Codice A1911A
D.D. 16 ottobre 2026, n. 426
D.Lgs. 4 settembre 2024 n. 138. Disposizioni per adempiere agli obblighi in materia di sicurezza informatica. Approvazione dell'impianto documentale NIS da parte degli organi di amministrazione e direttivi di cui all'articolo 23, comma 1, lett. a) del Decreto NIS.

REGIONE PIEMONTE

ATTO DD 426/A1911A/2026 DEL 16/10/2026

DETERMINAZIONE DIRIGENZIALE
A19000- COMPETITIVITA' DEL SISTEMA REGIONALE
A1911A - Sistema informativo regionale

OGGETTO: D.Lgs. 4 settembre 2024 n. 138. Disposizioni per adempiere agli obblighi in materia di sicurezza informatica. Approvazione dell'impianto documentale NIS da parte degli organi di amministrazione e direttivi di cui all'articolo 23, comma 1, lett. a) del Decreto NIS

Premesso che:

- La Direttiva (UE) 2022/2555 (NIS 2) del Parlamento Europeo e del Consiglio, stabilisce misure volte a garantire un livello comune 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;

- il D.Lgs. 4 settembre 2024 n. 138, , anche definito "Decreto NIS", recepisce la direttiva (UE) 2022/2555 (NIS 2), e dispone all'art 3, comma 6 che "Il presente decreto si applica, altresì, anche indipendentemente dalle loro dimensioni, alle pubbliche amministrazioni di cui all'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, ricomprese nelle categorie elencate nell'allegato III";

- il sopra richiamato "Decreto NIS" dispone all'art. 6, comma 3 che "sono considerati soggetti importanti i soggetti di cui all'articolo 3 che non sono considerati essenziali ai sensi dei commi 1 e 2 del presente articolo";

- il D.Lgs. 4 settembre 2024 n. 138, all'art 23 espressamente sancisce che gli organi di amministrazione e gli organi direttivi dei soggetti importanti "approvano le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica adottate da tali soggetti ai sensi dell'articolo 24";

- il "Decreto NIS" prevede altresì all'art 24 che i soggetti importanti "adottano misure tecniche, operative e organizzative adeguate e proporzionate, secondo le modalità e i termini di cui agli articoli 30, 31 e 32, alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete

che tali 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";

- il D.Lgs. 4 settembre 2024 n. 138, all'art 38, comma 6, in caso di violazione delle disposizioni in esso contenute, stabilisce l'applicazione delle sanzioni amministrative nei confronti delle persone fisiche "ivi inclusi agli organi di amministrazione e gli organi direttivi di cui all'articolo 23 dei soggetti essenziali e dei soggetti importanti, nonché di quelle che svolgono funzioni dirigenziali a livello di amministratore delegato o rappresentante legale di un soggetto essenziale o importante" .

Premesso inoltre che:

- ai sensi dell'articolo 7, comma 1, lettera c), del "decreto NIS" il Presidente della Regione Piemonte ha delegato in data 19 febbraio 2025, tramite atto di delega resa in forma di dichiarazione sostitutiva di Atto di Notorietà, ex articolo 47 del D.P.R. n. 445/2000, quale "Punto di contatto" il Responsabile del Settore "Sistema informativo regionale" di Regione Piemonte, nominato con DGR 3-474 del 03 dicembre 2024 "Referente per la Cybersicurezza", in ottemperanza all'articolo 8 della legge n. 90/2024.

- la D.G.R.- n. 15-1430 del 28 luglio 2025 "Decreto legislativo n. 138/2024. Determinazione del Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale n. 136430 del 12 aprile 2025, di riconoscimento della Regione Piemonte quale entità critica per la cybersicurezza nazionale. Disposizioni per adempiere agli obblighi in materia di sicurezza informatica" ha individuato i soggetti da indicare nella sezione del Portale NIS appositamente dedicata all'elencazione degli organi amministrativi e direttivi dell'Ente, come previsto dall'articolo 23 comma 1, lettera c), del medesimo del "decreto NIS";

- la D.G.R. sopra richiamata ha disposto di rinviare a successivi provvedimenti le valutazioni di impatto dei necessari interventi in materia.

Considerato che

- le disposizioni di cui al D.Lgs. 4 settembre 2024 n. 138 si applicano anche a Regione Piemonte in virtù del disposto dell'art. 3 comma 6 e dell'allegato III del decreto legislativo stesso;

- Regione Piemonte è considerato "soggetto importante" ai fini dell'applicazione della normativa di riferimento per le ragioni di cui in premessa;

- nel mese di ottobre 2026 è fissato il termine ultimo per l'attuazione delle misure di sicurezza di base, in conformità al periodo di 18 mesi decorrente dalla data della comunicazione via PEC di inserimento nell'elenco dei soggetti NIS;

- l'obbligo di approvazione dell'impianto documentale, coerente con le FAQ ACN ODA.10 e le linee guida NIS sulle specifiche di base non è delegabile, in quanto la normativa vigente e le indicazione ACN presenti nelle FAQ ODA.8 attribuiscono esclusivamente agli organi di amministrazione e direttivi la responsabilità collegiale di approvare tali atti. Tale obbligo, infatti, rimane in capo agli organi suddetti e non può essere trasferito né a singoli membri, né ad altri organi o funzioni del soggetto NIS, indipendentemente dal modello di governance adottato dall'Ente;

Considerato inoltre che

- Per adempiere a tali obblighi, il Referente per la Cybersicurezza ha predisposto, grazie alla collaborazione del Gruppo di lavoro interdirezionale “Attuazione della normativa in materia di Cybersicurezza”, istituito con Determinazione Dirigenziale n. 11/A1000A/2025 del 22/01/2025, un impianto documentale organico, conforme ai requisiti delle misure di sicurezza, che ne richiede l’approvazione e comprende i seguenti elementi:

- Organizzazione per la sicurezza informatica
- Politiche di sicurezza informatica
- Valutazione del rischio relativo 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

Gli organi amministrativi di vertice, come individuati dal decreto legislativo 138/2024, hanno:

- già provveduto ad approvare il Piano per la gestione degli incidenti di sicurezza informatica, attraverso validazione da parte del Comitato di Coordinamento dei Direttori in data 16 dicembre 2025 e successiva approvazione mediante Determinazione Dirigenziale da parte di ciascun Direttore regionale;
- condiviso, esaminato e validato i restanti documenti dell’impianto documentale NIS nella seduta del Comitato di Coordinamento dei Direttori tenutasi il 6 ottobre 2026, stabilendo di procedere alla loro adozione e approvazione con successivo specifico atto.

Ritenuto opportuno, per quanto sopra esposto:

- approvare in qualità di componente degli organi di amministrazione e direttivi di cui all’articolo 23, comma 1, lett. a) del decreto NIS, l’impianto documentale sopra elencato condiviso in sede di Comitato di Coordinamento Direttori e contenente le funzioni di gestione, indirizzo e pianificazione strategica che riflettono e declinano i requisiti delle misure di sicurezza di cui agli obblighi riferiti ai “soggetti importanti” come Regione Piemonte.

- dare effettiva attuazione ai documenti, mantenendo un costante rapporto con il Referente per la Cybersicurezza e le strutture organizzative dell’Ente competenti per materia.

Attestato che, in esito all’istruttoria sopra richiamata, il presente provvedimento non comporta effetti contabili diretti né effetti prospettici sulla gestione finanziaria, economica e patrimoniale della Regione Piemonte.

Tutto ciò premesso e considerato

IL DIRIGENTE

Richiamati i seguenti riferimenti normativi:

- il decreto legislativo n. 82/2005 "Codice dell'Amministrazione Digitale";
- il decreto legislativo n. 196/2003 "Codice in materia di protezione dei dati personali";
- la legge n. 190/2012 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione";
- la L. 2 luglio 2024 n. 90 "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici";
- la deliberazione della Giunta regionale n. 3-2182/2026/XII del 30/01/2026: Approvazione del Piano integrato di attività e organizzazione (PIAO) della Giunta regionale del Piemonte per gli anni 2026-2028, ai sensi del Decreto Legge n. 80 del 9 giugno 2021, convertito in Legge n. 113 del 6 agosto 2021.;
- il regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR);
- il D.Lgs. 4 settembre 2024 n. 138 "Decreto Legislativo e regolamenti associati per l'adozione della Diretiva NIS2";
- la D.G.R.- n. 15-1430 del 28 luglio 2025 "Decreto legislativo n. 138/2024. Determinazione del Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale n. 136430 del 12 aprile 2025, di riconoscimento della Regione Piemonte quale entità critica per la cybersicurezza nazionale. Disposizioni per adempiere agli obblighi in materia di sicurezza informatica";
- la D.D. 22 gennaio 2025, n. 11 "Istituzione del Gruppo di lavoro interdirezionale "Attuazione della normativa in materia di Cybersicurezza"' '.;

determina

per le motivazioni in premessa che integralmente e sostanzialmente si richiamano:

- di prendere atto del verbale del Comitato di Coordinamento Direttori del 06/10/2026 con il quale sono stati condivisi, esaminati e validati i documenti che verranno approvati dagli organi di amministrazione e direttivi di cui all’articolo 23, comma 1, lett. a) del decreto NIS;

- di approvare e adottare in qualità di componente degli organi di amministrazione e direttivi di cui all’articolo 23, comma 1, lett. a) del decreto NIS , come convenuto, i seguenti documenti:

- Organizzazione per la sicurezza informatica
- Politiche di sicurezza informatica
- Valutazione del rischio relativo 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

, di cui all’Allegato 1, parte integrante e sostanziale della presente provvedimento per quanto di competenza;

La presente determinazione non è soggetta alla pubblicazione ai sensi del Decreto Legislativo 33/2013, in materia di trasparenza nella pubblica amministrazione.

La presente determinazione sarà pubblicata sul Bollettino ufficiale della Regione Piemonte ai sensi dell'articolo 61 dello Statuto e dell' art. 5 della legge regionale 12 ottobre 2010, n. 22.

IL DIRIGENTE (A1911A - Sistema informativo regionale)
Firmato digitalmente da Luigi Citriniti