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici;

Considerato che:

le pubbliche amministrazioni centrali, regionali e locali, e altri soggetti pubblici come enti di regolazione, enti produttori di servizi economici, enti a struttura associativa, enti produttori di servizi assistenziali, ricreativi e culturali, enti e istituzioni di ricerca, e istituti zooprofilattici sperimentali sono inclusi nell' ambito soggettivo di applicazione del Decreto NIS 2 secondo la classificazione "Soggetti essenziali e soggetti importanti" in base ai criteri individuati dall'art. 6 del citato Decreto NIS 2;
con determinazione del direttore generale di ACN n. 136430 del 12 aprile 2025, il Consiglio regionale del Piemonte è stato individuato quale soggetto importante;
il d.lgs. 138 del 2024 impone ai soggetti qualificati come importanti l'adozione di misure minime di sicurezza, organizzative e tecniche;
il Consiglio regionale è tenuto ad adempiere agli obblighi previsti dal d.lgs. 138/2024 e dalla l. 90/2024, ad aggiornare periodicamente le proprie politiche ICT nel Piano Integrato di Attività e Organizzazione e nel Piano Triennale per l'Informatica, a promuovere la formazione continua del personale e dei dirigenti e adottare misure di sicurezza basate su criteri di proporzionalità, resilienza e accountability;

Dato atto che, ai fini dell'attuazione delle misure di sicurezza previste dal d.lgs. 138/2024, il Consiglio regionale è tenuto, fra

l'altro, a dotarsi di idonea documentazione in merito all'adozione delle medesime;

Dato altresì atto che nell'ambito della documentazione già adottata dal Consiglio regionale rientra anche il *"Piano generale di attuazione della direttiva (UE) 2022/2555 "Nis 2" e del d.lgs. 138/2024 in Consiglio regionale del Piemonte"* (o anche solo Piano generale di attuazione NIS 2), che, sebbene non previsto espressamente dalla normativa, è stato introdotto e approvato con deliberazione dell'Ufficio di Presidenza n. 318 del 18 dicembre 2025, quale strumento di indirizzo strategico volto a rafforzare la capacità dell'Ente di prevenzione, gestione e risposta alle minacce cibernetiche, andando oltre i meri adempimenti normativi e perseguendo un modello di sicurezza proattivo e documentato;

Considerato che il citato Piano generale di attuazione NIS 2 costituisce lo strumento di riferimento per il monitoraggio degli adempimenti del Consiglio regionale e per la verifica periodica dello stato di attuazione delle misure previste dal Decreto NIS 2, e deve essere aggiornato in relazione all'evoluzione normativa e attuativa, alle indicazioni dell'ACN e alle esigenze organizzative dell'Ente;

Vista la determinazione dirigenziale n. A0304C/88/2026 dell'8 ottobre 2026 *"NIS 2 - Adozione delle misure di sicurezza di base di cui all'allegato 1 alla determinazione del Direttore generale dell'Agenzia per la cybersicurezza nazionale (ACN) n. 379907 del 19 dicembre 2025"*, di approvazione di parte della documentazione di cui il Consiglio regionale deve dotarsi al fine di adempiere gli obblighi previsti dal decreto NIS 2, nel rispetto del Vademecum NIS e del calendario dei termini (soggetti 2025) adottati da ACN e trasmessi al Consiglio regionale del Piemonte in data 14 settembre 2026 (ns. prot. n. 20207 del 14/09/2026);

Rilevato che il contenuto della citata determinazione dirigenziale incide sul Piano generale di attuazione NIS 2 e, in particolare, sul capitolo 9, dove sono elencati i documenti di cui il Consiglio regionale deve dotarsi al fine di adempiere gli obblighi imposti dal decreto NIS 2;

Ritenuto pertanto di procedere all'aggiornamento del capitolo 9 del citato "*Piano generale di attuazione della direttiva (UE) 2022/2555 "NIS 2" e del D.lgs. 138/2024 in Consiglio regionale del Piemonte*" nonché, contestualmente, di sottoporre a revisione generale l'intero documento, anche al fine di evidenziare lo stato di attuazione delle misure previste dal Decreto NIS 2 da parte del Consiglio regionale;

Ritenuto quindi di procedere all’approvazione della versione aggiornata (V02) del "*Piano generale di attuazione della direttiva (UE) 2022/2555 “NIS 2” e del d.lgs. 138/2024 in Consiglio regionale del Piemonte*", **allegata** alla presente deliberazione per farne parte integrante e sostanziale;

L'Ufficio di Presidenza, all'***unanimità dei presenti***,

D E L I B E R A

1. di dare atto che le premesse costituiscono parte integrante e sostanziale della presente deliberazione;

2. di approvare il “*Piano generale di attuazione della direttiva (UE) 2022/2555 "NIS 2" e del d.lgs. 138/2024 in Consiglio regionale del Piemonte. Aggiornamento (V02)*", **allegato** alla presente deliberazione per farne parte integrante e sostanziale;

3. di dare atto che la versione V02 integra e aggiorna la versione precedentemente approvata con deliberazione dell’Ufficio di Presidenza n. 318 del 18 dicembre 2025.

Piano generale di attuazione della direttiva (UE) 2022/2555 "NIS 2" e del d.lgs. 138/2024 in Consiglio regionale del Piemonte

Stato delle variazioni

Versione	Atto di approvazione	Paragrafo o pagina	Descrizione della variazione
V01	DUP 318/2025	Intero documento	Prima versione
V02	Da completare a seguito dell'approvazione	Intero documento	Tutti i capitoli: aggiornati riferimenti normativi e a provvedimenti ACN. Par. 3.3: inseriti numero e data DUP di adozione Piano V01. Capp. 6, 8, 9, 10: aggiornati. Cap. 7: modificato titolo, aggiornato.

Sommario

STATO DELLE VARIAZIONI 1

1 SCOPO DEL DOCUMENTO PIANO GENERALE DI ATTUAZIONE 3

2 CONTESTO NORMATIVO: INTRODUZIONE ALLA DIRETTIVA NIS 2 3

2.1 Premessa 3

2.2 Quadro normativo di riferimento 3

2.2.1 Normativa europea 3

2.2.2 Principi chiave della NIS 2 4

2.2.3 Normativa nazionale di contesto e strumenti di programmazione e pianificazione rilevanti ai fini dell'attuazione della direttiva NIS 2 (Decreto legislativo 4 settembre 2024, n. 138) 4

2.2.4 Normativa nazionale di recepimento 5

2.2.5 Natura e competenze dell'Agenzia per la Cybersicurezza Nazionale (ACN) 6

3 RUOLO DEL CONSIGLIO REGIONALE DEL PIEMONTE E RESPONSABILITÀ DEGLI ORGANI DI AMMINISTRAZIONE E DIRETTIVI 6

3.1 Premessa 6

3.2 Classificazione del Consiglio regionale come soggetto importante ai sensi della NIS 2 7

3.3 Responsabilità degli organi amministrativi e direttivi (art. 23 d.lgs. 138/2024) 7

3.4 Attività e servizi rilevanti ai fini NIS 2 8

4 PIANO GENERALE DI ATTUAZIONE DELLA DIRETTIVA NIS 2 8

4.1 Premessa 8

4.2 Funzione del Piano 9
4.3 Il valore dell'adeguamento alla NIS 9
5 ADEMPIMENTI DECRETO LEGISLATIVO 4 SETTEMBRE 2024, N. 138 9
6 REGISTRAZIONE DEL CONSIGLIO REGIONALE E AGGIORNAMENTO DELLE INFORMAZIONI SUL PORTALE NIS 2 ACN (ADEMPIMENTO ART. 7) 11
7 PIANO DELLA FORMAZIONE (ADEMPIMENTO ART. 23) 12
8 PIANO DI IMPLEMENTAZIONE DELLE MISURE DI SICUREZZA DI BASE (ADEMPIMENTO ART. 24) 13
9 EVIDENZE DOCUMENTALI 14
10 ELENCO DEI SISTEMI INFORMATIVI E DI RETE RILEVANTI 16
10.1 Criteri per individuare i sistemi informativi e di rete rilevanti 16
10.2 Elenco sistemi informativi e di rete rilevanti 16
10.3 Autenticazione multifattore (MFA) 17
11 NOTIFICA DEGLI INCIDENTI (ADEMPIMENTO ART. 25) 17
12 ORGANIZZAZIONE PER LA SICUREZZA 18
13 AGGIORNAMENTO E REVISIONE DEL DOCUMENTO 19

1 Scopo del documento Piano generale di attuazione

Il presente Piano generale di attuazione della direttiva NIS 2 (Network and Information Security) è finalizzato a delineare un quadro sistematico e organico delle misure, delle responsabilità e delle procedure adottate dal Consiglio regionale del Piemonte per assicurare un elevato livello di sicurezza informatica e resilienza dei propri servizi informatici e infrastrutturali. Il documento individua le azioni da intraprendere, i soggetti responsabili e le modalità operative necessarie a garantire la protezione dei dati e la continuità dei servizi, promuovendo un approccio integrato tra sicurezza informatica e tutela dei dati personali.

La sua redazione non costituisce un adempimento previsto dal decreto legislativo 4 settembre 2024, n. 138, ma rappresenta una scelta di governo consapevole da parte dell'Ente, che ha ritenuto opportuno dotarsi di uno strumento di indirizzo strategico volto a rafforzare la propria capacità di prevenzione, gestione e risposta alle minacce cibernetiche, andando oltre i meri adempimenti normativi e perseguendo un modello di sicurezza proattivo e documentato.

Per il Consiglio regionale, come si evince dagli obiettivi strategici degli ultimi anni, la cybersicurezza è una componente strutturale dell'azione amministrativa e costituisce garanzia essenziale di trasparenza, efficienza e tutela dei cittadini e delle imprese piemontesi nell'ecosistema digitale regionale. In tale prospettiva, il Consiglio ha da tempo investito, anche attraverso il Piano di sviluppo informatico, nel potenziamento delle proprie infrastrutture e in iniziative continuative di formazione e sensibilizzazione degli utenti sui temi della cybersicurezza. Gli adempimenti NIS 2 si innestano quindi in un percorso di rafforzamento della sicurezza informatica già avviato da tempo.

2 Contesto normativo: introduzione alla direttiva NIS 2

2.1 Premessa

Il presente capitolo illustra il quadro normativo europeo e nazionale di riferimento in materia di cybersicurezza e disciplina gli obblighi di adeguamento che coinvolgono il Consiglio regionale del Piemonte, quale soggetto rientrante nel perimetro applicativo della direttiva (UE) 2022/2555, nota come "direttiva NIS 2". L'obiettivo è fornire una cornice chiara, completa e coerente, che consenta di orientare le azioni organizzative e tecniche dell'Ente nel rispetto delle disposizioni europee e nazionali in materia di sicurezza delle reti e dei sistemi informativi.

Ai fini del presente documento, per semplicità espositiva, il termine "NIS" è utilizzato in forma abbreviata per riferirsi alla direttiva NIS 2 e alla relativa disciplina nazionale di attuazione.

2.2 Quadro normativo di riferimento

2.2.1 Normativa europea

La direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un **livello comune elevato di cybersicurezza nell'Unione**, ha sostituito la precedente direttiva (UE) 2016/1148 "NIS 1", introducendo un sistema più omogeneo di prevenzione, gestione e risposta agli incidenti informatici.

Essa si inserisce in un più ampio contesto strategico delineato dall'Unione europea, comprendente il Cybersecurity Act (reg. (UE) 2019/881), il Cyber Resilience Act (reg. (UE) 2024/2847) e la strategia europea per la sicurezza digitale 2020 –2030.

2.2.2 Principi chiave della NIS 2

La direttiva NIS 2 si fonda su alcuni **principi essenziali,** volti a garantire un approccio organico alla cybersicurezza:

- **gestione del rischio**: ogni ente, pubblico o privato, deve valutare i rischi informatici e adottare misure adeguate a prevenirli o mitigarli;
- **obblighi di notifica degli incidenti**: ogni incidente informatico significativo (cioè un evento di sicurezza informatica che compromette la disponibilità, l'integrità, l'autenticità o la riservatezza di reti e sistemi informativi con un impatto rilevante sui servizi) deve essere comunicato tempestivamente alle autorità competenti, secondo modalità e tempi definiti;
- **governance interna**: gli enti devono nominare figure responsabili della sicurezza informatica, dotarsi di politiche interne e procedure chiare per la gestione dei rischi;
- **cooperazione internazionale**: la direttiva promuove lo scambio di informazioni e le migliori pratiche tra Stati membri e tra enti pubblici e privati;
- **protezione dei servizi essenziali e digitali**: assicurare la continuità operativa dei servizi critici e delle infrastrutture fondamentali è un obiettivo primario.

2.2.3 Normativa nazionale di contesto e strumenti di programmazione e pianificazione rilevanti ai fini dell'attuazione della direttiva NIS 2 (decreto legislativo 4 settembre 2024, n. 138)

L'adeguamento alla direttiva NIS 2 si innesta in un quadro più ampio di riforme nazionali, tra le quali rilevano, in particolare:

- decreto legislativo 30 marzo 2001, n. 165 – Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche;
- decreto legislativo 30 giugno 2003, n. 196, così come modificato dal decreto legislativo 10 agosto 2018, n. 101;
- decreto legislativo 7 marzo 2005, n. 82 – Codice dell'Amministrazione Digitale (CAD);
- regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE - Regolamento generale sulla protezione dei dati (GDPR);
- decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni dalla legge 18 novembre 2019, n. 133, Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica (e di disciplina dei poteri speciali nei settori di rilevanza strategica);
- decreto-legge 14 giugno 2021, n. 82 convertito con modificazioni dalla legge 4 agosto 2021, n. 109, Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale;

- decreto-legge 21 marzo 2022, n. 21 convertito con modificazioni dalla legge 20 maggio 2022, n. 51, Misure urgenti per contrastare gli effetti economici e umanitari della crisi ucraina;
- decreto legislativo 31 marzo 2023, n. 36 così come modificato dal decreto legislativo 31 dicembre 2024, n. 209 – Codice dei contratti pubblici;
- legge 28 giugno 2024, n. 90 – Disposizioni in materia di cybersicurezza per le pubbliche amministrazioni e i soggetti pubblici e privati operanti in settori strategici.

Tra gli strumenti di programmazione e pianificazione rilevanti ai fini dell'attuazione della direttiva NIS 2 risultano:

- PIAO – Piano Integrato di Attività e Organizzazione, nel quale sono confluiti:
  - PTPCT – Piano Triennale di Prevenzione della Corruzione e della Trasparenza;
  - Piano della Formazione del Personale;
  - Piano dei Fabbisogni di Personale e Piano della Performance;
- Piano Triennale per l'Informatica nella Pubblica Amministrazione;
- Piano Nazionale di Cybersicurezza;
- Linee guida ACN.

2.2.4 Normativa nazionale di recepimento

L'Italia ha recepito la direttiva NIS 2 con il d. lgs. n. 138/2024, in vigore dal 16 ottobre 2024, che definisce:

- l'elenco dei soggetti "essenziali" e "importanti" (art. 3 e allegati I-IV);
- le competenze dell'Agenzia per la Cybersicurezza Nazionale (ACN) quale Autorità nazionale competente NIS;
- le procedure di registrazione e vigilanza (artt. 6–9);
- gli obblighi di governance, formazione, adozione di misure di sicurezza e notifica degli incidenti (artt. 23–24-25);
- il regime sanzionatorio (artt. 38–39).

Inoltre, introduce gli adempimenti per l'adeguamento alla direttiva europea, di cui al successivo capitolo 5, i quali, in estrema sintesi, si possono così riassumere:

- adozione di misure tecniche e organizzative per ridurre i rischi informatici;
- piani di continuità operativa per garantire il funzionamento dei servizi critici in caso di attacco;
- obbligo di segnalazione di incidenti significativi all'Agenzia per la Cybersicurezza Nazionale (ACN);
- monitoraggio continuo dei sistemi e aggiornamento delle misure di sicurezza.

Infine, all'articolo 38, vengono individuate le sanzioni amministrative a carico dei soggetti inadempienti.

Nel seguito del presente documento il termine «NIS» è utilizzato, per brevità, in luogo di «NIS 2».

2.2.5 Natura e competenze dell'Agenzia per la Cybersicurezza Nazionale (ACN)

L'Agenzia per la Cybersicurezza Nazionale (ACN) è il soggetto nazionale di riferimento per la cybersicurezza in Italia. Istituita con funzioni di coordinamento strategico, indirizzo e supervisione, l'ACN opera sotto la responsabilità del Presidente del Consiglio dei ministri e dell'Autorità delegata per la Sicurezza della Repubblica.

Tra i principali compiti dell'ACN si annoverano:

- l'elaborazione e il coordinamento dell'attuazione della Strategia nazionale di cybersicurezza;
- il monitoraggio degli incidenti informatici rilevanti, la raccolta di segnalazioni e l'analisi del rischio cyber a livello nazionale;
- l'attività di controllo, promozione di linee guida, indirizzi operativi e supporto alle pp.aa. e agli operatori privati nei processi di adeguamento normativo;
- la promozione di progetti di sviluppo tecnologico e formazione nel settore della cybersicurezza, al fine di sviluppare le competenze necessarie e rafforzare l'autonomia strategica nazionale.

L'ACN rappresenta un interlocutore centrale non solo per l'adeguamento normativo, ma anche per la cooperazione operativa in caso di incidenti e per l'allineamento alle best-practice nazionali.

Non è solo un'autorità di controllo, ma è il regolatore tecnico della cybersicurezza nazionale. Le sue determinazioni sono vincolanti.

Essa emana il Catalogo Nazionale delle Misure Minime di Cybersicurezza. Questo documento tecnico è lo standard di riferimento per tutte le implementazioni. Ad esempio, la misura sull'Autenticazione a più Fattori (MFA) dovrà seguire le specifiche tecniche di robustezza definite nel Catalogo ACN.

L'ACN ha la facoltà di richiedere in qualsiasi momento al Consiglio regionale del Piemonte la documentazione relativa alla valutazione del rischio (la Gap Analysis) e ai piani di attuazione, per verificare l'effettiva adozione delle misure.

3 Ruolo del Consiglio regionale del Piemonte e responsabilità degli organi di amministrazione e direttivi

3.1 Premessa

Il Consiglio regionale del Piemonte è l'Assemblea legislativa rappresentativa dei cittadini piemontesi. Esso esercita funzioni di indirizzo e controllo politico-amministrativo nei confronti della Giunta regionale e approva, attraverso l'Ufficio di Presidenza, i programmi e i piani strategici di sviluppo istituzionale.

Nell'ambito degli obiettivi strategici dell'Ente, l'Ufficio di Presidenza del Consiglio regionale:

- approva con deliberazione i Piani triennali per l'informatica del Consiglio Regionale (SICR), volti alla digitalizzazione e all'innovazione dei servizi, che costituiscono obiettivo e programma da attuare da parte delle competenti strutture ai sensi dell'articolo 16, della l.r. n. 23 del 28.07.2008;

- integra nel PIAO gli obiettivi di sicurezza e affidabilità dei sistemi informativi, conformemente alle previsioni della legge 90/2024, del d.lgs. 138/2024 e delle Linee guida NIS – Specifiche di base predisposte da ACN.

Il Consiglio regionale del Piemonte opera quindi in un contesto in cui la continuità operativa digitale è inscindibile dalla funzionalità istituzionale.

3.2 Classificazione del Consiglio regionale come soggetto importante ai sensi della NIS 2

Tra le novità principali del d.lgs 138/2024, vi è la distinzione tra soggetti "essenziali" e soggetti "importanti". Tale classificazione si basa su elementi di criticità del settore, oltre che su alcune soglie dimensionali, ossia parametri quantitativi relativi al fatturato o al numero di dipendenti.

A seguito delle valutazioni condotte secondo i criteri del più volte richiamato d. lgs. 138/2024, il **Consiglio regionale del Piemonte è stato individuato tra i "soggetti importanti" ai sensi dell'art. 3, comma 2**.

Tale individuazione comporta in particolare:

- responsabilità diretta degli organi di amministrazione e direttivi (art. 23);
- obblighi di adozione di misure di sicurezza proporzionate ai rischi (art. 24);
- obblighi in materia di notifica di incidente (art. 25);
- controlli e verifiche ex post da parte dell'ACN.

3.3 Responsabilità degli organi amministrativi e direttivi (art. 23 d.lgs. 138/2024)

La normativa attribuisce agli organi di amministrazione e direttivi le **responsabilità** di approvare, sovrintendere e verificare l'attuazione delle misure di gestione dei rischi di sicurezza informatica, **riassumibili nei seguenti criteri:**

- **responsibility**: approvazione delle modalità di implementazione delle misure di sicurezza e gestione dei rischi (art. 23, c. 1, lett. a);
- **accountability:** vigilanza sull'attuazione delle misure e rendicontazione delle attività (lett. b);
- **liability**: responsabilità legale per violazioni dell'art. 20 della Direttiva ("Governance").

Tali organi sono inoltre tenuti a:

- seguire formazione specifica in materia di sicurezza informatica (art. 23, c. 2, lett. a);
- promuovere formazione periodica per tutto il personale (lett. b);
- ricevere informazioni tempestive sugli incidenti e sulle notifiche (c. 3).

Con **deliberazione n. 198 del 30 luglio 2025**, l'Ufficio di Presidenza ha individuato quali "organi di amministrazione e direttivi" i Direttori del Consiglio regionale e la Responsabile del settore Sistemi informativi e banca dati Arianna.

Con **deliberazione n. 318 del 18 dicembre 2025**, di approvazione del presente Piano generale di attuazione, l'Ufficio di Presidenza ha espunto dagli "organi di amministrazione e direttivi" la Responsabile del settore Sistemi informativi e banca dati Arianna.

3.4 Attività e servizi rilevanti ai fini NIS 2

Le attività che rendono il Consiglio regionale soggetto NIS 2 sono quelle che:

- **supportano la continuità delle funzioni fondamentali riconosciute dalla Costituzione alle assemblee legislative regionali** (legislative, indirizzo, controllo);
- **gestiscono dati pubblici, personali e particolari** (atti, nomine, informazioni personali di dipendenti, dati di bilancio, ecc.);
- **contribuiscono alla trasparenza e alla legalità amministrativa** (pubblicazione atti, gestione contratti);
- **garantiscono sicurezza fisica e operativa** di sedi e persone;
- **hanno un impatto esterno** su cittadini, enti locali e soggetti istituzionali.

Possono essere quindi individuate le seguenti categorie di attività e servizi rilevanti ai fini NIS 2:

Categoria NIS 2	**Attività/Servizi del Consiglio regionale**
Servizi istituzionali	Supporto all'Assemblea e agli organi istituzionali
Servizi amministrativi di supporto	Gestione bilancio, personale, gare, contratti
Servizi di trasparenza e comunicazione pubblica	Siti web, amministrazione trasparente
Servizi di sicurezza e continuità	Gestione sedi, accessi, vigilanza, emergenze

4 Piano generale di attuazione della direttiva NIS 2

4.1 Premessa

La digitalizzazione dei processi ha creato un patrimonio informativo vastissimo e di rilevanza critica per l'azione amministrativa. Questa evoluzione, sebbene fondamentale per l'efficienza e la trasparenza, ha esposto l'Ente a una nuova e crescente tipologia di minaccia: il rischio cibernetico.

Gli attacchi moderni non sono casuali: si tratta di campagne mirate, spesso finanziate e condotte da attori statali o da gruppi criminali organizzati, che vedono le amministrazioni pubbliche come obiettivi ad alto valore per l'estrazione di dati riservati o per l'interruzione di servizi essenziali.

Un attacco basato su malware di tipo estorsivo che blocchi il sistema di gestione degli atti o una violazione della normativa in materia di protezione dei dati personali tramite un data breach non sono semplici inconvenienti tecnici, ma incidenti di sicurezza significativi che compromettono la fiducia del cittadino e mettono a rischio la sovranità digitale della Regione.

Il recepimento della direttiva NIS 2 segna un passaggio strategico per la sicurezza informatica del Consiglio regionale del Piemonte, imponendo un modello di governance condivisa e responsabilità diffusa.

L'Ente si impegna pertanto a:

- assicurare la piena conformità al d.lgs. 138/2024 e alla l. 90/2024;

- aggiornare periodicamente le proprie politiche ICT nel Piano Triennale e nel PIAO;
- promuovere la formazione continua del personale e dei dirigenti;
- adottare misure di sicurezza basate su criteri di proporzionalità, resilienza e accountability.

4.2 Funzione del Piano

Il Piano generale di attuazione NIS serve a tradurre in azioni concrete le disposizioni della direttiva europea, adattandole al contesto organizzativo dell'Ente. In sintesi, **il Piano stabilisce che cosa deve essere fatto, chi è responsabile e come si deve agire per garantire la sicurezza informatica, in un'ottica di interoperabilità organizzativa e normativa, in primo luogo con la protezione dei dati personali**.

Esso, pertanto, si propone di fornire il quadro, non solo operativo, delle misure e iniziative adottate dal Consiglio regionale del Piemonte al fine di:

- adeguarsi alla normativa NIS;
- identificare i servizi essenziali e le infrastrutture informatiche critiche dell'Ente;
- definire ruoli e responsabilità in materia di sicurezza informatica;
- introdurre misure preventive e procedure di risposta agli incidenti;
- promuovere la formazione e la consapevolezza del personale;
- favorire la collaborazione con gli organismi nazionali competenti (come l'Agenzia per la Cybersicurezza Nazionale – ACN e il CSIRT Italia).

4.3 Il valore dell'adeguamento alla NIS

Adeguarsi alla NIS significa anche rafforzare la fiducia dei cittadini nei confronti dei servizi digitali della pubblica amministrazione. Un sistema sicuro e ben gestito non solo protegge i dati personali ma assicura che i servizi restino sempre disponibili e funzionanti anche in situazioni critiche.

Questo Piano rappresenta, dunque, un impegno collettivo dell'Ente: un passo importante verso una gestione più matura, responsabile e sostenibile della sicurezza informatica. Conoscere e applicare i principi contenuti nella NIS 2 ci aiuta a costruire una pubblica amministrazione più sicura, resiliente e moderna, capace di affrontare con competenza le sfide digitali del presente e del futuro.

5 Adempimenti decreto legislativo 4 settembre 2024, n. 138

I principali adempimenti previsti dal decreto NIS sono:

1. Registrazione e aggiornamento dati

Obbligo: registrazione o aggiornamento sulla piattaforma digitale dell'Autorità nazionale competente NIS (ACN), con comunicazione di ragione sociale, indirizzo e recapiti aggiornati, designazione di un punto di contatto con recapiti aggiornati, tipologia di soggetto di cui agli allegati I, II, III e IV.

Scadenza registrazione e invio dichiarazione annuale: dal 1° gennaio al 28 febbraio di ogni anno (art. 7, comma 1).

Scadenza invio aggiornamento annuale: dal 15 aprile al 31 maggio di ogni anno (art. 7, comma 4).

Aggiornamento continuo (in corso d'anno): ogni modifica va comunicata tempestivamente e comunque entro 14 giorni (art. 7, comma 7).

Obbligo: aggiornamento sulla piattaforma digitale dell'Autorità nazionale competente NIS (ACN) dei dati inerenti a spazio di indirizzamento IP pubblico e nomi di dominio in uso o nella disponibilità del soggetto, responsabili di cui all'articolo 38, comma 5 - indicando il ruolo presso il soggetto e i loro recapiti aggiornati, compresi gli indirizzi e-mail e i numeri di telefono - sostituto del punto di contatto di cui al comma 1, lettera c), indicando il ruolo presso il soggetto e i recapiti aggiornati, compresi gli indirizzi e-mail e i numeri di telefono.

2. Obblighi per gli Organi di amministrazione e direttivi

Obbligo: approvare le modalità di implementazione delle misure, supervisionare l'attuazione delle misure di sicurezza e garantire che le risorse siano adeguate, promuovere programmi di formazione per dirigenti e personale coinvolto nella gestione della sicurezza informatica, integrare la gestione del rischio cyber nella governance complessiva dell'ente, rispondere delle violazioni (il mancato rispetto di tali obblighi può comportare responsabilità amministrativa e sanzioni pecuniarie (art. 23)).

3. Gestione del rischio e misure di sicurezza

Obbligo: adozione di misure tecniche, operative e organizzative adeguate e proporzionate per la gestione dei rischi informatici (art. 24).

Dettaglio misure: analisi dei rischi, gestione degli incidenti, continuità operativa, sicurezza della catena di approvvigionamento, gestione delle vulnerabilità, formazione del personale, uso della crittografia, controllo accessi, autenticazione a più fattori (art. 24, comma 2). Le misure di sicurezza di base applicabili sono stabilite dalla determinazione ACN n. 379907 del 19 dicembre 2025, allegato 1.

4. Notifica degli incidenti

Obbligo: notifica tempestiva al CSIRT Italia di ogni incidente significativo che impatti sulla fornitura dei servizi (art. 25). La tassonomia di incidente significativo è descritta nell'Allegato 3 della determinazione del Direttore generale dell'Agenzia per la cybersicurezza nazionale n. 379907/2025.

Tempistiche: pre-notifica tempestiva e comunque entro 24 ore, notifica completa tempestiva e comunque entro 72 ore, relazione finale entro un mese (art. 25, comma 5).

5. Comunicazione agli utenti

Obbligo: comunicazione degli incidenti significativi e delle minacce informatiche rilevanti agli utenti dei servizi coinvolti, ove opportuno e sentito il CSIRT Italia (art. 25, commi 9-10).

6. Accordi di condivisione delle informazioni

Obbligo: notifica all'ACN della partecipazione o del recesso da eventuali accordi di condivisione di informazioni sulla sicurezza informatica (art. 17, commi 2-4).

7. Audit e scansioni di sicurezza

Obbligo: esecuzione di audit e scansioni di sicurezza su richiesta dell'Autorità nazionale competente NIS (ACN), in caso di incidenti o violazioni (art. 35, comma 3; art. 37, comma 3).

8. Generale collaborazione con l'Autorità nazionale

Obbligo: collaborazione con l'Autorità nazionale competente NIS (ACN) e con il CSIRT Italia per tutte le attività di vigilanza, monitoraggio e supporto (art. 38, comma 10).

9. Elencazione e categorizzazione delle attività e dei servizi

Obbligo: predisposizione e aggiornamento sulla piattaforma ACN dell'elenco delle attività e dei servizi dell'Ente, ricondotti alle macro-aree e classificati secondo i livelli di impatto minimo, basso, medio e alto previsti dalla det. ACN n. 155238/2026, con le modalità procedurali stabilite dalla det. ACN n. 127437/2026.

Scadenza categorizzazione annuale: dal 1° maggio al 30 giugno di ogni anno (art. 30, comma 1).

6 Registrazione del Consiglio regionale e aggiornamento delle informazioni sul portale NIS 2 ACN (adempimento art. 7)

L'art. 7, co. 1 del d.lgs. 138/2024 ha introdotto - per i soggetti di cui al precedente art. 3, tra i quali rientra il Consiglio regionale - l'obbligo di registrazione sulla piattaforma digitale e di aggiornamento della registrazione resa disponibile dall'Autorità nazionale competente NIS (ACN), nel periodo compreso tra il 1° gennaio e il 28 febbraio di ogni anno successivo alla data di entrata in vigore del decreto. Le informazioni da fornire nell'ambito di tale registrazione sono: la ragione sociale, l'indirizzo e i recapiti aggiornati, compresi gli indirizzi e-mail e i numeri di telefono, la designazione di un punto di contatto, indicando il ruolo presso il soggetto e i recapiti aggiornati, compresi gli indirizzi e-mail e i numeri di telefono, la tipologia di soggetto di cui all'allegato III del decreto.

Il Consiglio regionale ha effettuato la registrazione in data 15/01/2025 con dichiarazione n. DNISA00001035.

L'ACN, con determinazione del Direttore generale n. 136430 del 12/04/2025, ha individuato il Consiglio regionale del Piemonte quale soggetto importante, attribuendogli il codice identificativo ITU6WR99 e inserendolo nel relativo elenco. Tale inserimento è stato successivamente notificato all'Ente con specifica comunicazione prot. n. 8893 del 14/04/2025.

L'art. 7, co. 4 del d.lgs. 138/2024 prevede, a carico dei soggetti che hanno ricevuto la suddetta comunicazione, l'obbligo di fornire e aggiornare, mediante la medesima piattaforma digitale, tra il 15 aprile e il 31 maggio di ogni anno successivo alla data di entrata in vigore del decreto, le informazioni previste dalle lettere a), b), c) e d) dello stesso comma; l'art. 7, comma 7 prevede invece che l'aggiornamento delle informazioni vada comunicato tempestivamente tramite piattaforma digitale entro 14 giorni dalla variazione.

L'ACN, in considerazione dell'elevato numero di richieste di supporto avanzate in merito dai soggetti NIS, ha differito il termine del 31/05/2025 al 31/07/2025, con comunicazione tramite

PEC prot. n. 11963 del 27/05/2025. Tali informazioni sono state fornite dal Punto di contatto in data 31/07/2025.

Il Consiglio regionale ha effettuato la registrazione per l'anno 2026 in data 16/02/2026 con dichiarazione n. DNISA00037151.

L'ACN ha notificato la permanenza dell'Ente nell'elenco dei soggetti NIS importanti con specifica comunicazione prot. n. 8652 del 15/04/2026.

Sempre in data 16/02/2026 è stata effettuata la classificazione dei dati e dei servizi digitali dell'Ente, convalidata dall'ACN con nota prot. n. 3626 del 19/02/2026, successivamente aggiornata in data 31/07/2026 e convalidata con nota prot. n. 18018 del 03/08/2026.

In data 23/06/2026, il Punto di contatto del Consiglio regionale ha inviato l'elenco riguardante la categorizzazione delle attività e dei servizi dell'Ente tramite il Portale dei servizi ACN, come da ricevuta prot. n. 14875 del 23/06/2026.

Le modalità di aggiornamento annuale e continuo delle informazioni sono attualmente disciplinate dalla det. ACN n. 127437/2026.

7 Piano della formazione (adempimento art. 23)

La direttiva NIS, tra le misure previste per aumentare la resilienza dei paesi dell'Unione europea agli attacchi informatici, impone l'obbligo di formazione sulla cybersicurezza per il personale dei soggetti individuati, inclusa la dirigenza, e sottolinea l'importanza della diffusione di una cultura aziendale della sicurezza informatica.

Il requisito concernente il Piano di formazione viene soddisfatto mediante la programmazione formativa del Consiglio regionale contenuta nel PIAO anno per anno vigente e nei relativi aggiornamenti periodici.

Il Consiglio regionale del Piemonte da diversi anni mette a disposizione dei propri dipendenti corsi di formazione tesi a garantire loro piena consapevolezza nell'utilizzo delle nuove tecnologie nella gestione delle attività istituzionali; tuttavia, nel triennio 2024 – 2026 l'approccio alla materia si è evoluto in modo sostanziale.

Nel 2024 la formazione sull'adozione della direttiva NIS 2 e sul risk management è stata riservata alle figure apicali e agli addetti alla protezione dei dati, mentre la generalità dei dipendenti completava l'articolato progetto triennale sulle competenze digitali proposto dal Dipartimento della Funzione Pubblica sulla piattaforma Syllabus, che forniva, tra l'altro, gli elementi di base sul tema della sicurezza informatica.

Nel corso del 2025 l'attività formativa in questo ambito è stata decisamente incrementata: tutti i dipendenti hanno ricevuto una formazione specifica sulla cybersecurity e sui rischi connessi all'introduzione dell'intelligenza artificiale (15 ore di formazione per ogni dipendente), mentre i dipendenti individuati come referenti per la sicurezza informatica o per la protezione dei dati personali hanno seguito corsi di livello avanzato su risk management e IA (oltre 20 ore in media per ogni dipendente). Si deve sottolineare come alcuni dipendenti abbiano di propria iniziativa approfondito questi argomenti, iscrivendosi a corsi di livello specialistico. I dirigenti, il DPO, la Responsabile del settore Sistemi informativi e archivistici e i funzionari maggiormente coinvolti

nell'applicazione della direttiva NIS 2 hanno seguito corsi di livello avanzato e specialistico sugli stessi temi, con un focus particolare sulla mastering compliance, approfondendo anche le implicazioni etiche che l'introduzione dell'intelligenza artificiale solleva (18 ore di formazione in media per dipendente).

Nel 2026 i progetti formativi dedicati alla transizione digitale e alla sicurezza informatica, saldandosi con gli obiettivi di performance dell'Ente, mirano a dare piena realizzazione all'idea di governance by design che ispira la direttiva NIS 2. I dipendenti, oltre a seguire corsi di approfondimento sulla cybersecurity e sulla protezione dei dati (10 ore di formazione per dipendente) sono stati coinvolti in un progetto denominato "Laboratorio delle competenze digitali", che proseguirà nel 2027 e che, proponendosi in prima istanza di fornire le necessarie conoscenze per la redazione di documenti accessibili, si sviluppa in forma laboratoriale, consentendo ai partecipanti di approfondire le proprie competenze digitali sotto la guida di colleghi esperti. L'estensione temporale del progetto (10 ore in un arco di sei mesi), la possibilità di confrontarsi in una community, le prove pratiche calate sul lavoro concreto dei diversi uffici hanno prodotto una maggiore e più diffusa consapevolezza nell'utilizzo delle nuove tecnologie. Anche i corsi di addestramento informatico, per l'utilizzo dei diversi applicativi gestionali, sono stati decisamente incrementati e contribuiscono alla diffusione di una cultura organizzativa in cui l'utilizzo dell'informatica è integrato nativamente in qualsiasi processo. In un'ottica di miglioramento continuo delle competenze del personale, a seguito dello svolgimento, nel corso del 2026, delle attività formative programmate in materia di protezione dei dati personali, nel 2027 sarà assicurata la prosecuzione delle attività formative e di aggiornamento, rivolte, in particolare, all'approfondimento di specifiche tematiche connesse al trattamento dei dati personali, alla sicurezza dei trattamenti e all'impiego consapevole delle nuove tecnologie nei processi dell'Ente, con un approccio orientato non solo agli aspetti teorici e normativi, ma soprattutto all'analisi e alla gestione di casi pratici. Ai dipendenti che seguono le tematiche legate al lavoro agile è stato, inoltre, assegnato un corso di formazione di livello avanzato, che affronta, tra l'altro, il tema delle competenze digitali necessarie a questa modalità lavorativa.

Infine, nel 2026, coloro che in Consiglio regionale si occupano dell'applicazione della direttiva NIS 2, oltre alla formazione specifica già fruita negli scorsi mesi (una media di 6 ore per dipendente), seguiranno un master di 24 ore sull'intelligenza artificiale, che fornirà non solo un approfondimento sugli aspetti normativi della sua introduzione nella P.A, ma anche sulla cybersecurity e sulle strategie per l'integrazione dell'IA nei processi delle amministrazioni.

8 Piano di implementazione delle misure di sicurezza di base (adempimento art. 24)

L'articolo 24 del decreto NIS disciplina gli obblighi in materia di misure di gestione dei rischi per la sicurezza informatica prevedendo che i soggetti essenziali e importanti adottino misure tecniche, operative e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete che i soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi.

Le modalità e le specifiche di base per l'adempimento dei suddetti obblighi sono state stabilite dalla determinazione dell'Agenzia per la Cybersicurezza Nazionale n. 379907 del 19 dicembre 2025, che ha aggiornato la precedente determinazione n. 164179 del 14 aprile 2025, da qui in poi indicata come **determina 379907/2025**, che riporta i seguenti allegati tecnici:

- **Allegato 1:** misure di sicurezza di base per i soggetti importanti;
- **Allegato 2**: misure di sicurezza di base per i soggetti essenziali;
- **Allegato 3**: incidenti significativi di base per i soggetti importanti;
- **Allegato 4**: incidenti significativi di base per i soggetti essenziali.

Il termine per l'adozione delle misure di sicurezza di base è fissato in **diciotto mesi** dalla ricezione, da parte del soggetto NIS, della comunicazione di inserimento nell'elenco dei soggetti NIS. Il termine per l'adempimento dell'obbligo di notifica degli incidenti significativi di base è fissato in **nove mesi** dalla ricezione, da parte del soggetto NIS, della medesima comunicazione.

L'Allegato 1 include **87 requisiti**, di cui:

- **19 requisiti** da implementare entro il **31 dicembre 2025**;
- **68 requisiti** da implementare entro il **12 ottobre 2026**.

9 Evidenze documentali

Il Consiglio regionale, in quanto soggetto NIS importante, ai fini dell'attuazione delle misure di sicurezza e dell'attestazione dell'effettiva implementazione delle stesse, deve essere in possesso o provvedere all'elaborazione di una serie di documenti.

A seguire sono riportati i principali documenti richiesti raggruppati per tipologie:

- **elenchi**: personale dell'organizzazione di sicurezza informatica, sistemi ai quali è possibile accedere da remoto;
- **inventari**: apparati fisici, servizi, sistemi e applicazioni software, servizi erogati dai fornitori, fornitori;
- **piani**: gestione dei rischi, business continuity e disaster recovery, trattamento dei rischi, gestione delle vulnerabilità, adeguamento, formazione in materia di sicurezza informatica, risposta agli incidenti;
- **politiche di sicurezza informatica**: per almeno i requisiti riportati nella tabella 1 in appendice all'Allegato 1, per i soggetti importanti, e all'allegato 2, per i soggetti essenziali, della determina **379907/2025**;
- **procedure**: in relazione agli specifici requisiti per i quali sono richieste;
- **registri**: esiti del riesame delle politiche, attività formazione dei dipendenti.

In base al proprio contesto, ogni soggetto NIS può decidere come organizzare la propria documentazione richiesta da una specifica misura, ad esempio raggruppando i contenuti in un unico documento o distribuendoli tra più documenti.

Per alcuni di questi documenti, elencati di seguito, è richiesta l'approvazione da parte degli organi amministrativi e direttivi:

- Organizzazione per la sicurezza informatica;
- Politiche di sicurezza informatica;
- Valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete;
- Piano di trattamento del rischio;
- Piano di gestione delle vulnerabilità;

- Piano di adeguamento;
- Piano di continuità operativa;
- Piano di ripristino in caso di disastro;
- Piano di gestione delle crisi;
- Piano di formazione;
- Piano per la gestione degli incidenti di sicurezza informatica.

A fini di raccordo organico in materia di continuità operativa e gestione delle crisi, si ritiene opportuno adottare anche il seguente ulteriore documento:

- Modello metodologico per la continuità operativa e la gestione delle crisi.

Nella tabella seguente è contenuto l'elenco dei documenti richiesti dalla normativa NIS che il Consiglio regionale provvederà ad elaborare. Si riporta l'atto che approverà il documento, la scadenza che deve essere rispettata (nella prima fase si distingue solo tra 31/12/2025 e 12/10/2026).

Il presente documento, riportato nella prima riga della tabella, non è espressamente previsto dalla normativa NIS; tuttavia, si è ritenuto opportuno redigerlo e sottoporlo all'approvazione dell'Ufficio di Presidenza, al fine di disporre di uno strumento di governance e di monitoraggio del piano generale degli adempimenti.

Documento	Atto di approvaz.	Scadenza
Piano generale di attuazione	DUP	31/12/2025
Organizzazione per la sicurezza informatica	DD	31/12/2025
Elenco personale organizzazione per la sicurezza informatica	DD	31/12/2025
Piano per la gestione degli incidenti di cybersicurezza e dei data breach	DUP	31/12/2025
Elenco servizi informativi e di rete rilevanti	DUP	12/10/2026
Disciplinare degli strumenti informatici (aggiornamento)	DUP	31/12/2025
Valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete	DD	12/10/2026
Politiche di sicurezza informatica	DD	12/10/2026
Piano di trattamento del rischio	DD	12/10/2026
Piano di gestione delle vulnerabilità	DD	12/10/2026
Piano di adeguamento	DD	12/10/2026
Piano di continuità operativa	DD	12/10/2026

Piano di ripristino in caso di disastro	DD	12/10/2026
Piano di gestione delle crisi	DD	12/10/2026
Piano di formazione (contenuto nel PIAO del Consiglio regionale 2026-2028, par. 3.3.5, approvato con DUP 23/2026)	DD	12/10/2026

10 Elenco dei sistemi informativi e di rete rilevanti

Per i requisiti (**13** requisiti per i soggetti importanti e **22** requisiti per i soggetti essenziali) in cui è presente la clausola "… *per almeno i sistemi informativi e di rete rilevanti* …", il soggetto NIS ha la facoltà di limitare **l'ambito di applicazione** delle relative disposizioni ai sistemi **informativi e di rete rilevanti**, definiti – ai sensi dell'articolo 1 della determina ACN 379907/2025 – come i *sistemi informativi e di rete la cui compromissione comporterebbe un impatto significativo sulla riservatezza, integrità e disponibilità delle attività e dei servizi per i quali il soggetto rientra nell'ambito di applicazione del decreto NIS*.

La misura GV.OC-04 richiede di mantenere un elenco dei sistemi informativi e di rete rilevanti. In fase di prima applicazione il Consiglio regionale ha ritenuto di definire i criteri con i quali individuare tali sistemi e di predisporne un primo elenco da aggiornare periodicamente, anche in considerazione di alcuni importanti vincoli (es. servizi condivisi con altri Enti). Nel 2026 sono stati svolti approfondimenti con CSI Piemonte e con gli altri Enti consorziati, a seguito dei quali si sono confermati i criteri e si è pervenuti all'elenco riportato nel paragrafo 10.2.

10.1 Criteri per individuare i sistemi informativi e di rete rilevanti

I criteri per valutare la rilevanza dei sistemi informativi e di rete sono:

- prendere in considerazione solo sistemi informativi e di rete di supporto alle categorie di attività e servizi dell'ente rilevanti ai fini NIS (rif. 3.*4 Attività e servizi rilevanti ai fini NIS 2*);
- valutare se l'interruzione del sistema informativo o di rete ha un impatto trasversale sugli utenti interni o esterni (sì/no);
- valutare se l'interruzione del sistema informativo o di rete trasversale ha conseguenze bloccanti per altri sistemi informativi o di rete dell'Ente (sì/no);
- valutare se l'interruzione del sistema informativo o di rete trasversale ha un impatto significativo sulla confidenzialità, integrità o disponibilità dei sistemi informativi o di rete dell'Ente (sì/no);

10.2 Elenco sistemi informativi e di rete rilevanti

I sistemi informativi e di rete rilevanti del Consiglio regionale, individuati tramite i criteri sopra esposti, sono di seguito elencati:

- sistema di autenticazione ai servizi applicativi;
- sistemi e servizi di rete dati;
- sistemi di supporto all'attività legislativa e istituzionale;
- sito web istituzionale del Consiglio regionale.

Si tratta di servizi affidati in house a CSI Piemonte. I livelli di servizio sono indicati in specifico allegato del Catalogo dei Servizi che ogni anno viene approvato dagli enti consorziati.

10.3 Autenticazione multifattore (MFA)

Il Consiglio regionale, in ottemperanza al requisito PR.AA-03 («Utenti, servizi e hardware sono autenticati»), ha avviato, a partire da maggio 2025, l'adozione graduale di soluzioni di autenticazione multifattore (MFA) per gli utenti del proprio sistema informativo. Il completamento dell'attivazione dell'MFA per tutti gli utenti è raggiunto da ottobre 2026.

11 Notifica degli incidenti (adempimento art. 25)

L'articolo 25 del d.lgs. 138/2024 impone sia ai soggetti qualificati "essenziali" sia a quelli "importanti" **l'obbligo di notificare ogni incidente che ha un impatto significativo sulla fornitura dei loro servizi**.

Il termine per l'adempimento dell'obbligo di notifica degli incidenti significativi di base è fissato in nove mesi dalla ricezione, da parte del soggetto NIS, della comunicazione di inserimento nell'elenco dei soggetti NIS, **per il Consiglio regionale da gennaio 2026**, e prevede l'approvazione del **Piano per la gestione degli incidenti di sicurezza informatica** da parte degli organi di amministrazione e direttivi.

La notifica dev'essere effettuata al CSIRT, che è entità, all'interno dell'Agenzia per la cybersicurezza nazionale (ACN), che si occupa di prevenire, analizzare e rispondere agli incidenti di sicurezza informatica.

Un incidente è significativo se:

- ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;
- ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

L'Allegato 3 della determinazione del Direttore generale dell'Agenzia per la cybersicurezza nazionale del 19 dicembre 2025, n. 379907 individua anche le tipologie di incidenti significativi secondo il seguente schema:

Codice	Descrizione
IS-1	Il soggetto NIS ha evidenza della perdita di riservatezza, verso l'esterno, di dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.
IS-2	Il soggetto NIS ha evidenza della perdita di integrità, con impatto verso l'esterno, di dati di sua proprietà o sui quali esercita il controllo, anche parziale.
IS-3	Il soggetto NIS ha evidenza della violazione dei livelli di servizio attesi dei suoi servizi e/o delle sue attività, sulla base dei livelli di servizio atteso (SL) definiti ai sensi della misura DE.CM-01.

L'articolo 25, stabilisce anche che i soggetti interessati trasmettano al CSIRT la segnalazione degli incidenti significativi con le seguenti modalità e tempistiche:

- entro 24 ore, pre-notifica (segnalazione) che, ove possibile, indichi se l'incidente possa ritenersi il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero;
- entro 72 ore, notifica che, ove possibile, aggiorni le informazioni della pre-notifica e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione;
- su richiesta del CSIRT, relazione intermedia con aggiornamenti sulla situazione;
- entro 30 giorni, relazione finale che comprenda:

1. una descrizione dettagliata dell'incidente, ivi inclusi la sua gravità e il suo impatto;
2. il tipo di minaccia o la causa originale (root cause) che ha probabilmente innescato l'incidente;
3. le misure di attenuazione adottate e in corso;
4. ove noto, l'impatto transfrontaliero dell'incidente;

- se l'incidente è ancora in corso dopo 30 giorni, una relazione mensile sui progressi e una relazione finale entro un mese dalla conclusione della gestione dell'incidente.

I termini per gli obblighi di notifica decorrono dal momento in cui è acquisita l'evidenza dell'incidente.

12 Organizzazione per la sicurezza

Il modello di governance della sicurezza del Consiglio regionale del Piemonte si basa su una governance multilivello, che assicura la responsabilità diretta degli organi di vertice e una chiara distinzione tra ruoli decisionali, di coordinamento e operativi.

In coerenza con quanto richiesto dalle misure di sicurezza di base (rif. cap. 8), con riferimento alla funzione di governo, categoria ruoli e responsabilità, codice GV.RR-02:

1. è definita, approvata dagli organi di amministrazione e direttivi, e resa nota alle articolazioni competenti del soggetto NIS, l'organizzazione per la sicurezza informatica e ne sono stabiliti ruoli e responsabilità;
2. è mantenuto un elenco aggiornato del personale dell'organizzazione di cui al punto 1 avente specifici ruoli e responsabilità ed è reso noto alle articolazioni competenti del soggetto NIS;
3. all'interno dell'organizzazione per la sicurezza informatica di cui al punto 1, sono inclusi il punto di contatto, e almeno un suo sostituto, di cui alla determina adottata ai sensi dell'articolo 7, comma 6 del decreto NIS.

Queste informazioni sono definite nel documento "Organizzazione per la sicurezza informatica", approvato, unitamente ai documenti correlati, con determinazione dirigenziale rep. n. A0304B/396/2025 del 29/12/2025, comunicato a tutto il personale e pubblicato sulla rete intranet dell'Ente.

13 Aggiornamento e revisione del documento

Nel contesto del Consiglio regionale, i Direttori sono individuati quali organi di amministrazione e direttivi ai sensi dell'art. 23 del d.lgs. 138/2024. In tale veste, essi, tra l'altro, approvano le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica, sovrintendono all'attuazione degli obblighi previsti dal decreto NIS, sono destinatari delle informazioni periodiche sugli incidenti e sull'esposizione al rischio, rispondono delle eventuali violazioni degli obblighi di sicurezza e curano la propria formazione in materia di cybersicurezza, promuovendo adeguati percorsi formativi per il personale.

Il presente Piano generale di attuazione NIS costituisce lo strumento di riferimento per il monitoraggio dell'avanzamento degli adempimenti e per la verifica periodica dello stato di attuazione delle misure previste.

Verrà aggiornato ogniqualvolta se ne manifesti la necessità e sarà sottoposto all'approvazione dell'Ufficio di Presidenza.

L'aggiornamento del presente documento (V02) è stato curato dal gruppo di lavoro inter-direzionale dedicato agli adempimenti NIS, i cui componenti sono elencati di seguito.

Anna Amorosini
Erica Botticelli
Francesco Canuto Anelli
Tiziana Cardella
Fabrizio d'Alonzo
Cinzia Ghiazza
Daniela Oberto
Angela Scelzi