

ATTI DEL CONSIGLIO DI AMMINISTRAZIONE - ANNO 2026

Deliberazione n. 34/2026/7 del 29 luglio 2026**Pag. 1 di 4**

Oggetto: Direttiva NIS 2 – Approvazione della “Politica sulla protezione delle reti e delle comunicazioni”, della “Politica di monitoraggio degli eventi di sicurezza”, della “Politica di risposta agli incidenti e ripristino”, del “Piano per la gestione degli incidenti di sicurezza informatica”, della Politica di gestione dell’autenticazione, delle identità digitali e del controllo accessi” e della “Politica per la sicurezza fisica”.

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 2022/2525, 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 2022/2525, 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;

ATTI DEL CONSIGLIO DI AMMINISTRAZIONE - ANNO 2026

Deliberazione n. 34/2026/7 del 29 luglio 2026**Pag. 2 di 4**

- Rilevato che l'INRiM ha predisposto il documento "Politica sulla protezione delle reti e delle comunicazioni", codice POL-PROT-RETI-COM, che stabilisce i principi, le regole e le responsabilità per la protezione delle reti, dei sistemi di interconnessione e delle comunicazioni di INRiM, in coerenza con il D. Lgs. 138/2024, con la Direttiva NIS 2 e con la Determinazione ACN n. 379907/2025;
- Rilevato che l'INRiM ha predisposto il documento "Politica di monitoraggio degli eventi di sicurezza", codice POL-MON-EVENTI-SIC, che definisce i principi, le regole e i requisiti per il monitoraggio degli eventi di sicurezza informatica, al fine di rilevare tempestivamente gli eventi rilevanti e gli incidenti, per almeno i sistemi informativi e di rete rilevanti, limitandone l'impatto e l'estensione;
- Rilevato che l'INRiM ha predisposto il documento "Politica di risposta agli incidenti e ripristino", codice POL-RISP-INC-RIP, volto a definire i principi, gli obblighi e le responsabilità per la gestione degli incidenti di sicurezza informatica dell'Ente
- Rilevato che la Politica individua, tra le misure da implementare, gli obblighi di notifica al CSIRT Italia, la comunicazione verso i soggetti interessati, il ripristino del normale funzionamento dei sistemi e l'apprendimento dagli eventi occorsi, al fine di limitare gli impatti sui servizi e sulle informazioni dell'Ente;
- Rilevato che l'INRiM ha predisposto il "Piano per la gestione degli incidenti di sicurezza informatica", codice PIANO-GEST-INC-SIC, che definisce le modalità operative adottate da INRiM per la gestione degli incidenti di sicurezza informatica, in attuazione della Politica di Risposta agli Incidenti e Ripristino;
- Rilevato che l'INRiM ha predisposto la "Politica di gestione dell'autenticazione, delle identità digitali e del controllo accessi", codice POL-AUT-ID-ACC, che definisce i principi, le regole e i requisiti per la gestione delle identità digitali, delle credenziali, dell'autenticazione e del controllo degli accessi ai sistemi informativi e di reti dell'Ente;
- Rilevato che l'INRiM ha predisposto la "Politica per la sicurezza fisica", codice POL-SIC-FIS, che stabilisce i principi, le regole e i requisiti per la protezione fisica dei sistemi informativi e di rete dell'Ente e delle aree che li ospitano, al fine di prevenire accessi fisici non autorizzati, danneggiamenti e manomissioni e sottrazioni di apparati, dati e supporti;
- Accertato che i documenti sopra richiamati costituiscono un impianto coordinato di governance della sicurezza informatica dell'Istituto, volto a disciplinare:
 - con approccio proporzionato in relazione agli incidenti e alla protezione delle reti e delle comunicazioni, le politiche, i piani, le responsabilità, le evidenze e i meccanismi di controllo, risposta e ripristino necessari per il percorso di conformità al quadro NIS 2;
 - la definizione dei principi, regole e dei requisiti per il monitoraggio degli eventi di sicurezza informatica, al fine di rilevare tempestivamente gli eventi rilevanti e gli incidenti, per almeno i sistemi informativi e di rete rilevanti, limitandone l'impatto e l'estensione
 - i principi, le regole e le responsabilità per la protezione delle reti, dei sistemi di interconnessione e delle comunicazioni di INRiM

- i principi, le regole e i requisiti per la gestione delle identità digitali, delle credenziali, dell'autenticazione e del controllo degli accessi ai sistemi informativi e di rete dell'Ente, al fine di consentire l'accesso alle sole utenze autorizzate, limitatamente a quanto necessario allo svolgimento delle attività lavorative, e di garantire la tracciabilità delle operazioni svolte
- i principi, le responsabilità e i requisiti organizzativi con cui INRiM protegge fisicamente locali, impianti, apparati, sistemi informativi, supporti e informazioni da accessi non autorizzati, danneggiamenti, manomissioni, furti e altri eventi ambientali o accidentali;
- Ritenuto necessario procedere all'approvazione dei suddetti documenti al fine di assicurare l'adozione formale delle politiche e dei piani richiesti dal quadro NIS 2;
- 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, qualora durante l'operatività ordinaria si rendessero necessarie modifiche alle politiche e ai piani di cui sopra;
- 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 sulla protezione delle reti e delle comunicazioni" codice POL-PROT-RETI-COM, Allegato 1, che costituisce parte integrante e sostanziale della presente Deliberazione;
- 2) di approvare e adottare la "Politica di monitoraggio degli eventi di sicurezza", codice POL-MON-EVENTI-SIC, Allegato 2, che costituisce parte integrante e sostanziale della presente Deliberazione;
- 3) di approvare e adottare la "Politica di risposta agli incidenti e ripristino", codice POL-RISP-INC-RIP, Allegato 3, che costituisce parte integrante e sostanziale della presente Deliberazione;
- 4) di approvare e adottare il "Piano per la gestione degli incidenti di sicurezza informatica", codice PIANO-GEST-INC-SIC, Allegato 4, che costituisce parte integrante e sostanziale della presente Deliberazione;
- 5) di approvare e adottare la "Politica di gestione dell'autenticazione, delle identità digitali e del controllo accessi, codice POL-AUT-ID-ACC, Allegato 5, che costituisce parte integrante e sostanziale della presente Deliberazione;
- 6) di approvare e adottare la "Politica per la sicurezza fisica", codice POL-SIC-FIS, Allegato 6, che costituisce parte integrante e sostanziale della presente Deliberazione;
- 7) 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

ATTI DEL CONSIGLIO DI AMMINISTRAZIONE - ANNO 2026

Deliberazione n. 34/2026/7 del 29 luglio 2026**Pag. 4 di 4**

all'attuazione delle misure previste dai documenti approvati, secondo le priorità, le responsabilità, le tempistiche e le modalità operative in essi indicate;

- 8) di stabilire che i documenti approvati siano riesaminati e aggiornati secondo le periodicità in essi previste;
- 9) 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 sulla protezione delle reti e delle comunicazioni” – POL-PROT-RETI-COM;
- Allegato 2_Documento “Politica di monitoraggio degli eventi di sicurezza” – POL-MON-EVENTI-SIC;
- Allegato 3_Documento “Politica di risposta agli incidenti e ripristino” – POL-RISP-INC-RIP;
- Allegato 4_Documento “Piano per la gestione degli incidenti di sicurezza informatica” – PIANO-GEST-INC-SIC;
- Allegato 5_Documento “Politica di gestione dell'autenticazione, delle identità digitali e del controllo accessi” – POL-AUT-ID-ACC;
- Allegato 6_Documento “Politica per la sicurezza fisica” – POL-SIC-FIS.

IL DIRETTORE GENERALE
(dott. Moreno Tivan)



Firmato digitalmente da:
Tivan Moreno
Firmato il 29/07/2026 17:58
Seriale Certificato: 4972971
Valido dal 16/10/2025 al 16/10/2028
InfoCert - Qualified Electronic Signature CA

IL PRESIDENTE
(prof. Pietro Asinari)



Pietro
Asinari
29.07.2026
19:12:14
GMT+02:00

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