

ATTI DEL CONSIGLIO DI AMMINISTRAZIONE - ANNO 2026

Deliberazione n. 39/2026/8 del 28 settembre 2026**Pag. 1 di 4**

Oggetto: Direttiva NIS 2 – Approvazione della “Politica di gestione degli asset”, della “Politica di sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete”, della “Politica di gestione dei rischi per la sicurezza informatica della catena di approvvigionamento”, della “Politica per l’affidabilità delle risorse umane” e della Politica e del Piano di “Gestione della vulnerabilità”.

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 gestione degli asset, dei rischi legati alla catena di approvvigionamento, di affidabilità delle risorse umane, nonché di gestione della vulnerabilità;
- 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 degli asset", codice POL-GESTIONE-ASSET, che stabilisce i principi, le regole e i requisiti per l'identificazione, la registrazione e il mantenimento aggiornato degli inventari degli asset hardware, software, servizi e sistemi che compongono i sistemi informativi e di rete dell'Ente, 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 sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete", codice POL-SVIL-CONF-MAN-DISM, che definisce i principi, le responsabilità e i requisiti di sicurezza applicabili all'intero ciclo di vita dei sistemi informativi e di rete, dalla progettazione e configurazione alla manutenzione, aggiornamento e dismissione, affinché tali attività siano autorizzate, tracciate e svolte secondo modalità sicure e controllate;
- Rilevato che l'INRiM ha predisposto il documento "Politica di gestione dei rischi per la sicurezza informatica della catena di approvvigionamento", codice POL-CATENA-APPROVVIGIONAMENTO, che stabilisce i requisiti per la gestione dei rischi di sicurezza informatica derivanti dalla catena di approvvigionamento dell'Istituto e, in particolare, assicura che la funzione preposta alla sicurezza informatica sia coinvolta nei processi di approvvigionamento, che i fornitori siano noti, che i requisiti di sicurezza siano definiti e inseriti nei contratti e negli accordi, e che il rischio associato alle forniture sia valutato e monitorato lungo l'intero ciclo di vita del rapporto;
- Rilevato che l'INRiM ha predisposto il documento "Politica per l'affidabilità delle risorse umane", codice POL-AFF-RUM, volto ad assicurare che la sicurezza informatica sia inclusa nelle pratiche di gestione delle risorse umane dell'Istituto e, in particolare, ad assicurare che il personale autorizzato ad accedere ai sistemi informativi e di rete siano individuati e incaricati previa valutazione di esperienza, capacità e affidabilità e siano vincolati al pieno rispetto della normativa in materia di sicurezza informatica;
- Rilevato che l'INRiM ha predisposto il documento "Politica di gestione della vulnerabilità", codice POL-GESTIONE-VULNERABILITA, che stabilisce i requisiti per il monitoraggio delle divulgazioni, l'identificazione, la classificazione, il trattamento, la registrazione e la verifica delle vulnerabilità dei sistemi informativi e di rete dell'Istituto, al fine di ridurne tempestivamente l'esposizione al rischio;
- Rilevato che l'INRiM ha predisposto altresì il "Piano di gestione delle vulnerabilità", codice PIANO-GESTIONE-VULNERABILITA, che attua la relativa Politica sopra menzionata e rende eseguibile, aggiornabile e documentabile il processo con cui INRiM monitora le divulgazioni, identifica e conferma le vulnerabilità, ne determina la priorità, pianifica e verifica il trattamento e mantiene le relative evidenze;
- Accertato che i documenti sopra richiamati costituiscono un impianto coordinato di governance della sicurezza informatica dell'Istituto, volto a disciplinare:
 - la definizione dei principi, delle regole e dei requisiti per l'identificazione, la registrazione e il mantenimento aggiornato degli inventari degli asset hardware, software, servizi e sistemi che compongono i sistemi informativi e di rete dell'Ente, ivi inclusa la loro manutenzione e dismissione, tenuto conto che gli inventari costituiscono la base conoscitiva per la gestione

ATTI DEL CONSIGLIO DI AMMINISTRAZIONE - ANNO 2026

Deliberazione n. 39/2026/8 del 28 settembre 2026**Pag. 3 di 4**

del rischio, la protezione e il monitoraggio dei sistemi, assicurando che ogni asset sia noto, associato a un responsabile e autorizzato;

- i principi, le regole e le responsabilità per la gestione dei rischi di sicurezza informatica derivanti dalla catena di approvvigionamento dell'Istituto;
- i principi, le regole e i requisiti affinché la sicurezza informatica sia inclusa nelle pratiche di gestione delle risorse umane, affinché il pieno rispetto della normativa in materia di sicurezza informatica sia garantito da tutte le persone che, in ragione di un rapporto di lavoro, collaborazione, ricerca, studio, formazione, fornitura o altra relazione con INRiM, accedono o possono accedere a sistemi, reti, dati, informazioni, locali o asset dell'Istituto.
- i principi, le responsabilità e i requisiti organizzativi con cui INRiM monitora le divulgazioni, l'identificazione, la classificazione, il trattamento, la registrazione e la verifica dei sistemi informativi e di rete dell'Istituto, al fine di ridurre tempestivamente l'esposizione al rischio;
- 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 di gestione degli asset", codice POL-GESTIONE-ASSET, Allegato 1, che costituisce parte integrante e sostanziale della presente Deliberazione;
- 2) di approvare e adottare la "Politica di sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete", codice POL-SVIL-CONF-MAN-DISM, Allegato 2, che costituisce parte integrante e sostanziale della presente Deliberazione;
- 3) di approvare e adottare la "Politica di gestione dei rischi per la sicurezza informatica della catena di approvvigionamento", codice POL-CATENA-APPROVVIGIONAMENTO, Allegato 3, che costituisce parte integrante e sostanziale della presente Deliberazione;
- 4) di approvare e adottare la "Politica per l'affidabilità delle risorse umane", codice POL-AFF-RUM, Allegato 4, che costituisce parte integrante e sostanziale della presente Deliberazione;
- 5) di approvare e adottare la "Politica di gestione della vulnerabilità", codice POL-GESTIONE-VULNERABILITA, Allegato 5, che costituisce parte integrante e sostanziale della presente Deliberazione;

ATTI DEL CONSIGLIO DI AMMINISTRAZIONE - ANNO 2026

Deliberazione n. 39/2026/8 del 28 settembre 2026**Pag. 4 di 4**

- 6) di approvare e adottare il “Piano di gestione delle vulnerabilità”, codice PIANO-GESTIONE-VULNERABILITA, 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 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 di gestione degli asset” - POL-GESTIONE-ASSET;
- Allegato 2_Documento “Politica di sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete” - POL-SVIL-CONF-MAN-DISM;
- Allegato 3_Documento “Politica di gestione dei rischi per la sicurezza informatica della catena di approvvigionamento” - POL-CATENA-APPROVVIGIONAMENTO;
- Allegato 4_Documento “Politica per l’affidabilità delle risorse umane” - POL-AFF-RUM;
- Allegato 5_Documento “Politica di gestione della vulnerabilità” - POL-GESTIONE-VULNERABILITA;
- Allegato 6_Documento “Piano di gestione delle vulnerabilità” - PIANO-GESTIONE-VULNERABILITA.

IL DIRETTORE GENERALE
(dott. Moreno Tivan)Firmato digitalmente da:
Tivan Moreno
Firmato il 28/09/2026 19:55
Seriale Certificato: 4972971
Valido dal 16/10/2025 al 16/10/2028
InfoCertum Qualified Electronic Signature CA**IL PRESIDENTE**
(prof. Pietro Asinari)Pietro
Asinari
29.09.2026
17:19:50
GMT+02:00

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