UNIMORE
UNIVERSITÀ DEGLI STUDI DI
MODENA E REGGIO EMILIA

# PIANO DI SICUREZZA INFORMATICA
# 2023-2025
# dell'Università di Modena e Reggio Emilia
# aggiornamento dicembre 2024

*Approvato dal Consiglio di Amministrazione nella seduta del 20.12.2024*

# PIANO DI SICUREZZA INFORMATICA 2023-2025

# dell'Università di Modena e Reggio Emilia


PREMESSA ..... 3

LA NORMATIVA E GLI STANDARD DI RIFERIMENTO ..... 3

*DISCIPLINA EUROPEA ..... 3*

*DISCIPLINA NAZIONALE ..... 3*

LA GOVERNANCE DELLA SICUREZZA INFORMATICA DELL'ATENEO ..... 4

LA FORMAZIONE IN MATERIA DI CYBERSECURITY E DATA PROTECTION ..... 4

ANALISI DELLA POSTURA DI ATENEO ..... 5

RISK ANALISYS ..... 5

MISURE DI SICUREZZA PER LA MITIGAZIONE DEL RISCHIO ..... 6

*GESTIONE BACKUP E SERVIZI DI DISASTER RECOVERY - BUSINESS CONTINUITY ..... 6*

*ATTIVAZIONE DELLA MULTI FACTOR AUTHENTICATION ..... 6*

*MISURE DI SICUREZZA DI RETE ..... 6*

*SOLUZIONI IN CLOUD ..... 7*

SERVIZI DI SICUREZZA ..... 7

*SERVIZIO DI INCIDENT RESPONSE TEAM E CYBER THREAT INTELLIGENCE ..... 7*

*VULNERABILITY ASSESSMENT + PENETRATION TEST (INFRASTRUTTURALE E WEBPP) ..... 8*

*CAMPAGNE DI PHISHING SIMULATO/AWARENESS ..... 8*

*MISURE MINIME DI SICUREZZA AGID ..... 8*

*POLICY E REGOLAMENTI AZIENDALI ..... 8*

AZIONI DI IMPLEMENTAZIONE, MONITORAGGIO E RIESAME ..... 9

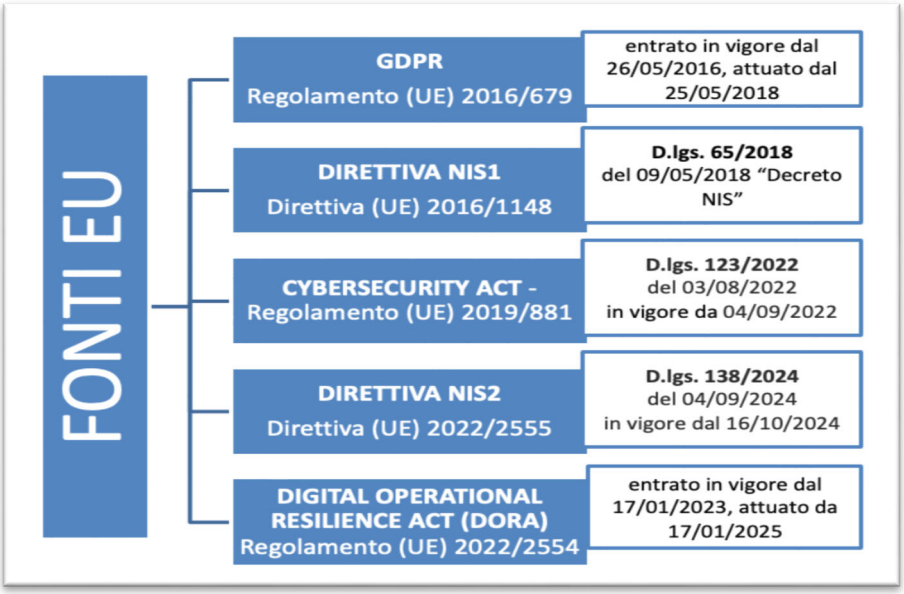
# Premessa

Il presente documento rappresenta un aggiornamento del "Piano di Sicurezza Informatica 2023-2025" dell'Università degli Studi di Modena e Reggio Emilia, approvato dal Consiglio di Amministrazione con Delibera n°491 del 21/12/2023.

L'obiettivo delle azioni di miglioramento elencate nel presente documento è quello di ridurre il rischio cyber ed aumentare la resilienza dell'Ateneo a fronte di eventi avversi che possano potenzialmente comportare perdita/esfiltrazione di dati (anche personali) ed interruzione di servizi.

# La normativa e gli standard di riferimento

## Disciplina Europea




## Disciplina nazionale

**UNI ISO 31000:2018 - Gestione del rischio - Linee guida**

**ISO/IEC 27001:2022 - Sistema di gestione della sicurezza delle informazioni**

## La governance della sicurezza informatica dell'Ateneo

Il responsabile della sicurezza informatica dell'Ateneo è il Responsabile della Transizione Digitale (RTD).

L'RTD dell'Università degli Studi di Modena e Reggio Emilia è la Dott.ssa Paola Michelini – nominata con delibera del Consiglio di Amministrazione nella seduta del 16 gennaio 2023. L'RTD nello svolgimento del proprio incarico si avvale di un Ufficio dirigenziale denominato Ufficio della Transizione Digitale (Ufficio RTD), i cui compiti sono elencati all'art. 17 CODICE DELL'AMMINISTRAZIONE DIGITALE - D.lgs 82/2005 e s.m.i.

L'Ufficio della Transizione Digitale dell'Ateneo è la Direzione Sistemi Informativi ed Assicurazione della Qualità (DIAQ). All'interno dell'Ufficio RTD è presente un'unità operativa "Ufficio Reti, Sistemi, Fonia e Cybersecurity" che coordina le attività tecniche in materia di sicurezza informatica.

L'Ufficio della Transizione Digitale dell'Ateneo si avvale della collaborazione e del supporto tecnico e specialistico del Centro di Ricerca Interdipartimentale sulla Sicurezza e la prevenzione dei rischi (CRIS) di UNIMORE coordinata dal prof. Mirco Marchetti e con la partecipazione dei proff. Luca Ferretti e Mauro Andreolini.

L'Ateneo ha sottoscritto un protocollo d'intesa per la prevenzione e contrasto dei crimini informatici sui sistemi informativi "critici" dipendenti da UniMORE con la Polizia di Stato - Centro Operativo per la Sicurezza Cibernetica Emilia-Romagna (Rif. deliberazione del Senato Accademico Repertorio n. 18/2023 Prot n. 46538 del 15/02/2023 e deliberazione del Consiglio di Amministrazione n. 42/2023 Prot n. 63315 del 27/02/2023.

Nel Consiglio di Amministrazione del 19/07/2024 i proff. Mirco Marchetti e Francesco Guerra hanno illustrato un'informativa sullo stato di attuazione delle misure di rafforzamento della sicurezza delle informazioni.

## La formazione in materia di Cybersecurity e Data Protection

L'attività ha l'obiettivo di accrescere la conoscenza, la consapevolezza e la responsabilità del personale dell'Ateneo in merito alle tematiche di sicurezza informatica e data protection (Cybersecurity Awareness).

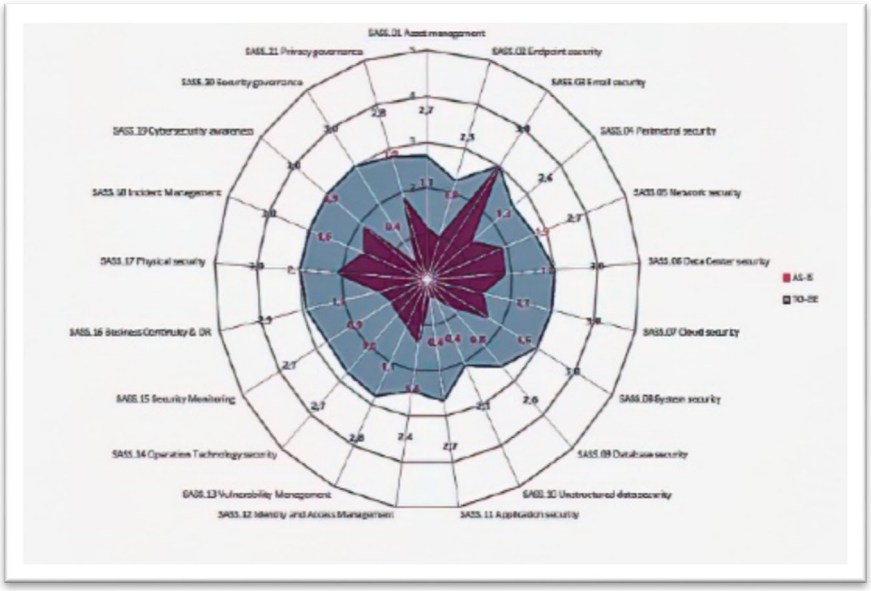
Il CRIS sta predisponendo video formativi sui seguenti contenuti:

- cyber security awareness;
- phishing;
- ransomware;
- identità digitale, autenticazione, autorizzazione;
- Misure Minime di Sicurezza predisposte dall'Agenzia per l'Italia Digitale (AGID);

- lavorare in cloud, avvertenze di sicurezza nella condivisione di file e informazioni;
- avvertenze nella gestione dei dati particolari e cenni di privacy (con il contributo del DPO dell'Ateneo);
- autenticazione a singolo fattore: problemi e gestione sicura delle password;
- autenticazione multifattore: perché è importante;
- single sign-on, identità federata, autorizzazioni delegate;
- uso di spid.

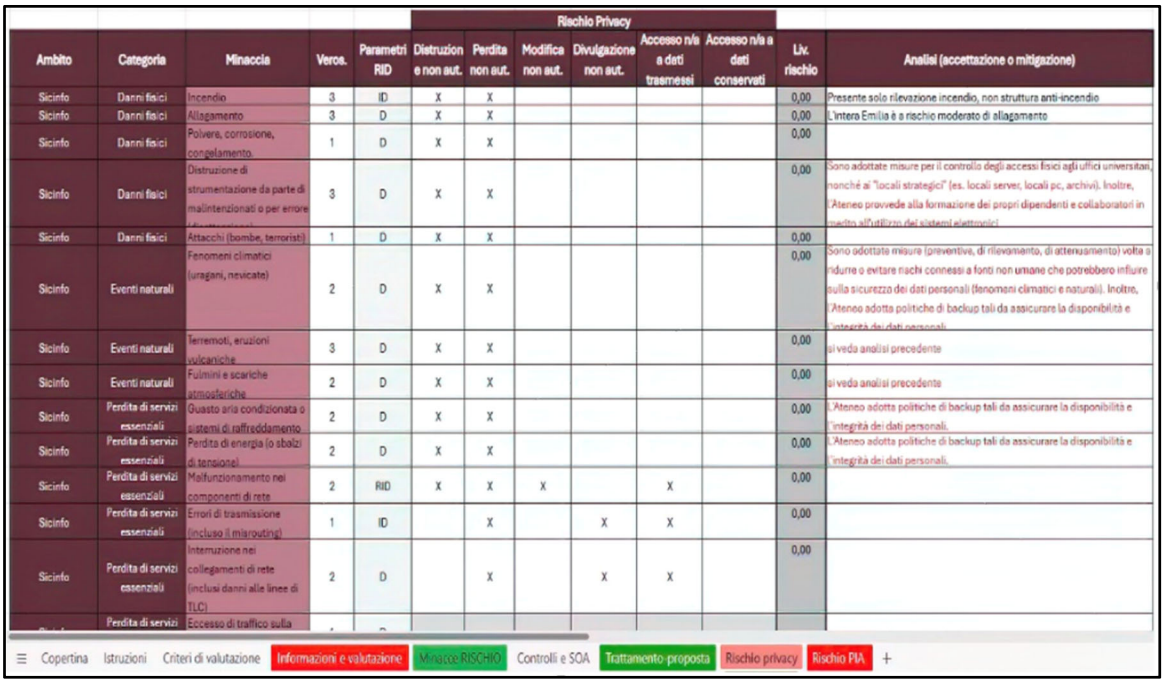
## Analisi della postura di Ateneo

Tra le prime attività avviate nel 2024, è stata implementata l'analisi della postura dell'Ateneo (Asset Management) che ha costituito la base di conoscenza per il piano di lavoro biennale che l'Ateneo sta perseguendo. Si prevede di riaggiornare l'analisi a fine 2025.



## Risk Analisys

È stata eseguita l'analisi dei rischi, con calcolo dell'indice di rischio e definizione delle azioni di mitigazione/contenimento del medesimo. Di seguito un'immagine rappresentativa del documento, riservato agli atti.



| | | | | | Rischio Privacy | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ambito | Categoria | Minaccia | Veros. | Parametri RID | Distruzione non aut. | Perdita non aut. | Modifica non aut. | Divulgazione non aut. | Accesso n/a a dati trasmessi | Accesso n/a a dati conservati | Liv. rischio | Analisi (accettazione o mitigazione) |
| Sicinfo | Danni fisici | Incendio | 3 | ID | X | X | | | | | 0,00 | Presente solo rilevazione incendio, non struttura anti-incendio |
| Sicinfo | Danni fisici | Allagamento | 3 | D | X | X | | | | | 0,00 | L'intera Emilia è a rischio moderato di allagamento |
| Sicinfo | Danni fisici | Polvere, corrosione, congelamento | 1 | D | X | X | | | | | 0,00 | |
| Sicinfo | Danni fisici | Distruzione di strumentazione da parte di malintenzionati o per errore | 3 | D | X | X | | | | | 0,00 | Sono adottate misure per il controllo degli accessi fisici agli uffici universitari, nonché ai "locali strategici" (es. locali server, locali pc, archivi). Inoltre, l'Ateneo provvede alla formazione dei propri dipendenti e collaboratori in merito all'utilizzo dei sistemi elettronici |
| Sicinfo | Danni fisici | Attacchi (bombe, terroristi) | 1 | D | X | X | | | | | 0,00 | |
| Sicinfo | Eventi naturali | Fenomeni climatici (uragani, nevicate) | 2 | D | X | X | | | | | 0,00 | Sono adottate misure (preventive, di rilevamento, di attenuamento) volte a ridurre o evitare rischi connessi a fonti non umane che potrebbero influire sulla sicurezza dei dati personali (fenomeni climatici e naturali). Inoltre, l'Ateneo adotta politiche di backup tali da assicurare la disponibilità e l'integrità dei dati personali. |
| Sicinfo | Eventi naturali | Terremoti, eruzioni vulcaniche | 3 | D | X | X | | | | | 0,00 | si veda analisi precedente |
| Sicinfo | Eventi naturali | Fulmini e scariche atmosferiche | 2 | D | X | X | | | | | 0,00 | si veda analisi precedente |
| Sicinfo | Perdita di servizi essenziali | Guasto aria condizionata o sistemi di raffreddamento | 2 | D | X | X | | | | | 0,00 | L'Ateneo adotta politiche di backup tali da assicurare la disponibilità e l'integrità dei dati personali. |
| Sicinfo | Perdita di servizi essenziali | Perdita di energia (o sbalzi di tensione) | 2 | D | X | X | | | | | 0,00 | L'Ateneo adotta politiche di backup tali da assicurare la disponibilità e l'integrità dei dati personali. |
| Sicinfo | Perdita di servizi essenziali | Malfunzionamento nei componenti di rete | 2 | RID | X | X | X | | X | | 0,00 | |
| Sicinfo | Perdita di servizi essenziali | Errori di trasmissione (incluso il misrouting) | 1 | ID | | X | | X | X | | 0,00 | |
| Sicinfo | Perdita di servizi essenziali | Interruzione nei collegamenti di rete (inclusi danni alle linee di TLC) | 2 | D | | X | | X | X | | 0,00 | |
| | Perdita di servizi | Eccesso di traffico sulla | | | | | | | | | | |

Copertina | Istruzioni | Criteri di valutazione | Informazioni e valutazione | Minacce RISCHIO | Controlli e SOA | Trattamento proposta | Rischio privacy | Rischio PIA | +

# Misure di sicurezza per la mitigazione del rischio

## Gestione backup e servizi di disaster recovery - business continuity

L'infrastruttura di backup è un asset di elevata criticità in caso di attacco ransomware poiché è spesso oggetto di cifratura.

Si sta procedendo:

- alla progettazione ed implementazione di una soluzione di backup "air gapped";
- all'adozione di servizi di backup in cloud "non modificabili".

Parallelamente è in atto la predisposizione di un piano di Business Continuity/Disaster Recovery, a partire dai tempi di Recovery Time Objective (RTO) e Recovery Point Objective (RPO) individuati attraverso l'attività di Business Impact Analysis (BIA).

## Attivazione della Multi Factor Authentication

La Multi Factor Authentication (MFA) aggiunge ai meccanismi di autenticazione basati su username e password, un secondo fattore di autenticazione che utilizza un canale diverso rispetto a quello utilizzato per l'accesso. Ciò consente di proteggere l'accesso ai sistemi anche in caso di furto di credenziali. Il generatore del token d'accesso può essere indifferentemente Google Authenticator o Microsoft Authenticator.

Nel 2024 è stata condotta un'analisi di fattibilità finalizzata all'introduzione graduale e controllata dell'MFA (per gruppi di utenti, per ruolo/struttura o per gruppi di servizi). Il piano di attivazione prevede le seguenti fasi:

1) attivazione MFA per l'accesso ai servizi web;
2) attivazione MFA per l'accesso ai dispositivi;
3) attivazione MFA per l'accesso via VPN alla rete Unimore;
4) attivazione MFA sui singoli servizi interni e sul cloud.

La prima sperimentazione, applicata a un gruppo di volontari del CRIS e della DIAQ è partita a novembre 2024.

## Misure di sicurezza di rete

Il rafforzamento della sicurezza della rete prevede:

- la predisposizione di funzionalità avanzate sul firewall (es. funzionalità di SSL inspection);
- l'introduzione di sistemi Web Application Firewall (WAF);
- la segmentazione della rete dell'Ateneo;
- l'introduzione di sistemi di Endpoint Detection and Response (EDR), eventi di rete raccolti dalla piattaforma di Network Detection and Response (NDR);
- l'introduzione di sistemi Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)/Security Information and Event Management (SIEM) per il monitoraggio di sicurezza.

Nel 2024 è stata completata una prima analisi delle possibili architetture/tecnologie utilizzabili.

### Soluzioni in Cloud

Nell'ambito del potenziamento della strategia di migrazione al Cloud, si stanno verificando le politiche di sicurezza e privacy delle soluzioni cloud attive in Ateneo (Microsoft e Google) mentre è già stato migrato il Portale di Ateneo nel sistema cloud del CINECA.

La piattaforma Microsoft 365 è disponibile in Ateneo grazie alla convenzione CRUI-Microsoft rinnovata a Giugno 2024; ed è stato ridefinito il sistema di rilascio delle licenze utente. L'ambiente cloud Azure ospita attualmente la soluzione PaaS che gestisce la piattaforma della didattica e quello dell'orientamento agli studi. Su Azure sono attive anche sottoscrizioni ad hoc riservate a gruppi di ricerca. Attualmente l'accesso MFA è obbligatorio per gli amministratori ed è suggerito agli utenti finali.
La piattaforma Google Workspace consente l'accesso alle app di Google. L'accesso MFA è obbligatorio per gli amministratori ed è suggerito agli utenti finali.

## Servizi di sicurezza

### Incident Response Team e Cyber Threat Intelligence

La finalità dell'Incident Response Team (IRT) è quella di intervenire rapidamente a fronte di un attacco informatico andato a buon fine. L'attività dell'IRT consiste nell'analizzare le dinamiche di attacco che hanno portato alla compromissione degli asset dell'organizzazione, i vettori d'attacco che sono stati usati per fare breccia sui sistemi e le vulnerabilità che sono state sfruttate per eseguire azioni illecite sui server coinvolti, fornendo quindi indicazioni su come sanare le vulnerabilità che hanno consentito agli attaccanti di perpetrare azioni illecite sui sistemi e incrementare di fatto il livello globale di sicurezza dell'organizzazione.

Il servizio di Cyber Threat Intelligence (CTI) ha come obiettivo il monitoraggio delle allerte di sicurezza provenienti da varie fonti (OSINT e CLOSINT) al fine di identificare, classificare e notificare minacce di sicurezza informatica.

Nel dettaglio le attività riguarderanno:

- la capacità di identificazione, gestione, mitigazione e risoluzione degli attacchi informatici;
- la centralizzazione di tutte le attività di gestione di sicurezza;
- il monitoraggio in tempo reale dell'infrastruttura IT e di Sicurezza;
- la raccolta centralizzata e attraverso canali cifrati (SSL) di log ed eventi; la correlazione tra eventi diversi raccolti dal SIEM;
- la disponibilità di un cruscotto (dashboard) che fornisca agli analisti, in tempo reale, una rappresentazione della situazione dei sistemi di sicurezza;
- la produzione di report periodici di sintesi, di incident-report di dettaglio con istruzioni operative.

Il servizio sarà inizialmente dimensionato per la raccolta di 1000 eventi per secondo in modalità continuata.

La DIAQ ha aderito alla convenzione Intercenter "Servizi di IT System Management e Sicurezza Informatica 2" concordando con FASTWEB la creazione di un servizio triennale di gestione, monitoraggio, rilevazione e risposta alle minacce in una logica di Managed Detection and Response (MDR), attraverso un Security Operation Center (SOC).

## Vulnerability Assessment + Penetration Test (Infrastrutturale e Web App)

Il Vulnerability Assessment effettua una fotografia della infrastruttura e verifica eventuali falle nella sua configurazione. Ciò consente una valutazione dello stato dei sistemi di sicurezza implementati su reti, macchine o applicazioni aziendali, con l'obiettivo di rilevare eventuali carenze di protezione rispetto ad elenchi di vulnerabilità tecnologiche note.

Il Penetration Test è un'indagine sperimentale sulla sicurezza di un computer o di una rete, volta a individuare vulnerabilità che potrebbero essere sfruttate in caso di tentativo di accesso non autorizzato e a testare i controlli che dovrebbero proteggere i computer e le reti da tali tentativi. Il test è articolato sostanzialmente in due fasi:

- l'esplorazione dei presidi di sicurezza del sistema oggetto di verifica;
- tentativo di violare quei presidi e di penetrare il sistema stesso.

Nel 2024 è stato messo a punto un sistema di rilevazione periodico delle vulnerabilità, suddiviso per sedi/sottoreti, per informare i referenti informatici di struttura sullo "stato di salute" delle proprie attrezzature e procedere eventualmente alle correzioni dei propri sistemi, suggerite dai report prodotti.

## Campagne di phishing simulato/awareness

Il progetto si ispira alla necessità di sensibilizzare il dipendente circa il rischio informatico e all'importanza di dare il giusto peso all'aspetto della sicurezza delle informazioni aziendali. L'obiettivo del progetto è acquisire consapevolezza sul tema degli attacchi di ingegneria sociale, in particolare:

- rendere consapevole il dipendente del rischio di Cyber Crime;
- innalzare il livello di attenzione alla riservatezza e alla cura dei dati dell'organizzazione;
- verificare e migliorare le capacità di rilevamento in caso di attacco;
- monitorare la capacità di risposta del dipendente e dell'organizzazione.

La prima delle quattro campagne è stata realizzata nel mese di Dicembre 2024.

## Misure minime di sicurezza AGID

Le Misure Minime di Sicurezza (MMS) ICT, emanate dall'Agenzia per l'Italia Digitale (AgID) nel 2017, sono un documento per valutare e migliorare il livello di sicurezza informatica delle Amministrazioni , al fine di contrastare le minacce informatiche più frequenti. Le misure consistono in controlli di natura tecnologica, organizzativa e procedurale e utili alle Amministrazioni per valutare il proprio livello di sicurezza informatica.

L'adeguamento alle misure minime è a cura del RTD, come indicato dall'art. 17 del CAD. La prima versione è stata approvata in data 6/6/2019, alla quale è seguito un aggiornamento a giugno 2024, comunicato al Consiglio di Amministrazione nella seduta del 21/06/2024.

L' analisi della raccolta centralizzata delle tabelle di struttura (Amministrazione Centrale, Dipartimenti, Centri, CSBA, Facoltà di Medicina) relativa alle MMS previste dall'AgID ha evidenziato che in diversi casi il livello di sicurezza raggiunto è superiore a quello minimo, ed è già di livello Standard [S].

## Policy e regolamenti aziendali

Particolare attenzione è poi stata dedicata alla redazione di policy e regolamenti legati all'utilizzo degli asset, alla sicurezza e al trattamento dei dati. Nel corso del 2024 sono stati deliberati dal Consiglio di Amministrazione (21/6/2024), i seguenti documenti:

- politica per la gestione degli incidenti informatici;

- workflow per la segnalazione di un incidente informatico con la definizione di ruoli ed azioni. Registro degli incidenti informatici.
- procedura di gestione della violazione dei dati personali (in collaborazione con il DPO) - Policy e Procedure in caso di Data Breach.

## Azioni di implementazione, monitoraggio e riesame

- **NIS 2** – adesione al perimetro e relativi adempimenti (es. - nomina degli Amministratori di sistema [AdS] delle strutture).
- **Formazione –** nel 2025 verranno erogate a tutto il personale Unimore videopillole sulle tematiche cybersecurity elencate in precedenza;
- **Gestione backup e servizi di disaster recovery - business continuity** - Nel 2025 si sottoporrà agli OOAA il Piano di Business Continuity/Disaster Recovery;
- **Multi Factor Authentication -** nei primi mesi del 2025 è prevista una graduale estensione ad un gruppo più numeroso di utenti, per arrivare, entro l'anno, all'adozione completa della misura di sicurezza;
- **Misure di sicurezza di rete** - nel 2025 si migliorerà la segmentazione della rete aziendale;
- **Soluzioni in Cloud** – nel 2025,

  - per quanto riguarda la piattaforma Google, si valuterà la possibilità di migrare alla "cloud region" di Milano;
  - per quanto riguarda la piattaforma Microsoft-Azure si valuterà l'attivazione della gestione dei dispositivi (soluzione Defender cloud ed Intune).
- **Servizio di Incident Response Team e Cyber Threat Intelligence** - nei primi mesi del 2025 il servizio sarà pienamente operativo;
- **Vulnerability Assessment + Penetration Test -** nel 2025 l'attività sarà potenziata;
- **Campagne di phishing simulato/awareness** - nel 2025 seguiranno ulteriori verifiche/campagne al fine di conseguire un miglioramento continuo;
- **Misure minime di sicurezza AgID** – nel 2025 si prevede un aggiornamento del documento;
- **Policy e regolamenti aziendali** - nel 2025 saranno definite:
  - la Politica di gestione degli Asset informatici;
  - la Politica centralizzata per il browser Chrome mediante Chrome Enterprise Core;
  - linee guida Privacy per fornitori e terze parti e Scheda di valutazione dei fornitori;
  - allineamento tra il registro degli incidenti informatici con il Registro dei Data Breach (gestito dal DPO).