



DECRETO DEL DIRETTORE GENERALE - N. 4227 del 22/10/2026

OGGETTO: ADOZIONE DEL “MODELLO ORGANIZZATIVO PARTE GENERALE – SISTEMI INFORMATIVI E DATI ELETTRONICI” IN CONFORMITA’ ALLA DIRETTIVA (UE) 2022/2555 NIS 2 GOVERNANCE MODEL FRAMEWORK - ATTUATIVO DELLE DISPOSIZIONI DEL D.LGS. 138/2024” E DEL CORPUS DELLE POLITICHE DI SICUREZZA INFORMATICA, NONCHE’ INDIRIZZI PER L’ATTUAZIONE DEL PIANO DI ADEGUAMENTO NIS 2 – TITOLARIO 1.7.05/2026-13 ALL. 23

IL DIRETTORE GENERALE

su proposta del Direttore della SC Sistemi Informativi

PREMESSO che il Direttore della SC Sistemi Informativi dott. Fabrizio Pizzo, sottopone la proposta di provvedimento sull’ adozione del “Modello Organizzativo Parte Generale – Sistemi Informativi e Dati Elettronici” in conformità alla direttiva (UE) 2022/2555 NIS 2 Governance Model Framework - Attuativo delle disposizioni del d.lgs. 138/2024” e del corpus delle politiche di sicurezza informatica, nonché indirizzi per l’attuazione del piano di adeguamento NIS 2;

VISTI:

- il d.lgs. 30 dicembre 1992, n. 502, recante il riordino della disciplina in materia sanitaria;
- il d.lgs. 16 ottobre 2003, n. 288., come modificato dal d.lgs. 23 dicembre 2022, n. 200, recante la disciplina degli Istituti di Ricovero e Cura a Carattere Scientifico (IRCCS);
- il Regolamento (UE) 2016/679 (GDPR) e il d.lgs. 30 giugno 2003, n. 196 (Codice Privacy);
- la Direttiva (UE) 2022/2555 (Direttiva NIS 2), nonché il d.lgs. 4 settembre 2024, n. 138, avente di recepimento della predetta direttiva, con specifico riferimento agli articoli 23 e 24 che attribuiscono agli organi di amministrazione e agli organi direttivi dei soggetti essenziali la competenza esclusiva per l’approvazione delle misure di gestione dei rischi per la sicurezza informatica e la sovrintendenza alla loro attuazione;
- la DGR della Regione Lombardia n. XXII/3725 del 30.12.2024, con la quale la Giunta Regionale ha approvato l’ultimo “Aggiornamento del Piano di Organizzazione Aziendale Strategico (POAS) 2022-2024 della Fondazione Istituto di Ricovero e Cura a Carattere Scientifico (IRCCS) di diritto pubblico Ca’ Granda Ospedale Maggiore Policlinico di Milano;
- con Deliberazione Consiliare N. 86 del 29/01/2026 è stato approvato il “Piano Integrato delle Attività dell’Organizzazione - triennio 2026/2028;

PREMESSO che:

- la crescente pervasività delle tecnologie digitali nei processi sanitari, diagnostici, amministrativi e di supporto richiede un assetto di sicurezza logica, fisica e organizzativa coerente con i requisiti europei e nazionali di resilienza cibernetica e tutela dei dati;



- in attuazione di tali requisiti, la Fondazione IRCCS ha avviato un programma organico di adeguamento della propria *governance* e dei sistemi informatici, con particolare attenzione alla *compliance* documentale;
- in esito alle attività di assessment e gap analysis è stato predisposto il documento denominato "NIS 2 Governance Model Framework - Attuativo Delle Disposizioni Del D.LGS. 138/2024" (Titolario 1.7.05/2026-13 all. 1);

ATTESO che:

- il Framework costituisce il documento aziendale di indirizzo di primo livello in materia di sicurezza informatica e definisce i principi generali, il modello di governance, i ruoli, le responsabilità e gli ambiti di presidio adottati dalla Fondazione IRCCS;
- il Framework disciplina, in particolare, la gestione del rischio per la sicurezza informatica, l'affidabilità delle risorse umane, la conformità e gli audit di sicurezza, la gestione della catena di approvvigionamento, la gestione degli asset e delle vulnerabilità, la continuità operativa, il ripristino in caso di disastro, la gestione delle crisi informatiche, il controllo degli accessi, la sicurezza fisica, la formazione, la sicurezza dei dati, il ciclo di vita dei sistemi, la protezione delle reti, il monitoraggio degli eventi e la risposta agli incidenti;
- il Framework è attuato attraverso politiche, procedure, piani, istruzioni operative, registri ed evidenze, approvati e aggiornati secondo il sistema dei poteri e delle responsabilità vigente presso la Fondazione IRCCS;
- il Framework e la documentazione collegata sono stati predisposti tenendo conto delle risultanze dell'assessment e della gap analysis condotti rispetto ai requisiti applicabili;

CONSIDERATO che a supporto dell'attuazione del Framework è stato predisposto un corpus documentale di politiche di sicurezza informatica costituito dai seguenti documenti:

- Cyber Strategy Policy – (Titolario 1.7.05/2026-13 all. 2);
- Information & Cyber Risk Management Policy – (Titolario 1.7.05/2026-13 all. 3);
- Access Management Policy – (Titolario 1.7.05/2026-13 all. 4);
- Privileged Access Management Policy – (Titolario 1.7.05/2026-13 all. 5);
- Security Training & Awareness Policy – (Titolario 1.7.05/2026-13 all. 6);
- IT Supplier Management Policy – (Titolario 1.7.05/2026-13 all. 7);
- Service Level Management Policy – (Titolario 1.7.05/2026-13 all. 8);
- IT Asset Management Policy – (Titolario 1.7.05/2026-13 all. 9);
- Service Configuration Management Policy – (Titolario 1.7.05/2026-13 all. 10);
- Vulnerability e Patch Management Policy – (Titolario 1.7.05/2026-13 all. 11);
- Business Continuity Management Policy – (Titolario 1.7.05/2026-13 all. 12);
- Backup Management Policy – (Titolario 1.7.05/2026-13 all. 13);



- Data Encryption Policy – (Titolario 1.7.05/2026-13 all. 14);
- Utilizzo sicuro degli asset IT aziendali Policy – (Titolario 1.7.05/2026-13 all. 15);
- Change Management Policy – (Titolario 1.7.05/2026-13 all. 16);
- Secure Software Development Lifecycle Policy – (Titolario 1.7.05/2026-13 all. 17);
- Service Validation & Testing Policy – (Titolario 1.7.05/2026-13 all.18);
- Log Management Policy – (Titolario 1.7.05/2026-13 all. 19);
- Monitoring & Event Management Policy – (Titolario 1.7.05/2026-13 all. 20);
- Incident Management Policy – (Titolario 1.7.05/2026-13 all. 21);
- Information & Cyber Risk Assessment FrameWork – (Titolario 1.7.05/2026-13 all. 22);

CONSIDERATO ALTRESÌ che:

- il Framework e il corpus delle politiche costituiscono la base organizzativa e documentale per l'attuazione delle misure di gestione dei rischi per la sicurezza informatica;
- l'approvazione della documentazione di indirizzo non sostituisce l'attuazione operativa delle misure, che deve essere assicurata dalle strutture competenti e documentata mediante piani, registri, configurazioni, report, verbali, test e ulteriori evidenze;
- devono essere completati e mantenuti aggiornati, secondo le responsabilità e le tempistiche definite nel Piano di adeguamento NIS 2, almeno:
 - l'elenco unitario dei sistemi informativi e di rete rilevanti;
 - l'elenco dei soggetti interni ed esterni aventi specifici ruoli e responsabilità in materia di sicurezza informatica;
 - la verifica, il completamento e l'aggiornamento delle designazioni del Punto di contatto NIS, del relativo sostituto, del Referente CSIRT e degli eventuali sostituti;
 - il piano di gestione e trattamento dei rischi;
 - il piano di gestione delle vulnerabilità;
 - il piano di continuità operativa;
 - il piano di Disaster Recovery;
 - il piano di gestione delle crisi informatiche;
 - il piano di formazione in materia di sicurezza informatica;
 - il piano di gestione e notifica degli incidenti al CSIRT Italia;
 - i registri e le evidenze necessari a dimostrare l'attuazione delle misure adottate;

RITENUTO necessario:

- procedere alla formale approvazione e adozione del "NIS 2 Governance Model Framework – attuativo delle disposizioni del D.Lgs. 138/2024", quale documento aziendale di indirizzo di primo livello in materia di sicurezza informatica;



- procedere alla formale approvazione e adozione del corpus delle politiche di sicurezza informatica sopra richiamate, quali componenti del sistema aziendale di gestione della sicurezza delle reti e dei sistemi informativi;
- demandare alla SC Sistemi Informativi, con il coinvolgimento della funzione Sicurezza Informatica, della SC Ingegneria Clinica e delle ulteriori strutture competenti, il coordinamento dell'attuazione del Framework e delle politiche collegate;
- prevedere il supporto consultivo del Responsabile della protezione dei dati personali per gli aspetti relativi alla protezione dei dati personali;
- demandare alla SC Sistemi Informativi, con il coinvolgimento delle strutture competenti, la predisposizione del Piano di adeguamento NIS 2, la sua sottoposizione agli Organi competenti per l'approvazione e il successivo monitoraggio della relativa attuazione;
- assicurare il monitoraggio periodico dello stato di attuazione e la relativa rendicontazione agli Organi di amministrazione e direttivi;

RITENUTO altresì che:

- il Framework e le politiche collegate debbano essere comunicati alle articolazioni aziendali interessate, tenendo conto dei rispettivi ruoli e del principio della necessità di conoscere;
- la documentazione adottata debba essere sottoposta a riesame e aggiornamento secondo le periodicità e al verificarsi degli eventi indicati nel Framework e nelle politiche collegate;
- le responsabilità individuali e le nomine debbano essere formalizzate mediante specifici atti organizzativi, mantenuti aggiornati e resi disponibili alle strutture competenti;
- l'affidamento a fornitori o terze parti di attività operative non comporti il trasferimento delle responsabilità di governo, supervisione e controllo in capo alla Fondazione IRCCS;

CONSIDERATO che la presente proposta è formulata nel rispetto della normativa vigente in materia e che dal presente provvedimento non derivano oneri a carico del bilancio della Fondazione IRCCS;

VISTO l'art. 16, comma 2, dello Statuto della Fondazione IRCCS secondo il quale al Direttore Generale compete la gestione finanziaria, tecnica ed amministrativa dell'Ente;

PRESO ATTO che il Proponente del presente provvedimento, firmandone la proposta, a seguito dell'istruttoria effettuata, attesta la regolarità tecnico-amministrativa e la legittimità nella forma e nella sostanza;

PRESO ATTO che il Direttore della SC Sistemi Informativi, dott. Fabrizio Pizzo, proponente del presente provvedimento, ne ha dichiarato la regolarità tecnica e la legittimità;



ACQUISITI i pareri del Direttore Amministrativo, del Direttore Sanitario e del Direttore Scientifico

DECRETA

per tutti i motivi in premessa indicati, di:

1. approvare e adottare il documento denominato “NIS 2 Governance Model Framework – attuativo delle disposizioni del D.Lgs. 138/2024”, custodito agli atti a cura del Responsabile del procedimento in atti Titolario n. 1.7.05/2026-13 all. 1;
2. approvare e adottare il corpus delle politiche di sicurezza informatica richiamate in premessa, quali componenti del sistema aziendale di gestione della sicurezza delle reti e dei sistemi informativi, custodite agli atti a cura del Responsabile del procedimento;
3. stabilire che il Framework e le politiche collegate costituiscano documenti vincolanti, per quanto applicabile in funzione dei rispettivi ruoli e responsabilità, per tutte le articolazioni aziendali, il personale dipendente, convenzionato e ad altro titolo autorizzato, nonché per i fornitori e i prestatori di servizi ICT e cloud operanti per conto della Fondazione IRCCS;
4. demandare al Direttore della SC Sistemi Informativi, con il supporto della funzione Sicurezza Informatica e con il coinvolgimento della SC Ingegneria Clinica e delle ulteriori strutture competenti, il coordinamento dell’attuazione operativa, dell’aggiornamento e dell’integrazione nei processi aziendali del Framework e delle politiche approvate;
5. prevedere il supporto consultivo del Responsabile della protezione dei dati personali per gli aspetti relativi alla protezione dei dati personali e alla gestione delle violazioni dei dati personali;
6. demandare alla SC Sistemi Informativi, con il coinvolgimento delle strutture competenti, la predisposizione e l’aggiornamento del Piano di adeguamento NIS 2, recante almeno gli interventi necessari, le priorità, i responsabili, le strutture di supporto, le tempistiche e le evidenze richieste per la chiusura delle azioni, nonché la sua sottoposizione agli Organi competenti per l’approvazione e il successivo monitoraggio;
7. demandare alle strutture competenti il completamento, l’approvazione, l’attuazione e il mantenimento della documentazione operativa prevista dal Framework, inclusi gli inventari, i registri, le nomine, i piani e le procedure necessari a dimostrare l’effettiva attuazione delle misure di sicurezza;
8. stabilire che lo stato di attuazione del Framework e del Piano di adeguamento NIS 2 sia oggetto di monitoraggio periodico e di una relazione almeno annuale agli Organi di amministrazione e direttivi, ferme restando le comunicazioni straordinarie in presenza di incidenti significativi o criticità rilevanti;



9. disporre la pubblicazione, la comunicazione e la conservazione del Framework e delle politiche collegate secondo le regole del sistema documentale aziendale e tenendo conto della classificazione delle informazioni e del principio della necessità di conoscere;
10. stabilire che il Framework e le politiche siano sottoposti a riesame secondo le periodicità previste e, comunque, in occasione di rilevanti evoluzioni normative, incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai rischi;
11. dare atto che le responsabilità individuali previste dal modello di governance della sicurezza informatica sono formalizzate mediante specifici atti di nomina, disposizioni organizzative o deleghe coerenti con il sistema dei poteri vigente;
12. dare atto che il Direttore della SC Economico Finanziaria attesta la regolarità contabile del provvedimento e che da esso non derivano oneri;
13. dare atto che il presente provvedimento è messo a disposizione del Collegio Sindacale, ai sensi dell'art. 3-ter del D.lgs. n. 502/1992 e s.m. e dell'art. 12, comma 14 della L.R. n. 33/2009, così come modificata dalla L.R. n. 23/2015, mediante accesso all'intranet aziendale, nella sezione dedicata;
14. disporre la pubblicazione del presente provvedimento all'Albo online dell'azienda, dando atto che lo stesso è immediatamente esecutivo (art. 17 comma 6, L.R. n. 33/2009 così come sostituito dall'art. 1 della L.R. n. 23/2015);
15. disporre l'invio del presente decreto alle strutture interessate.

Firmato digitalmente

IL DIRETTORE GENERALE
(Dott. Matteo Stocco)