Oggetto: Direttiva NIS 2 – Approvazione della "Politica di Gestione del Rischio per la Sicurezza Informatica", del "Piano di Gestione dei Rischi per la sicurezza informatica", del "Piano di Trattamento dei Rischi per la sicurezza informatica" e della "Politica di sicurezza informatica - Conformità e audit di sicurezza".

IL CONSIGLIO DI AMMINISTRAZIONE

- Visto il decreto legislativo 21 gennaio 2004, n. 38, recante "Istituzione dell'Istituto nazionale di ricerca metrologica (INRiM)", pubblicato sulla G. U. n. 38, del 16 febbraio 2004;
- Visto lo Statuto dell'INRiM, emanato ai sensi del D.Lgs. 25/11/2016, n. 218, in vigore dal 1° marzo 2018;
- Vista la Direttiva UE 2022/2025, entrata in vigore in data 17 gennaio 2023, che modifica il regolamento UE n. 910/2014 e la direttiva UE 2018/1972, abrogando la direttiva (UE) 2016/1148 (NIS), da recepirsi obbligatoriamente da parte di tutti gli Stati membri dell'Unione Europea;
- Visto che la suddetta Direttiva NIS 2 stabilisce misure finalizzate ad assicurare un livello elevato e uniforme di sicurezza informatica nell'Unione, definendo obblighi di governance, gestione del rischio, adozione di misure tecniche, operative e organizzative, nonché obblighi di notifica degli incidenti;
- Visto il Decreto Legislativo 4 settembre 2024, n. 138 ("Decreto NIS"), di recepimento della Direttiva UE 2022/2005, recante disposizioni per un livello comune elevato di cybersicurezza nell'Unione e richiamati, in particolare, gli obblighi posti a carico dei soggetti essenziali e importanti in materia di gestione dei rischi per la sicurezza informatica;
- Richiamato che i soggetti inclusi nel campo di applicazione del Decreto NIS sono classificati come "soggetti essenziali" o "soggetti importanti", ai sensi dell'articolo 6 del Decreto stesso;
- Dato atto che l'INRiM è stato individuato quale "soggetto importante" con comunicazione prot. 8201/2025 del 14 aprile 2025;
- Richiamato che gli organi di amministrazione e direzione dei soggetti essenziali e importanti sono tenuti agli adempimenti di cui al capo IV del decreto, ivi inclusa l'approvazione delle modalità di implementazione degli obblighi in materia di sicurezza informatica, nonché la supervisione sull'attuazione delle misure di gestione dei rischi;
- Vista la Determinazione ACN n. 379907/2025 e, in particolare, l'Allegato 1, recante misure di sicurezza di base applicabili ai soggetti importanti, con specifico riferimento alle misure relative alle politiche di sicurezza informatica, alla governance, alla gestione dei rischi, al trattamento dei rischi, alla conformità e all'audit;
- Rilevato che la disciplina NIS 2 e le misure di base ACN richiedono che la gestione del rischio per la sicurezza informatica sia definita, attuata, documentata, monitorata e periodicamente riesaminata, mediante un impianto organico di politiche, piani, registri, evidenze e responsabilità chiaramente individuate;

- Rilevato che l'INRiM ha predisposto il documento "Politica di gestione del rischio per la sicurezza informatica", codice POL-GESTIONE-RISCHIO, che stabilisce i principi, le responsabilità, il metodo, la propensione al rischio e le regole adottate dall'Istituto per la gestione dei rischi di sicurezza informatica, in coerenza con il D. Lgs. 138/2024, con la Direttiva NIS 2 e con la Determinazione ACN n. 379907/2025;
- Rilevato che la predetta Politica definisce, tra l'altro, il processo strutturato di identificazione, analisi, ponderazione, trattamento, monitoraggio e riesame dei rischi relativi ai sistemi informativi e di rete, con particolare riferimento ai sistemi rilevanti, nonché i criteri di classificazione dei rischi inerenti e residui, le soglie di tolleranza e le modalità di accettazione dei rischi residui;
- Rilevato che l'INRiM ha predisposto il "Piano di gestione dei rischi per la sicurezza informatica", codice PIANO-GESTIONE-RISCHI, che definisce il processo di gestione dei rischi per la sicurezza informatica dell'Istituto, individuando ruoli, responsabilità, input, output, periodicità, modalità operative, registro dei rischi, flussi di comunicazione, reporting e aggiornamento:
- Rilevato che l'INRiM ha predisposto il "Piano di trattamento dei rischi per la sicurezza informatica", codice PIANO-TRATT-RISCHI, volto a documentare, pianificare, assegnare, monitorare e sottoporre ad approvazione il trattamento dei rischi di sicurezza informatica sul perimetro IT, OT, IoT, cloud e servizi rilevanti;
- Rilevato che il Piano di trattamento dei rischi individua, per ciascun ambito di intervento, le opzioni di trattamento, le misure da attuare, le priorità, i responsabili, le tempistiche, i rischi residui attesi, le eventuali misure compensative e le evidenze di chiusura;
- Rilevato che, secondo l'impostazione adottata dall'Istituto, i rischi residui classificati come "bassi" sono accettabili in via ordinaria se documentati e monitorati, i rischi residui "medi" richiedono motivazione documentata e monitoraggio periodico, mentre i rischi residui "alti" non sono accettabili in via ordinaria e richiedono trattamento prioritario ovvero, nei casi consentiti, accettazione temporanea espressa da parte del Consiglio di amministrazione, corredata da motivazione e misure compensative;
- Rilevato che l'INRiM ha predisposto la "Politica di sicurezza informatica – Conformità e audit di sicurezza", codice POL-CONF-AUDIT, che stabilisce principi, regole e responsabilità per garantire la conformità normativa, la verificabilità delle politiche di sicurezza informatica, la conduzione degli audit, la gestione delle evidenze, il miglioramento continuo e la preparazione dell'Ente a eventuali verifiche esterne o richieste documentali da parte delle autorità competenti;
- Accertato che i documenti sopra richiamati costituiscono un impianto coordinato di governance della sicurezza informatica dell'Istituto, volto a disciplinare, con approccio proporzionato e basato sul rischio, le politiche, i piani, le responsabilità, le evidenze e i meccanismi di controllo necessari per il percorso di conformità al quadro NIS 2;
- Ritenuto necessario procedere all'approvazione dei suddetti documenti al fine di assicurare l'adozione formale delle politiche, dei piani e degli strumenti di gestione del rischio richiesti

dal quadro NIS 2, nonché di garantire la tracciabilità delle responsabilità, delle decisioni di trattamento e del monitoraggio dei rischi residui:

- Ritenuto altresì necessario demandare alle strutture competenti l'attuazione delle misure previste nei documenti approvati, secondo le priorità, le tempistiche e le modalità ivi indicate, con rendicontazione periodica al Consiglio di amministrazione sullo stato di avanzamento, sui rischi residui, sulle eventuali deroghe, sulle non conformità e sulle misure compensative;
- Accertato che l'attuazione delle misure previste avverrà nel rispetto della programmazione dell'Istituto, delle disponibilità di bilancio, delle procedure interne e della normativa applicabile in materia di contratti pubblici, organizzazione, protezione dei dati personali e sicurezza informatica;
- Con voti unanimi favorevoli, espressi nei modi di legge,

d e l i b e r a:

1) di approvare e adottare la "Politica di gestione del rischio per la sicurezza informatica" codice POL-GESTIONE-RISCHIO, Allegato 1, che costituisce parte integrante e sostanziale della presente Deliberazione;
2) di approvare e adottare il "Piano di gestione dei rischi per la sicurezza informatica", codice PIANO-GESTIONE-RISCHI, Allegato 2, che costituisce parte integrante e sostanziale della presente Deliberazione;
3) di approvare e adottare il "Piano di trattamento dei rischi per la sicurezza informatica", codice PIANO-TRATT-RISCHI, Allegato 3, che costituisce parte integrante e sostanziale della presente Deliberazione;
4) di approvare e adottare la "Politica di sicurezza informatica – Conformità e audit di sicurezza", codice POL-CONF-AUDIT, Allegato 4, che costituisce parte integrante e sostanziale della presente Deliberazione;
5) di dare mandato al Responsabile della sicurezza informatica, all'Unità Organizzativa "Cyber and Information Security", all'Unità Organizzativa "Sistemi Informatici e Reti" e alle ulteriori strutture competenti, ciascuna per quanto di rispettiva competenza, di procedere all'attuazione delle misure previste dai documenti approvati, secondo le priorità, le responsabilità, le tempistiche e le modalità operative in essi indicate;
6) di stabilire che i documenti approvati siano riesaminati e aggiornati secondo le periodicità in essi previste;
7) di dare atto che la presente deliberazione costituisce adempimento obbligatorio per l'INRiM, in quanto soggetto importante ai fini della direttiva NIS2, e rappresenta un presidio tecnico-organizzativo indispensabile a garantire tempestività, competenza e uniformità nella gestione degli incidenti di cybersicurezza.

Si allega:

- Allegato 1_Documento "Politica di gestione del rischio per la sicurezza informatica" – POL-GESTIONE-RISCHIO;

- Allegato 2_Documento “Piano di gestione dei rischi per la sicurezza informatica” – PIANO-GESTIONE-RISCHI;
- Allegato 3_Documetno “Piano di trattamento dei rischi per la sicurezza informatica” – PIANO-TRATT-RISCHI;
- Allegato 4_Documento “Politica di sicurezza informatica – Conformità e audit di sicurezza” – POL-CONF-AUDIT.

IL PRESIDENTE
(prof. Pietro Asinari)

Pietro
Asinari
02.07.2026
18:06:25
GMT+02:00

IL DIRETTORE GENERALE
(dott. Moreno Tivan)

Firmato digitalmente da:
Tivan Moreno
Firmato il 01/07/2026 19:33
Seriale Certificato: 4972971
Valido dal 16/10/2025 al 16/10/2028
InfoCamere Qualified Electronic Signature CA

Documento informatico sottoscritto con firma digitale ai sensi del d.lgs. 82/2005