UNIMORE
UNIVERSITÀ DEGLI STUDI DI
MODENA E REGGIO EMILIA

PIANO DI SICUREZZA INFORMATICA

2023-2025

dell'Università di Modena e Reggio Emilia

aggiornamento ottobre 2025

Approvato dal CdA in data……

PIANO DI SICUREZZA INFORMATICA 2023-2025
dell'Università di Modena e Reggio Emilia

PREMESSA 3

INTRODUZIONE 3

LA NORMATIVA E GLI STANDARD DI RIFERIMENTO 4

LA GOVERNANCE DELLA SICUREZZA INFORMATICA DELL'ATENEO 5

LA FORMAZIONE IN MATERIA DI CYBERSECURITY E DATA PROTECTION 6

POLITICHE DI ANALISI DEI RISCHI E DI SICUREZZA DEI SISTEMI INFORMATIVI 7

ANALISI DELLA POSTURA DI ATENEO..... 7

MISURE DI SICUREZZA PER LA MITIGAZIONE DEL RISCHIO..... 8

Premessa

Il presente documento rappresenta l'aggiornamento annuale 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 e con monitoraggio e aggiornamento deliberati dal Consiglio di Amministrazione del 20/12/2024.

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.

Introduzione

A Febbraio 2025 l'Ateneo è stato individuato dall'Agenzia di Cybersicurezza Nazionale (ACN) come ente soggetto alla direttiva **Direttiva (UE) 2022/2555 (NIS2)** e ha provveduto alla registrazione (codice dichiarazione DNISA00018210).

Il 14 Aprile 2025 con Decreto legislativo 4 settembre 2024, n. 138 ACN ha individuato l'Università Degli Studi Di Modena (00427620364) quale "soggetto importante" in relazione alla/e tipologia/e di soggetto di seguito indicata/e.

- 1. Ricerca 1.1. Organizzazioni di ricerca
- 2. Ulteriori Tipologie di Soggetti (Punto 2)
    - 2.1. Istituti di istruzione che svolgono attività di ricerca

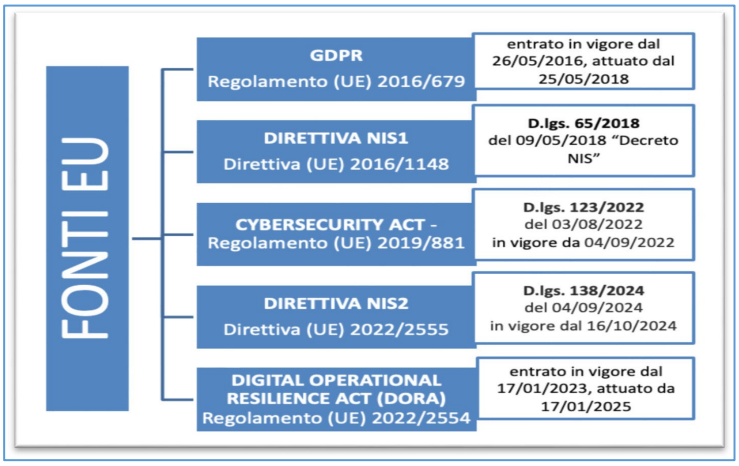
ACN ha attribuito ad Unimore il codice identificativo **ITTSDSY9**.

Entro Ottobre 2026 l'Ateneo dovrà rispondere alle azioni richieste dalle Misure di Sicurezza di Base di ACN.

Questo aggiornamento intende analizzare ogni ambito di intervento richiesto da NIS2 e definire lo stato dell'arte dell'Ateneo e le azioni avviate e pianificate per migliorare la postura di sicurezza ICT di Ateneo e per rispondere alle richieste e ai tempi dettati da ACN.

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 compi 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 Rete, Sistemi, Fonia e Cybersecurity" che coordina le attività tecniche in materia di sicurezza informatica.

Sono individuati in Ateneo queste figurei di controllo e gestione:

Gruppo Sicurezza ICT di Ateneo, RTD che si relazionano con ACN

- Paola Michelini, RTD di Ateneo
- Dario Montardi, Referente della sicurezza ICT di Ateneo
- Roberta Cantaroni, Referente per il coordinamento delle attività relative alla Sicurezza ICT di Ateneo;

Gruppo CSIRT Unimore per la gestione degli incidenti informatici

- Dario Montardi, Referente della sicurezza ICT di Ateneo
- Marco Barbieri coordinatore del CSIRT e responsabile della rete di Ateneo
- Massimo Vignone responsabile dei sistemi di Ateneo
- Claudia Ferrari responsabile delle attività di sicurezza connesse alla Data Protection.
- Roberta Cantaroni referente per il coordinamento delle attività relative alla Sicurezza ICT di Ateneo;
- Francesco Malvezzi responsabile della gestione delle identità Unimore

Il Gruppo Sicurezza ICT si avvale della collaborazione:

- del **Centro di Ricerca Interdipartimentale sulla Sicurezza e Prevenzione dei Rischi (CRIS)** coordinato dal prof. Marchetti per attività di consulenza e di gestione degli incidenti informatici, per l'attività di VAPT, per la gestione dell'autenticazione MFA e per la formazione in materia di sicurezza informativa rivolta al personale;
- dei **Referenti di sicurezza delle strutture (Dipartimenti, Centri, CSBA, Facoltà di Medicina)** che agiscono come primo punto di contatto all'interno della struttura e raccordo con la DIAQ;
- del **DPO di Ateneo** per ogni attività riguardante il trattamento dei dati, la privacy, la gestione di incidenti di data breach o data leaks;
- del **COSC** (Centro Operativo per la Sicurezza Cibernetica) dell'Emilia-Romagna attraverso un protocollo di intesa per la prevenzione e contrasto dei crimini informatici sui sistemi informativi "critici" dell'Ateneo;
- di **fornitori esterni sulla base di convenzioni e/o contratti**. Attualmente sono attivi contratti con:
    - **Engineering/Cybertech** (supporto alla documentazione e ai flussi del progetto, campagne di phishing, analisi forense)
    - **Fastweb/Certego** (SOC)
    - **NAIS/Knowbe4** (Campagne di phishing e awareness)
    - **Proge Software** (aumento del secure score di Azure/Microsoft 365 e realizzazione applicativo per gestione CSIRT e incidenti informatici)

Nel Consiglio di Amministrazione del 20/12/2024 i proff. Mirco Marchetti e Francesco Guerra hanno illustrato lo stato di attuazione delle misure di rafforzamento della sicurezza delle informazioni.

In osservanza a quanto richiesto da ACN, la Dott.ssa Paola Michelini è stata nominata Punto di contatto per le attività con ACN, con Atto di Delega del Rettore in data 26.02.2025.

Il Sig. Dario Montardi è stato nominato Sostituto del Punto di contatto dell'Università degli Studi di Modena e Reggio Emilia, con Atto di Delega del Rettore in data 28.05.2025.
la Dott.ssa Roberta Cantaroni, in qualità di Supporto al Coordinamento delle attività relative alla Sicurezza ICT di Ateneo, nominata con Decreto del Dirigente della DIAQ prot. n. 0011480 del 16.01.2025.

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 Gruppo Sicurezza ICT ha organizzato:

- Realizzazione di una prima campagna di phishing a Dicembre 2024 con Cybertech;
- Acquisto soluzione Knowbe4 livello Platinum per campagne di phishing e formazione cyber;
- Realizzazione di 3 Workshop di formazione sulla sicurezza in ambito Microsoft 365 a cura di Proge Software e dedicati agli amministratori della piattaforma (Thread intelligence, Data protection, Copilot 365);
- Realizzazione di incontri periodici di aggiornamento con i referenti di sicurezza e i referenti informatici;
- Attivazione portale www.sicurezzaict.unimore.it;
- Realizzazione di due campagne di phishing nel mese di Luglio 2025 rivolte al personale della DIAQ (42 persone) e ai referenti informatici di Dipartimento/Centro (43 persone), piattaforma utilizzata Knowbe4;
- Avvio di due nuove campagne di phishing dirette al personale strutturato e ai docenti entro il mese di Dicembre 2025 tramite la piattaforma Knowbe4.

Il personale del Gruppo Sicurezza ICT della DIAQ ed i referenti di sicurezza delle strutture (Dipartimenti, Centri) hanno partecipato al **Corso di formazione sulla Cyber Sicurezza** organizzato dal MUR che si è tenuto dal 22 settembre al 15 ottobre per un totale di 32 ore erogate.

L'Ateneo ha aderito all' Iniziativa **Cybersecurity e Governance Universitaria: Strategie, Norme e Innovazione** promossa dall'associazione Cyber 4.0 in collaborazione col CODAU per la formazione dei ruoli apicali in ambito cybersecurity, con l'obiettivo di trasmettere le conoscenze essenziali per comprendere i rischi e le minacce più rilevanti e conoscere il quadro normativo e i propri obblighi di responsabilità, attività che verrà svolta nel 2026.

Il Gruppo Sicurezza ICT ha aderito al **Piano di Supporto agli Atenei per l'adeguamento alla Direttiva NIS2** organizzato sempre dal MUR con l'obbiettivo di accompagnare gli Atenei ad uno sviluppo coordinato della Cybersicurezza. Gli interventi sono previsti tra novembre 2025 e marzo 2026.

Il CRIS predisporrà video formativi sui seguenti contenuti relativi alla cybersecurity awarness, con particolare riguardo al phishing, all'autenticazione multifattore, gestione sicura delle password e delle Misure Minime di Sicurezza predisposte dall'Agenzia per l'Italia Digitale (AGID).

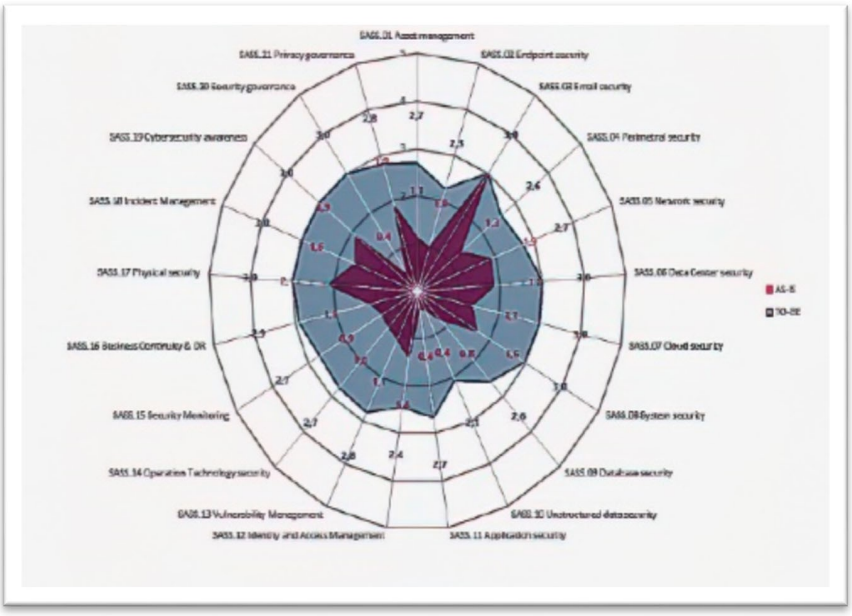
Politiche di analisi dei rischi e di sicurezza dei sistemi informativi

Diversi documenti e procedure sono stati introdotte per identificare e valutare e normare i rischi associati ai sistemi informatici e di rete dell'ateneo. In particolare:

- Approvato documento "**Politica di gestione degli incidenti informatici e segnalazione data breach**", CdA 21 Giugno 2024 (secondo GV.PO-01, p.1, lettere "p", "o", "l")
- Approvato documento "**Politica di gestione degli asset**" con decreto riorganizzazione Direzione Sistemi Informativi e Direzione Economico-Finanziaria), CdA 21 Gennaio 2025(secondo GV.PO-01, p.1, lettera "f")
- Approvato documento "**Procedura di gestione delle patch e delle vulnerabilità**", CdA 21 Febbraio 2025 (secondo GV.PO-01, p.1, lettera "g")
- Approvato documento "**Politica di gestione del cloud**", CdA 21 Gennaio 2025 (secondo GV.PO-01, p.1, lettera "l"
- Approvato documento "**Procedura di utilizzo dei dispositivi istituzionali**", CdA 21 Febbraio 2025 (secondo GV.PO-01, p.1, lettera "i")
- Approvata revisione delle "**Linee guida identità digitale**", CdA 21 Febbraio 2025
- Approvata revisione delle "**Linee guida posta elettronica**", CdA 21 Dicembre 2023 (secondo GV.PO-01, p.1,lettere "n", "l")
- Redazione "**DPIA, Datat Protection Impact Assessment, Google Workspace for Education**" in collaborazione con il DPO di Ateneo, documento interno concordato col DPO il 15 Settembre 2025
- Costituito un gruppo di lavoro sull'AI in Ateneo
- Avviata la **Business Impact Analysis (BIA)** su processi/servizi/sistemi informatici per applicativi e rete basata su form fornito da Cybertech
- Avviata la **Risk Analisys** per la determinazione dell'indice di rischio cyber basata su form fornito da Cybertech
- Stesura bozza "Procedura di utilizzo del cloud", documento in fase di approvazione.

Analisi della postura di Ateneo

Dopo l'implementazione dell'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 riaggiornerà l'analisi nel primo trimestre 2026 con un audit di confronto volto a evidenziare i risultati raggiunti.



Business Impact Analysis

È in fase di completamento, previsto entro fine 2025, la Business Impact Analisys (BIA) finalizzata ad ottenere la lista dei servizi strategici, dei sistemi coinvolti e dei tempi di ripristino tollerati a fronte di incidenti informatici.

Risk Analisys

La prima parte dell'analisi dei rischi è stata completata nel 2024, con il calcolo dell'indice di rischio e definizione delle azioni di mitigazione/contenimento del medesimo, ed è programmato l'aggiornamento entro dicembre 2025 con le ulteriori informazioni provenienti dalla Direzione Tecnica e dall'ufficio SPP.

L'insieme dei risultati provenienti da queste due analisi permetterà di applicare correttamente le misure di sicurezza per la mitigazione dei rischi, di seguito descritte.

Misure di sicurezza per la mitigazione del rischio

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, prevista nel 2026;
- 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 corso del 2026 verrà ulteriormente rafforzata la sicurezza della rete di Ateneo attraverso l'implementazione della metodologia NAC (Network Access Control), che prevede di concedere l'accesso alla rete solo a quelle entità che siano conformi alle policy di Ateneo, sia per quanto attiene alla sicurezza del sistema che l'utente utilizza (registrazione del PC, presenza di antivirus, Patch aggiornate etc etc), sia per l'esistenza dei giusti diritti ad accedere alle risorse per le quali l'utente richiede il collegamento

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. Per mitigare questi pericoli verranno affrontati nel corso del prossimo anno i seguenti temi:

- progettazione ed implementazione di una soluzione di backup "air gapped";
- adozione di servizi di backup di secondo livello in cloud "non modificabili".
- progettazione ed implementazione di un sistema di Disaster Recovery.

Attivazione della Multi Factor Authentication

La Multi Factor Authentication (MFA) aggiunge ai meccanismi di autenticazione basata 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 prevedeva 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.

Si è deciso di affrontare per prima cosa l'attivazione dell'MFA per l'accesso ai servizi web che richiedono l'autenticazione SSO.

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

Nel corso del 2025, con il supporto del CRIS è stato configurato il servizio IDP di Unimore, creato il portale mfaselfservice.unimore.it per l'attivazione in autonomia del secondo fattore, è stato istituto presso la DIAQ il supporto di II livello e sono stati incaricati del supporto di I livello i referenti di sicurezza delle strutture.

Per supportare il passaggio al MFA **per tutto il personale strutturato dell'Ateneo**, che si è completato il 20 ottobre 2025, sono stati organizzati tre corsi di formazione per il personale della sede di Reggio Emilia, per quello di Modena ed uno particolare rivolto al personale dell'Amministrazione Centrale, con il supporto dei vari referenti coinvolti e un supporto istituito ad hoc per il personale dell'Amministrazione centrale.

Soluzioni in Cloud

Nell'ambito del potenziamento della strategia di migrazione al Cloud, sono in corso di verifica le politiche di sicurezza e privacy delle soluzioni cloud attive in Ateneo (Microsoft e Google) ed 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; 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.
È stata approvato il documento "**Politica di gestione del cloud**" nel CdA 21 gennaio 2025.
È stato rilasciato il documento "**DPIA, Datat Protection Impact Assessment, Google Workspace for Education**" in collaborazione con il DPO di Ateneo, documento interno del 15 settembre 2025 volto ad aumentare il livello di sicurezza dell'ambiente Office 365 attraverso il partner Microsoft erogando inoltre una specifica formazione.

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 sta usa 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 fa o 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.

La DIAQ ha aderito nel gennaio 2025 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).

Nel dettaglio sono state sviluppate le seguenti attività:

- Attivazione servizio SOC con Certego s.r.l. e altri fornitori della convenzione Fastweb;
- Attivato backup di II livello delle VM critiche della piattaforma Nutanix su datacenter Lepida di Ravenna;
- Installato il client Carbon Black su PC, server e thin client dell'Amministrazione Centrale per invio dati al SOC;
- Approvato documento "Politica di gestione degli incidenti informatici e segnalazione data breach", CdA 21 giugno 2024 (secondo GV.PO-01, p.1, lettere "p", "o", "l");
- Costituito il gruppo CSIRT e l'organigramma, decreto DIAQ del 16 gennaio 2025, Prot. N. 0011480;
- Definizione workflow operativo;
- Analisi tassonomia ACN;
- Individuazione referente di sicurezza in ogni struttura compresa l'Amministrazione Centrale e formazione periodica ai referenti sui temi della sicurezza
- Attivazione Fascicolo delle evidenze come da POL01
- Adesione servizio Ihavebeenpwned con sottoscrizione annuale
- Adesione servizio IOC di CERT-Agid per Clamav e Forticlient https://cert-agid.gov.it/scarica-il-modulo-accreditamento-feed-ioc/ (indicatori di compromissione)
- Realizzazione di un applicativo per la gestione del registro incidenti e del flusso operativo di un incidente da parte del CSIRT (affidamento Proge Software, rilascio 2 Ottobre 2025).

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 implementa su rete, 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.

Sono state implementate le seguenti azioni:

- Individuazione dei referenti di sicurezza di struttura;
- Attivazione sistema di scansioni periodiche delle sottoreti e analisi vulnerabilità da parte dei referenti di sicurezza (VAPT, realizzato da CRIS) e attivazione sito SharePoint dedicato https://unimore365.sharepoint.com/sites/SicurezzaICT
- Progressiva sostituzione desktop del personale dell'Amministrazione Centrale con thin client sulla base del Progetto di virtualizzazione dei desktop.

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 informa che più frequenti. Le misure consistono in controlli di natura tecnologica, organizzativa e procedurale utile 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].

E’ prevista una revisione periodica delle MMS di strutture e dell’Amministrazione Centrale, prossima revisione con adeguamento a misure di livello Standard [S] entro Dicembre 2025 con il supporto dei referenti di sicurezza delle strutture e con il referente del DSCG, Massimo Barbieri, con cui è partita una collaborazione sui temi di sicurezza a seguito di autorizzazione del Direttore del DSCG.