Codice A1007E
D.D. 19 febbraio 2026, n. 55
D.Lgs. 4 settembre 2024 n. 138. Disposizioni per adempiere agli obblighi in materia di sicurezza informatica. Presa d'atto e adozione del ''Piano di Formazione in materia di Sicurezza Informatica''.

ATTO DD 55/A1007E/2026 DEL 19/02/2026

DETERMINAZIONE DIRIGENZIALE
A1000A - DIREZIONE DELLA GIUNTA REGIONALE
A1007E - Sviluppo e Capitale umano

OGGETTO: D.Lgs. 4 settembre 2024 n. 138. Disposizioni per adempiere agli obblighi in materia di sicurezza informatica. Presa d'atto e adozione del "Piano di Formazione in materia di Sicurezza Informatica".

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 9 luglio 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 pro-tempore 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;

- il Decreto NIS 2 prevede espressamente l'adozione di misure organizzative e di formazione continua del personale, ivi compresi i dirigenti e gli organi di vertice, finalizzate ad accrescere la consapevolezza in materia di cybersicurezza e gestione dei rischi;

- la Determinazione ACN 379907/2025 prevede che il soggetto NIS, 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, tra cui il Piano di Formazione in materia di sicurezza informatica;

- per ottemperare a tale obbligo il Settore Sviluppo e Capitale Umano, in qualità di Settore preposto alla predisposizione e gestione del Piano della Formazione, ha predisposto – in raccordo con il Settore Sistema informativo regionale - il Piano di Formazione in materia di Sicurezza Informatica, volto a definire obiettivi, contenuti formativi, destinatari, modalità di erogazione e monitoraggio degli interventi formativi in materia di sicurezza informatica;

- l’obiettivo del Piano è garantire:
• il rafforzamento delle competenze del personale in materia di Cybersicurezza;
• la diffusione della cultura della sicurezza informatica;
• la riduzione del rischio di incidenti derivanti da comportamenti non consapevoli;
• la conformità agli obblighi formativi previsti dalla normativa NIS 2;

- Gli organi amministrativi di vertice, così come previsto dal decreto legislativo 138/2024, sono stati informati del Piano nella seduta del Comitato di Coordinamento Direttori in data 16.12.2025, successivamente validato nella seduta del 03.02.2026.

Ritenuto opportuno, per quanto sopra esposto:

- adottare misure organizzative e formative finalizzate alla gestione dei rischi di cybersicurezza, attraverso l’adozione del “Piano di Formazione in materia di Sicurezza Informatica”;
- dare effettiva attuazione al Piano, in raccordo con il Referente per la Cybersicurezza.

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 in quanto finanziato da fondi statali.

Tutto ciò premesso e considerato,

IL DIRIGENTE

Richiamati i seguenti riferimenti normativi:

- il D.Lgs. n. 82/2005 "Codice dell'Amministrazione Digitale";
- il D.Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali";
- la L. 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";

determina

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

- di prendere atto del Piano di Formazione in materia di Sicurezza Informatica, validato dagli organi amministrativi di vertice, secondo quanto disposto dall'art. 23 del D. Lgs. 4 settembre 2024 n. 138;
- di adottare il "Piano di Formazione in materia di Sicurezza Informatica ", di cui all'Allegato 1, parte integrante e sostanziale della presente provvedimento.

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 (A1007E - Sviluppo e Capitale umano)
Firmato digitalmente da Marco Brandolini

Allegato

Anno 2026

MODULI PREVISTI

L'articolazione del piano formativo prevede corsi differenziati per specifici ruoli aziendali:

- Corso di Formazione per i **Soggetti Apicali**
- Corso di Formazione per **specifici Ruoli Specializzati**
- Corso di Formazione per **tutti i Dipendenti (Dirigenti e Funzionari)**

È infatti intenzione di Regione Piemonte mantenere, aggiornare e sviluppare le competenze in *ambito cyber* con un articolato programma formativo rivolto a tutto il personale.

Le persone coinvolte nell'aggiornamento formativo sono così distribuite:

Tipo corso	Partecipanti	Modalità formativa
SOGGETTI APICALI	11	In presenza
RUOLI SPECIALIZZATI	80	In presenza/FAD
DIPENDENTI	Tutto il personale regionale	In presenza/ FAD

PROGRAMMI FORMATIVI

Di seguito i programmi formativi definiti per i corsi previsti dal piano.

Corso di Formazione per Apicali

durata: 4 ore; modalità formativa: aula in presenza

Modulo 1

Conoscenze manageriali di base: Inquadramento del rischio Cyber, minacce e vulnerabilità:

1 Il contesto odierno: Cyberspazio e Cybersecurity
2 La direttiva NIS 2: Figure chiave e responsabilità degli organi Direttivi
3 Le Competenze degli organi Direttivi
  3.1 L'evoluzione del rischio Cyber
  3.2 Qualche dato (il rapporto CLUSIT).
  3.3 I problemi ed i rischi nelle aziende e negli Enti Pubblici
  3.4 Quanto può costare alla mia azienda/Ente un attacco informatico
4 Vulnerabilità e tecniche di attacco
  4.1 Le principali vulnerabilità delle infrastrutture IT
  4.2 Gli attacchi interni ed esterni
  4.3 Misure tecniche ed organizzative
5 Il fattore umano
  5.1 L'errore umano come prima causa (fattore abilitante) di attacco Cyber
  5.2 Social Engineering: mezzo di attacco sempre più usato
  5.3 Gli attacchi attraverso la posta elettronica e cellulare: phishing/smishing
  5.4 I deepfake ed attacchi con l'IA
  5.5 Gli attacchi al CEO

Modulo 2:

Competenze decisionali del manager: il “Cosa” chiedere ed il “Come” attuare”

1 Cosa significa “Fare Sicurezza”: impostare un Sistema Difensivo
  1.1 Le 3 Fasi Temporali: Prevenzione, Rilevamento, Reazione
  1.2 L’impostazione del MOGS (modello Organizzativo di gestione della Sicurezza ICT)
  1.3 La gestione del piano di rischi aziendali (metodologia e azioni)
  1.4 Elementi di Business continuity

1.5 Il monitoraggio delle attività: l'interazione degli organi direttivi con il CISO, il DPO, il responsabile Formazione, Ufficio Legale/contratti, il fornitore IT

2 Applicazione della NIS 2 in pratica (le azioni di valutazione degli Organi Direttivi)

2.1 L'impianto documentale da mantenere: il governo dei processi e regolamenti, elenchi, mappature

2.2 La Data Protection: perché non solo la Cybersecurity

2.3 Il piano formativo Cyber per i dipendenti.

2.4 La gestione degli incidenti:obblighi di notifica e azioni da attivare

Corso di Formazione per specifici Ruoli Specializzati

durata: 8 ore; modalità formativa: aula in presenza/FAD

- Introduzione al quadro normativo NIS2
- Panoramica sui requisiti e le responsabilità dei dirigenti
- Panorama attuale delle minacce cyber (ransomware, phishing, supply chain, ecc.)
- La predisposizione e gestione di un piano Cyber
- Definizione e monitoraggio delle policy di sicurezza
- Processi e procedure per la gestione degli incidenti
- Continuità operativa e Disaster Recovery
- Analisi e gestione delle vulnerabilità
- Incident Response
- Crisis Management
- Tassosonomia degli incidenti secondo ACN

Corso di Formazione per tutti i Dipendenti di Regione Piemonte

durata: 4 ore; modalità formativa: FAD

MODULO 1 Introduzione alla Direttiva NIS2

- Introduzione al modulo
- Il contesto normativo Europeo e Italiano
- NIS e NIS2 a confronto
- Come l'Italia si adegua alla NIS2

MODULO 2 I soggetti coinvolti e il loro ambito di applicazione

- Introduzione al modulo
- I soggetti Obbligati e i settori coinvolti
- Obblighi Normativi e Responsabilità

- Gestione del rischio
- Notifica degli incidenti
- Governance e Responsabilità
- Implementazione della NIS2: Ruoli, Politiche e Processi Organizzativi
- Ruoli e Responsabilità: la governance della sicurezza
- Politiche interne: formalizzazione e diffusione
- Formazione del personale: consapevolezza e reattività
- Qual è il ruolo dei fornitori ICT?

MODULO 3 Gestione degli incidenti di sicurezza informatica

- Introduzione al modulo
- Definizione di Incidente secondo NIS2
- Obblighi in materia di Sicurezza Informatica
- Sistemi Informativi e di rete Rilevanti
- Ulteriori misure di Sicurezza Informatica: Fondamenti Operativi per la Cybersecurity
- Continuità operativa, inclusi backup, disaster recovery e gestione delle crisi
- Sicurezza nello sviluppo e manutenzione dei sistemi
- Uso della crittografia e cifratura, ove opportuno
- Controllo degli accessi, gestione degli asset e affidabilità del personale
- Autenticazione multifattoriale o continua

MODULO 4 Regime sanzionatorio

- Introduzione al modulo
- Tipologie di Sanzioni
- Preparazione alle Ispezioni
- Timeline Adozione NIS2