Piano di formazione in materia di sicurezza informatica

Autore: DIREZIONE IT

Tipo Documento: Aziendale

Versione	Data	Descrizione
1.0	16/09/2026	Creazione documento

Ai fini della NIS2, il presente documento tiene conto dell'inquadramento dell'Ateneo quale soggetto importante e si coordina con il sistema di gestione per la sicurezza delle informazioni e con la documentazione relativa alla certificazione ISO/IEC 27001, ove applicabile.

EXECUTIVE SUMMARY

1.1 Il contesto e la necessità di governo

Gli articoli 23 e 24 del D.Lgs. 138/2024 richiedono che gli organi di amministrazione e direttivi seguano una formazione in materia di sicurezza informatica, promuovano una formazione periodica dei dipendenti e assicurino che la formazione costituisca parte delle misure di gestione del rischio. Le misure PR.AT-01 delle specifiche di base ACN richiedono inoltre un piano approvato, formazione dedicata ai ruoli specializzati e registri aggiornati delle attività svolte e delle eventuali verifiche.

Il presente Piano stabilisce il modello permanente con cui l'Ateneo pianifica, eroga, registra e valuta la formazione NIS2. La programmazione operativa è definita nel documento separato in formato Excel «Allegato A - Programmazione annuale della formazione», aggiornato ogni anno sulla base dei rischi effettivi, delle responsabilità assegnate, degli incidenti e degli esiti di audit e riesami.

1.2 Come funziona il modello formativo

- Vertici: percorso obbligatorio, orientato a responsabilità, supervisione, decisioni sul rischio e gestione delle crisi.
- Personale: sensibilizzazione periodica sui comportamenti sicuri, sul riconoscimento delle minacce e sui canali di segnalazione.
- Ruoli specialistici: formazione dedicata e commisurata ai compiti, ai privilegi e ai sistemi gestiti.
- Programmazione annuale: traduzione dei fabbisogni nel file Excel Allegato A, con destinatari, obiettivi, modalità, tempi e verifiche.
- Tracciabilità: registrazione coordinata con la Direzione Risorse Umane - Ufficio Formazione mediante U-Web Formazione e tassonomia controllata dei tag.
- Riesame: monitoraggio di copertura ed efficacia e aggiornamento conseguente del programma formativo.

1.3 Decisioni richieste agli Organi di Ateneo

- approvare il presente Piano e assicurarne l'attuazione;
- partecipare alla formazione prevista per gli organi di amministrazione e direttivi;
- approvare o recepire annualmente, nell'ambito degli atti di programmazione competenti, il file Excel Allegato A;
- esaminare periodicamente gli indicatori di completamento, copertura ed efficacia e disporre le eventuali azioni correttive.

2 SCOPO

Il Piano definisce principi, destinatari, responsabilità e modalità per assicurare una formazione in materia di sicurezza informatica coerente con i rischi, documentata e verificabile. Costituisce il riferimento stabile per la formazione dei vertici, per la sensibilizzazione generale e per lo sviluppo delle competenze del personale che ricopre ruoli specializzati.

3 CAMPO DI APPLICAZIONE

Il Piano si applica agli organi di amministrazione e direttivi dell'Ateneo e al personale dipendente. Sono inclusi, in relazione ai compiti, ai privilegi e alle modalità di accesso ai sistemi, anche personale strutturato e non strutturato, collaboratori, assegnisti, dottorandi, personale di enti collegati, fornitori e ogni altro soggetto che operi sui sistemi informativi e di rete dell'Ateneo o ricopra ruoli rilevanti ai fini NIS. L'inclusione è formalizzata nel programma annuale, negli atti di attribuzione del ruolo o negli obblighi contrattuali applicabili.

4 RIFERIMENTI

- Direttiva (UE) 2022/2555 (direttiva NIS2);
- D.Lgs. 4 settembre 2024, n. 138, in particolare articoli 23 e 24;
- Determinazione ACN n. 379907/2025, Allegato 1 per i soggetti importanti, con particolare riferimento a GV.PO-01, PR.AT-01 e PR.AT-02;
- Guida ACN alla lettura delle specifiche di base;
- ISO/IEC 27001 e ISO/IEC 27002, ove applicabili al sistema di gestione dell'Ateneo;
- politiche, piani e procedure interne in materia di sicurezza informatica, gestione dei rischi, incidenti, continuità operativa, protezione dei dati e gestione delle risorse umane.

5 PRINCIPI DEL MODELLO FORMATIVO

Proporzionalità e orientamento al rischio. Contenuti e profondità sono commisurati ai compiti, ai privilegi, all'esposizione e alla rilevanza dei sistemi e servizi.

Differenziazione per destinatari. I percorsi distinguono vertici, popolazione generale e ruoli specialistici.

Continuità. La formazione è periodica e viene integrata in occasione di ingresso, cambio ruolo, introduzione di tecnologie, incidenti o variazioni del rischio.

Concretezza. Quando opportuno, lezioni e aggiornamenti sono affiancati da esercitazioni, simulazioni, laboratori o casi d'uso universitari.

Tracciabilità. Partecipazione, contenuti, verifiche ed esiti sono registrati in modo coerente e interrogabile.

Miglioramento continuo. Esiti delle verifiche, incidenti, audit e indicatori orientano la programmazione successiva.

6 DESTINATARI E PERCORSI FORMATIVI

6.1 Formazione obbligatoria degli organi di amministrazione e direzione

Gli organi di amministrazione e direttivi partecipano a un percorso obbligatorio che consenta loro di approvare consapevolmente le modalità di attuazione delle misure, sovrintendere agli adempimenti e valutare l'impatto dei rischi sulle attività istituzionali. Il percorso è svolto all'assunzione dell'incarico o alla prima applicazione del Piano e successivamente aggiornato secondo gli obblighi applicabili e in occasione di cambiamenti rilevanti, in particolare

modifiche normative, organizzative o di rischio.

La formazione dei vertici tratta a livello decisionale almeno:

- quadro NIS2, responsabilità degli organi e sistema di governance dell'Ateneo;
- rischio cyber, criteri di priorità, accettazione del rischio e allocazione delle risorse;
- gestione e notifica degli incidenti, continuità operativa, ripristino e gestione delle crisi;
- esercitazioni o casi decisionali coerenti con i servizi universitari rilevanti.

La partecipazione è personale ed obbligatoria per almeno 4 ore annue. Eventuali assenze sono recuperate nella prima edizione utile o mediante sessione equivalente anche on line; l'Ufficio Formazione ne monitora la regolarizzazione.

6.2 Sensibilizzazione e formazione generale del personale

L'Ateneo assicura una formazione periodica di base almeno nei seguenti argomenti, oltre a quanto già previsto in forma generale per gli organi di amministrazione e direzione:

- le principali minacce, applicando le regole di igiene informatica e segnali tempestivamente anomalie ed eventi.
- phishing e ingegneria sociale, identità e credenziali
- autenticazione multifattore
- dispositivi, lavoro remoto e aggiornamenti
- protezione delle informazioni
- uso sicuro degli strumenti cloud e di collaborazione
- canali interni di segnalazione.

La formazione è assicurata all'ingresso e in occasione di mobilità o cambio mansione e viene erogata annualmente, oltre che quando incidenti, vulnerabilità, cambiamenti normativi o tecnologici lo rendano necessario. La partecipazione è personale ed obbligatoria per almeno 8 ore annue. Eventuali assenze sono recuperate nella prima edizione utile o mediante sessione equivalente anche on line; l'Ufficio Formazione ne monitora la regolarizzazione.

6.3 Formazione dei ruoli NIS, dei Responsabili SIR e degli owner

I soggetti che ricoprono ruoli NIS, i Responsabili dei SIR e gli owner partecipano a un percorso formativo proporzionato alle responsabilità assegnate, al perimetro di competenza e al livello di rischio. Il percorso è svolto prima o subito dopo l'attribuzione del ruolo e viene aggiornato secondo gli obblighi applicabili e in occasione di cambiamenti rilevanti, inclusi quelli riguardanti il ruolo, il SIR, le responsabilità o il profilo di rischio.

La formazione tratta almeno, oltre a quanto già previsto in forma generale per gli organi di amministrazione e direzione:

- responsabilità, autorità, deleghe e matrice RACI;
- valutazione, trattamento e accettazione del rischio;
- requisiti di sicurezza, continuità operativa e gestione dei fornitori;
- gestione degli incidenti, escalation e flussi informativi;
- reporting, registrazioni e conservazione delle evidenze;
- esercitazioni e casi applicativi riferiti ai SIR e ai servizi di competenza.

La partecipazione è personale ed obbligatoria per almeno 8 ore annue. Eventuali assenze sono recuperate nella prima edizione utile o mediante sessione equivalente anche on line; l'Ufficio Formazione ne monitora la regolarizzazione.

6.4 Formazione dei ruoli tecnici e privilegiati

Il personale che svolge ruoli tecnici o dispone di privilegi elevati partecipa a un percorso formativo proporzionato ai sistemi gestiti, alle attività svolte, ai privilegi assegnati e al relativo livello di rischio. La formazione è completata, quando necessario, prima dell'abilitazione o dell'ampliamento dell'accesso ed è aggiornata secondo gli obblighi applicabili e in occasione di cambiamenti rilevanti, quali nuove tecnologie, modifiche dei sistemi o delle procedure, nuove vulnerabilità, incidenti o variazioni dei privilegi.

La formazione tratta almeno, oltre a quanto già previsto in forma generale per gli organi di amministrazione e direzione:

- amministrazione sicura, configurazione e hardening dei sistemi;
- gestione delle identità, degli account e degli accessi privilegiati;
- logging, monitoraggio degli eventi e rilevazione delle anomalie;
- gestione delle vulnerabilità, aggiornamenti e applicazione delle patch;
- backup, ripristino e continuità operativa;
- risposta agli incidenti, escalation e conservazione delle evidenze;
- procedure operative e tecnologie specifiche dei sistemi gestiti.

L'efficacia della formazione è verificata mediante prove pratiche, esercitazioni o altre modalità proporzionate al rischio e alle competenze richieste. La partecipazione è personale ed obbligatoria per almeno 8 ore annue. Eventuali assenze sono recuperate nella prima edizione utile o mediante sessione equivalente anche on line; l'Ufficio Formazione ne monitora la regolarizzazione.

7 PROGRAMMAZIONE ANNUALE E ALLEGATO A

L'«Allegato A - Programmazione annuale della formazione» è un documento separato in formato Excel e costituisce la programmazione annuale di dettaglio del presente Piano. È aggiornato entro l'avvio di ciascun ciclo formativo dalla Direzione IT, con il supporto del RSGSI e in coordinamento con la Direzione Risorse Umane - Ufficio Formazione, ed è approvato o recepito dagli Organi di Ateneo competenti nell'ambito degli atti di programmazione applicabili.

Nei primi 60 giorni solari di ciascun anno, la Direzione IT, i Responsabili di Area e i Project Manager, con il supporto del RSGSI e il coordinamento della Direzione Risorse Umane - Ufficio Formazione, raccolgono e qualificano le richieste formative del personale.

L'aggiornamento annuale considera almeno:

- valutazione e piano di trattamento del rischio;
- elenco dei sistemi e servizi rilevanti e variazioni di ruoli, responsabilità o tecnologie;
- incidenti, quasi-incidenti, campagne di phishing e lezioni apprese;
- esiti di audit, riesami, test, esercitazioni e verifiche dell'apprendimento;
- minacce e vulnerabilità emergenti e indicazioni di ACN/CSIRT Italia;
- esigenze segnalate dalle strutture e fabbisogni connessi a ingresso, mobilità o cambio mansione;
- sovrapposizioni e sinergie con ISO/IEC 27001, GDPR, continuità operativa e altri obblighi.

Per ogni intervento il file Excel Allegato A specifica almeno destinatari, obiettivi e contenuti, modalità e durata indicative, periodo, soggetto responsabile, eventuale verifica e codifica per la registrazione. Aggiornamenti infrannuali urgenti possono essere disposti dalla Direzione IT e dall'Ufficio Formazione; sono tracciati nel medesimo file e sottoposti a ratifica o rendicontazione secondo le competenze interne. Per ogni nuovo progetto o

processo di change management sono inoltre rilevati gli eventuali gap formativi e le relative azioni sono collegate al programma annuale. Il programma è riesaminato e rendicontato entro la fine di ottobre, indicando attività svolte, rinviate, cancellate e aggiunte rispetto alla programmazione iniziale.

8 RUOLI E RESPONSABILITÀ

Ruolo	Responsabilità
Organi di amministrazione e direttivi	Approvano il Piano e la programmazione annuale; partecipano alla formazione; sovrintendono all'attuazione ed esaminano gli indicatori.
Direzione IT	Presidia i contenuti cyber, propone i fabbisogni, individua i destinatari specialistici con le strutture, supporta docenti ed esercitazioni e valuta l'efficacia tecnica.
RSGSI	Supporta l'allineamento alle misure NIS2 e al sistema di gestione, consolida evidenze, risultati di audit e input di rischio.
Direzione Risorse Umane - Ufficio Formazione	Coordina la pianificazione operativa, gestisce iscrizioni e recuperi, registra la formazione in U-Web Formazione, applica la tassonomia e produce estrazioni e report. La Direzione Risorse Umane mantiene la titolarità istituzionale della gestione della formazione.
~~Personale~~	~~Partecipa alle attività assegnate, svolge le verifiche previste e applica procedure e comportamenti appresi.~~
Fornitori di formazione	Erogano contenuti coerenti con i requisiti concordati e forniscono evidenze affidabili su programma, partecipazione e risultati.
Responsabile del SIR / responsabile organizzativo	Definisce i requisiti del ruolo nel proprio perimetro, verifica l'adeguatezza della persona, segnala i fabbisogni e assicura la partecipazione alle attività previste.
Gestore tecnico / responsabile operativo	Verifica le competenze tecniche necessarie, limita le attività alle persone abilitate e segnala scostamenti o necessità di aggiornamento.
Persona interessata	Partecipa alla formazione, mantiene le competenze richieste, rispetta le regole e segnala tempestivamente incidenti, errori, vulnerabilità o conflitti di interesse.

9 MODALITÀ DI EROGAZIONE E VERIFICA

Le attività possono essere erogate in presenza, a distanza sincrona o asincrona, mediante microlearning, workshop, laboratori, simulazioni, tabletop exercise o affiancamento. La modalità è scelta in funzione del risultato atteso e dell'accessibilità per i destinatari.

Le verifiche possono comprendere test di apprendimento, prove pratiche, esercitazioni, simulazioni di phishing, valutazione di casi o attestazione di completamento. Esiti insufficienti determinano recupero, approfondimento mirato o nuova verifica entro un termine definito nell'intervento annuale. Per i vertici è privilegiata la discussione di scenari decisionali; per i ruoli tecnici sono privilegiate prove applicative. Per le attività obbligatorie deve essere sempre documentata una verifica dell'apprendimento, dell'applicazione o dell'efficacia, oppure la motivazione della sua non pertinenza.

10 REGISTRAZIONE E TRACCIABILITÀ IN U-WEB FORMAZIONE

La registrazione dell'avvenuta formazione è effettuata attraverso il coordinamento con la Direzione Risorse Umane e, nello specifico, con l'Ufficio Formazione. U-Web Formazione costituisce il sistema istituzionale di registrazione delle attività e dei completamenti, salvo che specifici vincoli tecnici impongano l'uso temporaneo di evidenze complementari successivamente riconciliate.

L'Ufficio Formazione configura e mantiene una tassonomia controllata che consenta di distinguere, ricercare ed estrarre la formazione NIS2 dalla formazione riferita ad altri ambiti. Sono evitati tag liberi non normalizzati. Una singola attività può essere associata a più ambiti quando produce evidenze valide per più sistemi o obblighi.

Dimensione	Vocabolario minimo	Finalità
Ambito di conformità	NIS2; ISO27001; GDPR; CONTINUITA; ALTRO	Consente estrazioni per quadro normativo o sistema di gestione.
Requisito/controllo	NIS2-ART23; NIS2-PR.AT-01; ISO27001-A.6.3	Collega l'intervento alla prescrizione o al controllo.
Popolazione	VERTICI; GENERALE; SPECIALISTICA	Distingue obblighi e indicatori per destinatario.
Dominio	GOVERNANCE; INCIDENTI; IAM; CLOUD; RETI; SVILUPPO; SUPPLY-CHAIN; BC-DR; PRIVACY; LAB-IOT-OT	Permette analisi dei fabbisogni specialistici.
Carattere	OBBLIGATORIA; RACCOMANDATA; FACOLTATIVA	Supporta solleciti e rendicontazione.
Anno e versione	AAAA; EDIZIONE; VERSIONE-CONTENUTO	Rende confrontabili cicli e materiali.
Verifica	NESSUNA; TEST; PROVA-PRATICA; ESERCITAZIONE; SIMULAZIONE	Consente l'estrazione delle verifiche svolte.

Qualora U-Web Formazione non renda disponibili campi multipli o tag strutturati, l'Ufficio Formazione adotta una convenzione equivalente: categoria dedicata, prefisso normalizzato nel codice o nel titolo dell'attività e tabella di corrispondenza controllata. La soluzione deve comunque consentire l'estrazione per ambito, requisito, popolazione, dominio e anno.

Per ciascuna attività sono mantenuti almeno: identificativo dell'intervento; titolo e versione dei contenuti; destinatario e identificativo del partecipante; data, durata e modalità; stato di iscrizione e completamento; verifica prevista ed esito; eventuale recupero o esenzione; fornitore/docente; tag applicati. Le evidenze esterne a U-Web sono conservate secondo le regole documentali dell'Ateneo e collegate mediante identificativo univoco.

11 MONITORAGGIO, REPORTING ED EFFICACIA

L'Ufficio Formazione, con la Direzione IT e il RSGSI, produce almeno annualmente un rapporto sull'attuazione. Per attività obbligatorie o criticità rilevanti il monitoraggio è effettuato anche durante l'anno. Il rapporto è portato agli Organi di Ateneo competenti e contiene almeno:

- copertura e completamento per vertici, personale generale e gruppi specialistici;
- ritardi, assenze, recuperi, esenzioni e azioni correttive;
- risultati delle verifiche, delle simulazioni e delle esercitazioni;
- copertura dei ruoli specialistici e degli amministratori di sistema;
- correlazioni utili con incidenti, segnalazioni, audit e non conformità;
- proposte per il file Excel Allegato A dell'anno successivo.

Gli indicatori sono utilizzati per valutare l'efficacia della misura e non soltanto l'avvenuta partecipazione. I risultati individuali sono trattati nel rispetto dei principi di necessità, proporzionalità e riservatezza.

12 INADEMPIMENTI E RECUPERI

Per la formazione obbligatoria, l'Ufficio Formazione invia solleciti e comunica le posizioni non completate ai responsabili competenti. I responsabili assicurano la partecipazione alla prima sessione utile. Persistenti inadempimenti sono portati alla Direzione Risorse Umane e alla Direzione IT per le valutazioni di competenza e, se riguardano ruoli critici o privilegiati, per l'adozione di misure proporzionate al rischio.

13 CONSERVAZIONE DELLE EVIDENZE

Le registrazioni e le evidenze sono conservate per il periodo definito dal massimario e dalle politiche documentali dell'Ateneo, in modo da assicurare disponibilità per vigilanza NIS2, audit interni ed esterni e riesami. Accesso ed estrazione sono consentiti ai soli ruoli autorizzati.

14 AGGIORNAMENTO DEL PIANO

Il Piano è riesaminato almeno ogni due anni e, se opportuno, aggiornato in caso di modifiche normative, organizzative o tecnologiche rilevanti, incidenti significativi, mutamenti dell'esposizione alle minacce o carenze emerse dalle verifiche. Il file Excel «Allegato A - Programmazione annuale della formazione» è invece aggiornato ogni anno e ogniqualvolta esigenze urgenti rendano necessaria una modifica della programmazione.

Allegato A - Programmazione annuale della formazione

Modello operativo collegato al Piano di formazione in materia di sicurezza informatica dell'Ateneo

1. Dati identificativi del ciclo annuale

Ateneo	
Anno di riferimento	2026
Versione	1.2
Data	
Stato del documento	Bozza
Atto di approvazione/recepimento	[estremi o collegamento]

2. Come compilare e aggiornare l'Allegato A

1	**Raccogliere i fabbisogni**	Direzione IT e RSGSI consolidano rischi, incidenti, audit, minacce, cambiamenti e richieste delle strutture nel foglio Fabbisogni.
2	**Qualificare il fabbisogno**	Per ogni esigenza si indicano priorità, competenza da sviluppare e tipologia di risposta formativa più appropriata.
3	**Programmare gli interventi**	Nel foglio Programma annuale ogni riga rappresenta una singola attività. Le celle gialle sono compilabili; le celle azzurre sono calcolate.
4	**Approvare o recepire**	La programmazione annuale è sottoposta agli Organi di Ateneo secondo le competenze e gli atti applicabili.
5	**Registrare in U-Web**	L'Ufficio Formazione usa codice e tag normalizzati indicati nel programma, così da estrarre separatamente NIS2, ISO/IEC 27001 e altri ambiti.
6	**Monitorare e recuperare**	Durante l'anno si aggiornano stato, partecipanti, esiti e recuperi. Il foglio Monitoraggio riepiloga automaticamente i principali indicatori.
7	**Riesaminare**	A consuntivo si registrano scostamenti e azioni correttive; gli esiti alimentano il ciclo dell'anno successivo.

3. Regole essenziali di compilazione

Una riga, un elemento	Nel foglio Fabbisogni ogni riga identifica un'esigenza; nel Programma annuale ogni riga identifica un singolo intervento.
ID fabbisogno	È attribuito automaticamente quando si compila la descrizione dell'esigenza. Il codice usa l'anno indicato nei dati identificativi e un progressivo tecnico associato alla riga.
Tipologia di risposta	Selezionare dalla lista la risposta più appropriata: formazione, affiancamento, laboratorio pratico, esercitazione, simulazione, workshop o aggiornamento documentale/procedurale.
Destinatari	Selezionare la macro-categoria dalla lista e precisare nel campo successivo strutture, ruoli o gruppi effettivamente coinvolti.
Verifica	Selezionare la modalità prevista. "Nessuna" va utilizzata solo quando la verifica non è pertinente e la scelta è motivata nelle note.
Classificazione U-Web	Usare le voci controllate per ambito, requisito, popolazione, dominio e carattere. Il campo Tag U-Web viene generato automaticamente.
Più ambiti	Quando l'attività vale per più sistemi (es. NIS2 e ISO/IEC 27001), indicare l'ambito prevalente e riportare gli ulteriori riferimenti nelle note o nel sistema U-Web.
Modifiche infrannuali	Aggiunte, rinvii e annullamenti devono mantenere data, stato e motivazione; non cancellare la traccia delle decisioni già assunte.
Vocabolari	Il foglio Vocabolari alimenta le liste a discesa ed è protetto senza password. Può essere sbloccato per aggiornare consapevolmente le voci controllate.
Collegamento al programma	Nel Programma annuale selezionare l'ID fabbisogno dalla lista. Lo stesso ID può essere associato a più corsi quando più interventi soddisfano la medesima esigenza.

4. Legenda

Colore	Significato	Uso	
Giallo	Cella compilabile	Inserire o selezionare il dato	
Azzurro	Cella calcolata	Non sovrascrivere la formula	
Grigio	Etichetta o vocabolario	Contenuto strutturale/controllato	

Analisi dei fabbisogni formativi

Registrare l'esigenza, la competenza da sviluppare e la tipologia di risposta formativa

Compilazione: Direzione IT e RSGSI, con il contributo delle strutture. L'ID viene attribuito automaticamente; collegare l'esigenza al codice dell'intervento nel Programma annuale quando definito.

ID fabbisogno	Data rilevazione	Fonte	Descrizione dell'esigenza	Struttura/servizio interessato	Ruoli interessati	Competenza da sviluppare	Ambito	Dominio	Priorità	Tipologia di risposta formativa	Codice intervento collegato	Note
FAB-2026-001		Valutazione dei rischi	prova									

Programma annuale degli interventi formativi

Ogni riga corrisponde a un intervento e ne definisce gli scopi, le risorse, le fasi di progettazione, realizzazione e valutazione.

Compilare anche il foglio "Partecipanti" (codice edizione) e il calendario di ciascun intervento.

Pianificazione																						Monitoraggio e consuntivo							
Identificativo	Titolo	Semplificazione sanitaria	Area tutor	Scopo/obiettivo e specifica	Argomenti e materiali (riferimenti)	Durata	Periodo/fasi previste	Modalità	Metodologia/tecniche	Modalità	Ore totali	Ore FAD	Responsabile gestione	Referente amministrativo	Responsabile contenuto	Responsabile organizzativo	Soggetto erogatore	Costo	Privato	Anticipi/quote previste	Partecipanti effettivi	Ore aspetto verificato	Esonero, assenze	Luogo e date	Tag e video	Collegamento a edizione	Note
FAD-2025-0001	Aggiornamento PEIMA per gli Organi di Governo	Semplificazione sanitaria	Progetto di valorizzazione dei medici	Progetto di rilancio (riferimenti)	Regolamento, governo dei flussi, rilevanza, contenuti, controllo, Rilata e sistemi territoriali	2	Primo trimestre	FAD asincrona	Metodologia attiva	Interazione di un esperto	2	2	Area giuridica di riferimento	Docenti		Direzione Risorse Umane – Ufficio Formazione								Video lezione (max una durata di 1 ora)		Non necessita tutor, collaborano a piccolo gruppo
	Semplificazione gestione delle circolazioni informatiche	Semplificazione gestione delle circolazioni informatiche	Personale giuridico	Aggiornamento e interessata	Quadro informativo, (cruciale), circolazione, norme, (cruciale), delle informazioni su Rilata	1000	30/05/2025 al 31/07	4000499/99/00	Obbligatoria	E-learning, asincrona	1	1	Area di applicazione/utenti	Docenti		Direzione IT	Direzione Risorse Umane – Ufficio Formazione	(marcoformativa)	Proposta	45%		No					Strutture tecnologiche di riferimento durante tutto
	Formazione specialistica tecnica ed ecc.	Formazione specialistica	Personale non medico specialistico	Area, struttura e ruolo/e interessati	Contenuti, norme e/o Metodologia e e Rilata, attività, attività all'ente sociale	1000	30/05/2025 al 31/07	(osservazione)	Obbligatoria	Laboratorio		Prove pratiche	Docenti e tutor/esperti		Docenti e IT – responsabile tecnico	Direzione Risorse Umane – Ufficio Formazione	(marcoformativa)	Proposta	45%		No					Formazione in piccolo per gruppi specialistici (Rilata)

Monitoraggio e consuntivo

Indicatori alimentati dal Programma annuale e registro delle azioni correttive

Interventi censiti	Interventi conclusi	Completamento partecipanti	Recuperi richiesti
1	0	0,0%	0

Indicatori per popolazione

Destinatari	Partecipanti previsti	Partecipanti completati	% completamento
Organi di amministraz	0	0	0,0%
Personale generale	0	0	0,0%
Personale con ruoli sp	0	0	0,0%

Stato	Numero	% sul totale
Proposto	3	300,0%
Approvato	0	0,0%
Pianificato	0	0,0%
In corso	0	0,0%
Concluso	0	0,0%
Rinviato	0	0,0%
Annullato	0	0,0%
Non avviato	0	0,0%

Azioni correttive e priorità per l’anno successivo

ID	Data	Scostamento/evidenza	Azione	Responsabile	Scadenza	Stato	Note

Fonte fabbisogno

Valutazione dei rischi

Piano di trattamento del rischio	Affiancamento	Sensibilizzazione generale	ISO/IEC 27001	Personale generale	AWARENESS	NIS2-PR.AT-01	Raccomandata	Webinar sincrono	Test di apprendimento	Annuale	Proposto	Non svolta	Media	In approvazione	SI	In corso
Incidente	Laboratorio pratico	Formazione specialistica	GDPR	Personale con ruoli specializzati	INCIDENTI	ISO27001-A.6.3	Facoltativa	E-learning asincrono	Prova pratica	Semestrale	Approvato	Superata	Bassa	Approvato		Completata
Quasi-incidente	Esercitazione	Esercitazione/simulazione	Continuità operativa	Amministratori di sistema	IAM	ALTRO		Microlearning	Esercitazione	All'ingresso/cambio ruolo	Pianificato	Parzialmente superata		Superato		Rinviata
Campagna di phishing	Simulazione	Aggiornamento mirato	Formazione integrata	Sviluppatori/DevOps	CLOUD			Workshop	Simulazione di phishing	Secondo fabbisogno	In corso	Non superata				
Audit o riesame	Workshop			Responsabili di servizio/progetto	RETI			Laboratorio	Tabletop exercise	A seguito di evento	Concluso	Da recuperare				
Test o esercitazione	Aggiornamento documentale/procedurale			Acquisti e contratti	SVILUPPO			Tabletop exercise	Discussione di scenario		Rinviato					
Modifica normativa	Altro			Risorse Umane/Ufficio Formazione	SUPPLY-CHAIN			Affiancamento	Attestazione di completamento		Annullato					
Nuova minaccia o vulnerabilità				Privacy/legale/comunicazione	BC-DR			Modalità mista								
Cambiamento organizzativo o tecnologico				Laboratori/ricerca/HPC/IoT/OT	PRIVACY											
Richiesta della struttura				Fornitori/collaboratori	LAB-IOT-OT											