Università degli studi di Verona

NIS2: POLITICA PER LA SICUREZZA DEI SISTEMI INFORMATIVI E DI RETE

Adottata ai sensi del D.Lgs. 4 settembre 2024, n. 138

1 Contesto normativo e ambito di riferimento

La presente Politica si inserisce in un quadro normativo e tecnico di carattere multilivello, i cui elementi sono tra loro gerarchicamente ordinati e funzionalmente coordinati.

Al primo livello si colloca la Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 (di seguito, "Direttiva NIS2"), che stabilisce misure volte a garantire un livello comune elevato di cybersicurezza nell'Unione europea. La Direttiva definisce gli obblighi applicabili ai soggetti essenziali e importanti in materia di gestione del rischio per la sicurezza informatica, notifica degli incidenti significativi, sicurezza della catena di approvvigionamento e responsabilità degli organi di governo e direttivi. In quanto direttiva, essa vincola gli Stati membri quanto al risultato da conseguire, lasciando alla competenza degli ordinamenti nazionali la determinazione della forma e dei mezzi di recepimento.

Al secondo livello si colloca il Decreto legislativo 4 settembre 2024, n. 138 (di seguito, "Decreto NIS2"), che ha dato attuazione alla Direttiva NIS2 nell'ordinamento giuridico italiano. Il Decreto individua i soggetti destinatari degli obblighi, distinguendo tra soggetti essenziali e soggetti importanti in ragione del settore di appartenenza, delle dimensioni e del livello di esposizione al rischio, e definisce il sistema di vigilanza e il regime sanzionatorio applicabile. All'art. 31, il Decreto attribuisce all'Agenzia per la Cybersicurezza Nazionale (ACN), nella sua qualità di Autorità nazionale competente NIS e di CSIRT Italia, il potere di stabilire le modalità e le specifiche di base per l'adempimento degli obblighi previsti, nel rispetto del principio di proporzionalità riferito all'esposizione al rischio, alle dimensioni del soggetto e alla probabilità e gravità degli incidenti. Per il settore dell'istruzione superiore e della ricerca, il Ministero dell'Università e della Ricerca (MUR) esercita le funzioni di Autorità di settore NIS ai sensi degli artt. 10 e 11 del medesimo Decreto.

Al terzo livello si collocano le Determinazioni dell'ACN, adottate nell'esercizio dei poteri conferiti dal Decreto NIS2 e vincolanti nei rispettivi ambiti di applicazione. Rilevano in particolare la Determinazione ACN n. 379907 del 19 dicembre 2025, recante le specifiche di base per gli obblighi di sicurezza e di notifica, la Determinazione ACN n. 127437 del 13 aprile 2026, relativa alla piattaforma digitale, all'aggiornamento delle informazioni e agli ulteriori adempimenti connessi, e la Determinazione ACN n. 155238 del 20 aprile 2026, relativa alle categorie di rilevanza e al processo, alle modalità e ai criteri per l'elencazione, la caratterizzazione e la categorizzazione delle attività e dei servizi ai sensi dell'art. 30 del D.Lgs. 138/2024. Tali atti specificano, secondo il rispettivo oggetto, misure di sicurezza, requisiti minimi, incidenti significativi, ruoli e adempimenti informativi applicabili ai soggetti NIS.

Le misure di sicurezza definite dalle Determinazioni recepiscono, adattandolo al contesto normativo e operativo italiano, il NIST Cybersecurity Framework (CSF). Le sei funzioni del Framework — Govern, Identify, Protect, Detect, Respond, Recover — articolano la struttura portante entro cui sono classificate le misure applicabili al soggetto NIS, ciascuna identificata mediante il codice alfanumerico XX.YY-NN, indicativo della funzione, della categoria e della sottocategoria di appartenenza.

A partire dall’aprile 2025, l’Ateneo è stato incluso nell’elenco dei “soggetti importanti” ai sensi dell’art. 3 del Decreto, risultando pertanto destinatario dell’insieme degli obblighi previsti, in particolare, dagli artt. 21–26, tra cui l’adozione di misure tecniche, operative e organizzative adeguate e proporzionate, la

gestione del rischio informatico, la notifica degli incidenti significativi e la sottoposizione alle attività di supervisione da parte delle autorità competenti.

La presente Politica per la sicurezza dei sistemi informativi e di rete (di seguito, la "Politica") è adottata in attuazione dell'art. 21, par. 2, lett. a) della Direttiva NIS2, dell'art. 24 del Decreto NIS2 e delle specifiche di base adottate dall'ACN. La Politica è sottoposta all'approvazione del Consiglio di Amministrazione quale organo competente ai fini dell'art. 23 del D.Lgs. 138/2024; il parere del Senato Accademico interviene secondo il procedimento interno dell'Ateneo e le rispettive competenze statutarie e regolamentari.

Si applica all'intero perimetro organizzativo, tecnologico e informativo dell'Ateneo, secondo un approccio progressivo e basato sul rischio, coerente con quanto previsto dalla normativa di riferimento.

Le strutture dell'Ateneo — ivi compresi i Dipartimenti, i Centri di ricerca interdipartimentali e di Ateneo, le Scuole, i Centri di servizio, le Direzioni e le Aree dell'Amministrazione centrale, le Biblioteche e ogni altra struttura organizzativa comunque denominata — sono tenute al pieno rispetto della presente Politica e delle Procedure specifiche per argomento emanate in sua attuazione, ciascuna per quanto di propria competenza e in relazione ai sistemi informativi e di rete da esse utilizzati o gestiti.

La presente Politica si applica, quale indirizzo interno dell'Ateneo, alla totalità dei sistemi informativi, delle reti, delle applicazioni, dei dati e delle infrastrutture tecnologiche, indipendentemente dall'ubicazione fisica o dalla modalità di gestione. Ai fini degli obblighi NIS, l'individuazione dei sistemi informativi e di rete rilevanti (SIR) avviene secondo la normativa applicabile e il documento "Organizzazione per la sicurezza informatica". Sono destinatari della presente Politica tutti i soggetti che, a qualsiasi titolo, accedono o trattano sistemi informativi e di rete dell'Ateneo, incluse le parti esterne nei limiti dei rispettivi rapporti contrattuali.

1.1 Finalità e natura della presente Politica

La Politica definisce i principi, gli obiettivi e le responsabilità in materia di sicurezza informatica, costituendo il quadro di riferimento per la progettazione, l'attuazione, il monitoraggio e il miglioramento continuo delle misure di sicurezza adottate dall'Ateneo.

Il presente costituisce un documento di indirizzo strategico e di governo, volto a definire il quadro dei principi, degli impegni e delle priorità entro cui le misure di sicurezza devono essere progettate e attuate. La declinazione operativa dei suoi contenuti è demandata ai piani, alle politiche tematiche e alle procedure attuative, adottati dai competenti livelli di responsabilità secondo la matrice dei documenti NIS e dei livelli di approvazione contenuta nella presente Politica.

La Politica ha carattere vincolante per l'intera organizzazione e si configura come un documento dinamico, soggetto a revisione periodica almeno annuale, nonché ogniqualvolta si verifichino incidenti significativi o mutamenti rilevanti nel contesto operativo o nel profilo di rischio dell'Ateneo. La sua efficacia è strettamente connessa non solo alla qualità dei contenuti, ma anche alla capacità dell'organizzazione di tradurli in pratiche operative concrete, diffuse e costantemente aggiornate.

1.2 Impegno per la sicurezza

1.2.1 Stakeholder

L'Ateneo riconosce che la gestione del rischio informatico, quale presupposto essenziale per garantire la sicurezza dei sistemi informativi e di rete, costituisce un elemento fondamentale per la protezione dei servizi erogati, la tutela dei diritti e degli interessi degli utenti e dei portatori di interesse, nonché per l'assicurazione della continuità operativa delle funzioni istituzionali di didattica, ricerca e terza missione.

L'Ateneo riconosce, inoltre, che la sicurezza dei propri sistemi informativi e di rete non costituisce un ambito esclusivamente interno, ma incide direttamente sulla fiducia e sulle legittime aspettative di una pluralità di stakeholder, tra i quali:

- la comunità studentesca, ivi compresi gli studenti iscritti ai corsi di laurea, laurea magistrale, dottorato di ricerca, master, scuole di specializzazione e corsi di formazione continua, i cui dati personali, le carriere accademiche e l'accesso ai servizi digitali dipendono dalla sicurezza dei sistemi dell'Ateneo;

- il personale docente e ricercatore, strutturato e non strutturato, compresi assegnisti, borsisti e visiting professor, la cui attività di ricerca e didattica si fonda in misura crescente su infrastrutture digitali, piattaforme collaborative e banche dati;

- il personale tecnico-amministrativo, CEL e bibliotecario, che opera quotidianamente sui sistemi informativi dell'Ateneo e ne rappresenta al contempo un presidio operativo e un potenziale vettore di rischio;

- Rettrice/Rettore, Senato Accademico, Consiglio di amministrazione, Direttrice/Direttore Generale, Dirigenti, Nucleo di Valutazione, Collegio dei Revisori dei Conti, Presidio della Qualità — ai quali compete la responsabilità della supervisione delle misure di sicurezza sulle base delle rispettive competenze;

- le Autorità competenti e di vigilanza, in primo luogo l'ACN, il CSIRT Italia e il MUR in qualità di Autorità di settore NIS, nonché il Garante per la protezione dei dati personali, l'ANAC e gli altri organismi di controllo cui l'Ateneo è soggetto;

- i partner di ricerca nazionali e internazionali, incluse le università, gli enti pubblici di ricerca, le imprese e i consorzi con i quali l'Ateneo condivide dati, infrastrutture, laboratori e progetti collaborativi, e nei confronti dei quali sussistono obblighi di riservatezza e protezione delle informazioni spesso regolati da accordi specifici;

- le istituzioni pubbliche e gli enti finanziatori, tra cui il MUR, la Commissione Europea, le agenzie di finanziamento nazionali e internazionali, le fondazioni e gli enti territoriali, i quali affidano all'Ateneo risorse pubbliche e si attendono una gestione sicura e conforme delle informazioni connesse ai programmi finanziati;

- i fornitori, i prestatori di servizi e i partner tecnologici che accedono ai sistemi informativi dell'Ateneo o ne trattano i dati, e la cui catena di approvvigionamento costituisce essa stessa un vettore di rischio da presidiare;

- gli organismi di accreditamento e certificazione, sia in ambito accademico (ANVUR) sia in ambito di sicurezza delle informazioni (organismi di certificazione ISO/IEC 27001), nei confronti dei quali l'Ateneo è tenuto a dimostrare la conformità dei propri processi;

- le aziende e gli enti ospitanti tirocini, stage e percorsi di apprendistato, con i quali intercorrono flussi informativi relativi ai dati degli studenti;

- la collettività e il tessuto socio-economico del territorio, che beneficiano dei servizi pubblici erogati dall'Ateneo — dalla formazione alla ricerca applicata, dai servizi bibliotecari ai servizi sanitari universitari — e che hanno un legittimo interesse alla resilienza e alla continuità di tali servizi.

1.3 Obiettivi

La presente Politica esprime l'impegno dell'Ateneo a tutelare le aspettative di tutti i portatori di interesse sopra richiamati, mediante l'adozione di un livello di sicurezza adeguato, proporzionato e verificabile, assicurando al contempo trasparenza e responsabilità nella gestione del rischio informatico e mantenendo un dialogo costante e costruttivo con ciascuna categoria di stakeholder, nei modi e nelle forme appropriati al rispettivo ruolo e alle rispettive esigenze informative.

A tal fine, l'Ateneo si impegna a implementare misure tecniche, operative e organizzative adeguate e proporzionate ai rischi identificati, in conformità agli artt. 24 e 25 del D.Lgs. 138/2024, e perseguire i seguenti obiettivi:

- garantire la riservatezza, l'integrità e la disponibilità delle informazioni e dei servizi rilevanti per lo svolgimento delle attività istituzionali dell'Ateneo;

- gestire in modo sistematico i rischi connessi alla sicurezza dei sistemi informativi e di rete, attraverso un approccio multirischio e proporzionato che tenga conto dello stato dell'arte, delle peculiarità della nostra organizzazione, della probabilità e della gravità degli incidenti, nonché del loro potenziale impatto economico e sociale;

- rafforzare la resilienza complessiva dell'Ateneo, intesa come la capacità dell'organizzazione di prevenire, resistere, assorbire e ripristinare le proprie funzioni a fronte di eventi avversi che colpiscano i sistemi informativi e di rete, assicurando la continuità dei servizi essenziali anche in condizioni degradate;

- rafforzare le capacità di prevenzione, rilevazione, contenimento e risposta agli incidenti di sicurezza, riducendone al minimo gli impatti sulla continuità e sulla qualità dei servizi erogati, e garantendo il rispetto degli obblighi di notifica tempestiva alle Autorità competenti;

- ridurre la superficie di attacco dei sistemi informativi e di rete, adottando misure tecniche e organizzative adeguate allo stato dell'arte e coerenti con il contesto operativo, incluse pratiche di igiene informatica, gestione delle vulnerabilità e principi di sicurezza fin dalla progettazione (*security by design* e *security by default*);

- garantire la sicurezza della catena di approvvigionamento, valutando e gestendo i rischi derivanti dalle relazioni con i fornitori diretti e i prestatori di servizi, e integrando requisiti di sicurezza nei rapporti contrattuali;

- promuovere una cultura diffusa della sicurezza informatica a tutti i livelli dell'organizzazione, attraverso programmi di sensibilizzazione e formazione continua rivolti, ove pertinente, a tutti gli stakeholders;

- assicurare la governance della sicurezza informatica al più alto livello decisionale, tramite l'approvazione e la supervisione dei documenti strategici da parte del Consiglio di Amministrazione e l'adozione delle procedure attuative da parte della Direttrice/Direttore Generale o dei dirigenti competenti secondo l'assetto organizzativo interno;

- garantire il rispetto dei requisiti normativi e regolamentari applicabili, con particolare riferimento alla Direttiva NIS2, al Decreto di recepimento e alle determinazioni delle Autorità competenti; gli atti europei rivolti a specifiche categorie di soggetti, tra cui il Regolamento di esecuzione (UE) 2024/2690, sono considerati nei casi di diretta applicabilità e, ove pertinente, quali riferimenti tecnico-metodologici;

1.4 Risorse

Il Consiglio di amministrazione, su parere del Senato Accademico, nell'approvare la presente Politica, assume formalmente l'impegno a garantire la disponibilità delle risorse necessarie per la sua piena ed efficace attuazione. L'attuazione di questo impegno si sviluppa attraverso le seguenti componenti

- assicurare la disponibilità di personale sufficiente, dotato delle competenze richieste o messo nelle condizioni di acquisirle mediante percorsi formativi mirati, per l'esercizio dei ruoli e delle funzioni di sicurezza definiti dalla presente Politica, dalla struttura di governance e dalle politiche tematiche di settore; qualora le dimensioni o le specificità dell'organizzazione lo richiedano, l'Ateneo valuterà il ricorso a figure professionali dedicate o a competenze esterne qualificate;

- prevedere nei documenti di programmazione economico-finanziaria le risorse necessarie a sostenere gli investimenti in sicurezza informatica, coerentemente con i risultati della valutazione del rischio, le priorità definite nel piano di trattamento e gli obblighi normativi vigenti; la pianificazione terrà conto sia delle spese ricorrenti (manutenzione, licenze, formazione, servizi gestiti) sia degli investimenti straordinari richiesti per il percorso di adeguamento;

- definire, documentare e aggiornare i processi organizzativi e le procedure operative necessari a tradurre i principi della presente Politica in azioni concrete, misurabili e verificabili, assicurando la coerenza tra processi di sicurezza e processi istituzionali dell'Ateneo;

- dotare l'organizzazione di infrastrutture tecnologiche e strumenti tecnici adeguati al livello di sicurezza richiesto dalla normativa e proporzionati ai rischi identificati, garantendone aggiornamento e manutenzione nel tempo, tenendo conto dello stato dell'arte e delle indicazioni delle Autorità competenti.

1.5 Strategia e percorso di adeguamento

La presente Politica non opera in modo isolato, bensì si inserisce in modo organico nel sistema dei documenti di governo e di programmazione strategica dell'Ateneo, dei quali costituisce il naturale complemento per i profili attinenti alla sicurezza informatica. L'Ateneo riconosce la sicurezza informatica quale condizione abilitante per il perseguimento della propria missione istituzionale e assume la conformità alla Direttiva NIS2 come obiettivo strategico, da perseguire mediante un approccio progressivo, strutturato e sostenibile, fondato sulla valorizzazione delle iniziative già intraprese e sullo sviluppo di una cultura organizzativa orientata alla sicurezza.

1.6 Percorso di adeguamento

L'Ateneo riconosce che la conformità alla Direttiva NIS2 non costituisce un obiettivo statico, bensì un processo continuo e strutturato, basato su un approccio di miglioramento progressivo.

In tale ottica, la presente Politica formalizza l'impegno dell'organizzazione ad adottare un modello di gestione della sicurezza fondato sulla valutazione e sul trattamento del rischio, nonché sulla capacità di prevenzione, rilevazione e risposta agli incidenti di sicurezza.

Le misure, i piani, le procedure, i registri e gli ulteriori documenti attuativi richiamati dalla presente Politica sono adottati, aggiornati e attuati secondo il piano di adeguamento e il cronoprogramma approvati dagli organi competenti. Ove non ancora formalizzati alla data di approvazione della presente Politica, i relativi documenti attuativi saranno adottati entro le scadenze normative applicabili e resi coerenti con il quadro documentale NIS dell'Ateneo. Restano comunque fermi gli obblighi già vigenti, in particolare quelli relativi alla gestione e alla notifica degli incidenti di sicurezza informatica.

2 La certificazione ISO/IEC 27001:2022

Gli obblighi NIS non vengono calati in un Ateneo privo di esperienza in materia di cybersecurity, ma si considera la cultura di sicurezza informatica e la maturità già raggiunta nel contesto della Direzione Informatica e Tecnologie che dal 2023 è certificata secondo lo standard ISO 27001.

La certificazione ISO/IEC 27001:2022 rappresenta lo standard internazionale di riferimento per i sistemi di gestione della sicurezza delle informazioni e attesta l'adozione, da parte della Direzione Informatica e Tecnologie, di un modello fondato sulla gestione del rischio e sul miglioramento continuo, nonché l'implementazione di controlli tecnici e organizzativi a tutela della riservatezza, dell'integrità e della disponibilità delle informazioni.

Tale standard si pone in coerenza con i principali framework internazionali di cybersecurity, tra cui il NIST Cybersecurity Framework, con il quale condivide l'approccio basato sull'identificazione, protezione, rilevazione, risposta e recupero degli incidenti, e risulta pienamente allineato ai principi e agli obblighi introdotti dalla Direttiva NIS2. La certificazione ISO/IEC 27001, pertanto, costituisce un solido punto di partenza e un riferimento metodologico per l'estensione e il consolidamento delle misure

di sicurezza a livello di Ateneo, valorizzando il patrimonio di competenze e pratiche già sviluppato e favorendo un percorso strutturato di conformità alla normativa vigente.

L'Ateneo considera di particolare importanza mantenere livelli concentrici di sicurezza: la NIS2 copre il perimetro dell'Ateneo, ma per quanto riguarda la Direzione Informatica e Tecnologie, che sovrintende la maggioranza dei sistemi rilevanti, è ritenuto strategico un rafforzamento delle misure così come derivanti dalla Norma ISO.

La certificazione ISO/IEC 27001 conseguita dalla Direzione Informatica e Tecnologie costituisce quindi una base metodologica e organizzativa robusta per il percorso di adeguamento NIS dell'Ateneo. Essa non esaurisce, tuttavia, il perimetro degli obblighi NIS, che riguardano l'intera organizzazione secondo un approccio proporzionato, progressivo e basato sul rischio. L'estensione del modello richiede pertanto l'adattamento, la formalizzazione, l'attuazione e la verifica delle misure in relazione all'intero perimetro organizzativo, tecnologico e informativo dell'Ateneo.

Si illustra di seguito il panorama dei requisiti normativi derivanti dalla Direttiva (UE) 2022/2555 e dal decreto legislativo di recepimento, come declinati nella Determinazione ACN 379907/2025, recante le Specifiche per l'adozione delle misure di sicurezza per i soggetti di cui all'articolo 3 del decreto NIS2, che definisce nel dettaglio il framework di misure di sicurezza di base e le modalità di implementazione da parte dei soggetti essenziali e importanti.

A partire dalle misure di sicurezza di base l'Ateneo ha definito le misure tecniche e organizzative e la documentazione a loro sostegno.

Di seguito è riportata la tabella di correlazione tra le misure di sicurezza di base e la documentazione predisposta. Nella colonna documentale i riferimenti sono ordinati secondo una gerarchia esplicita: prima i documenti NIS di indirizzo, governo e pianificazione approvati o sottoposti all'approvazione del Consiglio di Amministrazione; a seguire gli eventuali allegati NIS; infine le procedure, i registri e le altre evidenze del SGSI ISO/IEC 27001 che ne supportano l'attuazione. La convenzione grafica adottata è la seguente: **neretto = documenti NIS**; *corsivo = procedure, registri ed evidenze SGSI ISO/IEC 27001*. Le procedure SGSI mantengono la propria validità operativa nel rispettivo perimetro, ma non sostituiscono né prevalgono sui documenti NIS di governo. La tabella ha funzione di raccordo e non sostituisce il testo vigente delle specifiche ACN: ai fini della conformità prevalgono in ogni caso la Determinazione ACN n. 379907/2025, il relativo Allegato 1 applicabile ai soggetti importanti e le successive determinazioni o modifiche vigenti.

Direttiva (UE) 2022/2555	**D.lgs. 138/2024**	**ID Framework NIST**	**MISURA DI SICUREZZA DI BASE** Determinazione ACN 379907/2025	**Documentazione di Ateneo (framework NIS e SGSI ISO/IEC 27001)**
1. GOVERNO (GOVERN)				
		GV.OC	**Il contesto – missione, aspettative degli stakeholder, dipendenze e requisiti legali, normativi e contrattuali – che influisce sulle decisioni di gestione del rischio di cybersecurity dell'organizzazione è compreso.**	

Art. 20	**Art. 23**	**GV.OC-04**	**Gli obiettivi, le capacità e i servizi critici dai quali gli stakeholder dipendono o che si aspettano dall'organizzazione sono compresi e comunicati.** 1. È mantenuto un elenco aggiornato dei sistemi informativi e di rete rilevanti.	▪ **POLITICA PER LA SICUREZZA DEI SISTEMI INFORMATIVI E DI RETE** ▪ **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** ▪ *PROCEDURA PER LA GESTIONE DELL'INVENTARIO DEI SISTEMI INFORMATIVI DI RETE*
		GV.RM	**Le priorità, i vincoli, le dichiarazioni sulla tolleranza e la propensione al rischio, e le assunzioni dell'organizzazione sono stabilite, comunicate e utilizzate per supportare le decisioni sul rischio operativo.**	
Art. 21 §2(a)	**Art. 24 c.2(a)**	**GV.RM-03**	**Le attività e gli esiti della gestione del rischio di cybersecurity sono parte integrante dei processi di gestione del rischio dell'organizzazione.** 1. Nell'ambito dei processi di gestione del rischio del soggetto NIS e nel rispetto delle politiche di cui alla misura GV.PO-01, è definito, attuato, aggiornato e documentato un piano di gestione dei rischi per la sicurezza informatica per identificare, analizzare, valutare, trattare e monitorare i rischi.	▪ **VALUTAZIONE DEL RISCHIO POSTO ALLA SICUREZZA DEI SISTEMI INFORMATIVI E DI RETE** ▪ **PIANO DI TRATTAMENTO DEL RISCHIO E DI GESTIONE DELLE CRISI** ▪ **ALL004 - ELENCO RISCHI INDIVIDUATI E RISK OWNER**

			GV.RR	**I ruoli, le responsabilità e i correlati poteri in materia di cybersecurity per promuovere l'accountability, la valutazione delle prestazioni e il miglioramento continuo sono stabiliti e comunicati.**	
Art. 21 §2(a)		**Art. 24 c.2(a)**	**GV.RR-02**	**I ruoli, le responsabilità e i correlati poteri relativi alla gestione del rischio di cybersecurity sono stabiliti, comunicati, compresi e applicati.** 1. È definita, approvata dagli organi di amministrazione e direttivi, e resa nota alle articolazioni competenti del soggetto NIS, l'organizzazione per la sicurezza informatica e ne sono stabiliti ruoli e responsabilità. 2. È mantenuto un elenco aggiornato del personale dell'organizzazione di cui al punto 1 avente specifici ruoli e responsabilità ed è reso noto alle articolazioni competenti del soggetto NIS. 3. All'interno dell'organizzazione per la sicurezza informatica di cui al punto 1, sono inclusi il Punto di contatto e il suo sostituto, il Referente CSIRT e gli eventuali suoi sostituti, secondo la determinazione adottata ai sensi dell'articolo 7, comma 6, del decreto NIS.	▪ **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** ▪ **ALLEGATO - MATRICE RACI** ▪ *ORGANIGRAMMA PER LA SICUREZZA (evidenza SGSI)* ▪ *PROCEDURA DI SELEZIONE E FORMAZIONE DEL PERSONALE (evidenza SGSI)*

				4. I ruoli e le responsabilità di cui al punto 1 sono riesaminati e, se opportuno, aggiornati periodicamente e comunque almeno ogni due anni, nonché qualora si verifichino incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.	
Art. 20	**Art. 23**	**GV.RR-04**	**La cybersecurity è inclusa nelle pratiche delle risorse umane.**	1. Per almeno i sistemi informativi e di rete rilevanti, il personale autorizzato ad accedervi è individuato previa valutazione dell'esperienza, capacità e affidabilità e deve fornire idonea garanzia del pieno rispetto della normativa in materia di sicurezza informatica. 2. Gli amministratori di sistema dei sistemi informativi e di rete sono individuati previa valutazione dell'esperienza, capacità e affidabilità e devono fornire idonea garanzia del pieno rispetto della normativa in materia di sicurezza informatica. 3. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1 e 2.	▪ **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA (cap. 12)** ▪ *PROCEDURA DI SELEZIONE E FORMAZIONE DEL PERSONALE* ▪ *PROCEDURA PER LA GESTIONE DELLA ATTIVAZIONE, VARIAZIONE E CESSAZIONE DEL RAPPORTO DI LAVORO*

			GV.PO	**La politica di cybersecurity dell'organizzazione è stabilita, comunicata e applicata.**	
Art. 21 §2(a)		**Art. 24 c.2(a)**	**GV.PO-01**	**La politica per la gestione del rischio di cybersecurity è stabilita in base al contesto organizzativo, alla strategia di cybersecurity e alle priorità, ed è comunicata e applicata.** 1. Sono adottate e documentate politiche di sicurezza informatica per almeno i seguenti ambiti: a) gestione del rischio; b) ruoli e responsabilità; c) affidabilità delle risorse umane; d) conformità e audit di sicurezza; e) gestione dei rischi per la sicurezza informatica della catena di	▪ **POLITICA PER LA SICUREZZA DEI SISTEMI INFORMATIVI E DI RETE** ▪ **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** ▪ **VALUTAZIONE DEL RISCHIO POSTO ALLA SICUREZZA DEI SISTEMI INFORMATIVI E DI RETE** ▪ **PIANO DI TRATTAMENTO DEL RISCHIO E DI GESTIONE DELLE CRISI** ▪ **PIANO DI GESTIONE DELLE VULNERABILITÀ** ▪ **PIANO DI ADEGUAMENTO DELLE MISURE DI SICUREZZA** ▪ **PIANO DI CONTINUITÀ OPERATIVA E DI RIPRISTINO IN CASO DI DISASTRO** ▪ **PIANO PER LA GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA** ▪ **PIANO DI FORMAZIONE IN MATERIA DI SICUREZZA INFORMATICA**

				approvvigionamento; f) gestione degli asset; g) gestione delle vulnerabilità; h) continuità operativa, ripristino in caso di disastro e gestione delle crisi; i) gestione dell'autenticazione, delle identità digitali e del controllo accessi; j) sicurezza fisica; k) formazione del personale e consapevolezza; l) sicurezza dei dati; m) sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete; n) protezione delle reti e delle comunicazioni; o) monitoraggio degli eventi di sicurezza; p) risposta agli incidenti e ripristino. 2. Per gli ambiti di cui al punto 1 sono incluse almeno le politiche in relazione ai requisiti indicati nella tabella 1 in appendice al presente allegato. 3. Le politiche di cui al punto 1 sono approvate dagli organi di amministrazione e direttivi.	
Art. 21 §2(a)	**Art. 24 c.2(a)**	**GV.PO-02**	**La politica per la gestione del rischio di cybersecurity è revisionata, aggiornata, comunicata e applicata per riflettere i cambiamenti nei requisiti, nelle minacce, nella tecnologia e nella missione dell'organizzazione.**		▪ **POLITICA PER LA SICUREZZA DEI SISTEMI INFORMATIVI E DI RETE** ▪ **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** ▪ **VALUTAZIONE DEL RISCHIO POSTO ALLA SICUREZZA DEI SISTEMI INFORMATIVI E DI RETE** ▪ **PIANO DI TRATTAMENTO DEL RISCHIO E DI GESTIONE DELLE CRISI** ▪ **PIANO DI GESTIONE DELLE VULNERABILITÀ** ▪ **PIANO DI ADEGUAMENTO DELLE MISURE DI SICUREZZA** ▪ **PIANO DI CONTINUITÀ OPERATIVA E DI RIPRISTINO IN CASO DI DISASTRO** ▪ **PIANO PER LA GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA**

					▪ **PIANO DI FORMAZIONE IN MATERIA DI SICUREZZA INFORMATICA** ▪ *PRO028 - PROCEDURA DI AUDITING E RAPPORTI DI AUDIT*
				1. Le politiche di cui alla misura GV.PO-01 sono riesaminate e, se opportuno, aggiornate periodicamente e comunque almeno con cadenza annuale, nonché qualora si verifichino evoluzioni del contesto normativo in materia di sicurezza informatica, incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi. 2. Ai fini del riesame di cui al punto 1, è verificata almeno la conformità delle politiche di cui alla misura GV.PO-01 alla normativa in materia di sicurezza informatica.	
			GV.SC	**I processi di gestione del rischio di cybersecurity della catena di approvvigionamento sono identificati, stabiliti, gestiti, monitorati e migliorati dagli stakeholder dell'organizzazione.**	
Art. 21 §2(d)		**Art. 24 c.2(d)**	**GV.SC-01**	**Sono stabiliti e accettati dagli stakeholder dell'organizzazione un programma, una strategia, obiettivi, politiche e processi di gestione del rischio di cybersecurity della catena di approvvigionamento.** 1. In merito all'affidamento di forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete, sono previsti: a) il coinvolgimento dell'organizzazione per la sicurezza informatica di cui alla misura GV.RR-02 nella definizione ed esecuzione dei processi di approvvigionamento a	▪ **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** ▪ **ALLEGATO - MATRICE RACI** ▪ *PROCEDURA PER LA SICUREZZA INFORMATICA DELLA CATENA DI APPROVVIGIONAMENTO E RELATIVI ALLEGATI*

					partire dalla fase di identificazione e progettazione della fornitura; b) in accordo agli esiti della valutazione del rischio associato alla fornitura di cui alla misura GV.SC-07, la definizione di requisiti di sicurezza sulla fornitura coerenti con le misure di sicurezza applicate dal soggetto NIS ai sistemi informativi e di rete.	
Art. 21 §2(d)		**Art. 24 c.2(d)**		**GV.SC-02**	**I ruoli e le responsabilità in materia di cybersecurity per fornitori, clienti e partner sono stabiliti, comunicati e coordinati internamente ed esternamente.** 1. Nell'ambito dell'organizzazione per la sicurezza informatica di cui alla misura GV.RR-02, sono definiti e resi noti alle articolazioni competenti del soggetto NIS gli eventuali ruoli e responsabilità in materia di sicurezza informatica assegnati al personale delle terze parti. 2. Il personale di cui al punto 1 avente specifici ruoli e responsabilità è incluso nell'elenco di cui al punto 2 della misura GV.RR-02.	▪ **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** ▪ **ALLEGATO - MATRICE RACI** ▪ *PROCEDURA PER LA SICUREZZA INFORMATICA DELLA CATENA DI APPROVVIGIONAMENTO E RELATIVI ALLEGATI*
Art. 21 §2(d)		**Art. 24 c.2(d)**		**GV.SC-04**	**I fornitori sono noti e prioritizzati in base alla criticità.** 1. È mantenuto un inventario aggiornato dei fornitori, le cui forniture hanno un potenziale impatto sulla sicurezza dei sistemi informativi e di rete,	▪ *PROCEDURA PER LA SICUREZZA INFORMATICA DELLA CATENA DI APPROVVIGIONAMENTO E RELATIVI ALLEGATI*

				che comprende almeno: a) gli estremi di contatto del referente della fornitura; b) la tipologia di fornitura.	
Art. 21 §2(d)		**Art. 24 c.2(d)**	**GV.SC-05**	**I requisiti per affrontare i rischi di cybersecurity nella catena di approvvigionamento sono stabiliti, prioritizzati e integrati nei contratti e in altri tipi di accordi con i fornitori e altre terze parti rilevanti.** 1. Fatte salve motivate e documentate ragioni normative o tecniche, i requisiti di sicurezza di cui alla misura GV.SC-01, punto 1, lettera b) sono inseriti nelle richieste di offerta, bandi di gara, contratti, accordi e convenzioni relativi alle forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete.	▪ *PROCEDURA PER LA SICUREZZA INFORMATICA DELLA CATENA DI APPROVVIGIONAMENTO E RELATIVI ALLEGATI*
Art. 21 §2(d)		**Art. 24 c.2(d)**	**GV.SC-07**	**I rischi posti da un fornitore, dai suoi prodotti e servizi e da altre terze parti sono compresi, registrati, prioritizzati, valutati, trattati e monitorati nel corso della relazione.** 1. Nell'ambito della valutazione del rischio di cui alla misura ID.RA-05, è valutato e documentato il rischio associato alle forniture. A tal fine, sono valutati almeno: a) il livello di accesso del fornitore ai sistemi informativi e di rete del soggetto NIS; b) l'accesso del fornitore alla proprietà intellettuale e ai dati anche sulla base della loro criticità; c) l'impatto di una grave interruzione della fornitura; d) i tempi e i costi di ripristino in caso di	▪ **VALUTAZIONE DEL RISCHIO POSTO ALLA SICUREZZA DEI SISTEMI INFORMATIVI E DI RETE** ▪ **ALL004 - ELENCO RISCHI INDIVIDUATI E RISK OWNER** ▪ *PROCEDURA PER LA SICUREZZA INFORMATICA DELLA CATENA DI APPROVVIGIONAMENTO E RELATIVI ALLEGATI*

				indisponibilità dei servizi; e) i ruoli e le responsabilità del fornitore nel governo dei sistemi informativi e di rete. 2. È verificata periodicamente e documentata la conformità dei fornitori ai requisiti di sicurezza definiti ai sensi della misura GV.SC-01, punto 1, lettera b).	
2. IDENTIFICAZIONE (IDENTIFY)					
			ID.AM	**Gli asset dell'organizzazione (dati, hardware, software, sistemi, strutture, servizi, persone) che consentono all'organizzazione di raggiungere gli obiettivi aziendali sono identificati e gestiti in modo coerente con la loro importanza per gli obiettivi organizzativi e la strategia di gestione del rischio dell'organizzazione.**	
Art. 21 §2(i)	**Art. 24 c.2(i)**		**ID.AM-01**	**Gli inventari degli asset di hardware dell'organizzazione (dispositivi endpoint dell'utente, dispositivi di rete, altri dispositivi fisici) sono mantenuti.** 1. È mantenuto un inventario aggiornato degli apparati fisici (quali server, apparati di rete, dispositivi endpoint) dei sistemi informativi e di rete, che comprende almeno: a) la tipologia di apparato; b) il sistema operativo installato e la relativa versione; c) il riferimento al sistema informativo e di rete di appartenenza.	▪ **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** ▪ **ALLEGATO - MATRICE RACI** ▪ *PROCEDURA CONSEGNA E RESTITUZIONE ASSET* ▪ *PROCEDURA DISMISSIONE DEI SUPPORTI* ▪ *PROCEDURA TRASPORTO SUPPORTI FISICI*

					▪ *PROCEDURA PER LA GESTIONE DELL'INVENTARIO DEI SISTEMI INFORMATIVI DI RETE*
Art. 21 §2(i)	**Art. c.2(i)**	**24**	**ID.AM-02**	**Gli inventari dei software, dei servizi e dei sistemi dell'organizzazione sono mantenuti.**	▪ **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** ▪ **ALLEGATO - MATRICE RACI** ▪ *PROCEDURA PER LA GESTIONE DELL'INVENTARIO DEI SISTEMI INFORMATIVI DI RETE*
				1. È mantenuto un inventario aggiornato dei servizi, dei sistemi e delle applicazioni software dei sistemi informativi e di rete, che comprende almeno: a) la tipologia; b) la versione; c) il riferimento al sistema informativo e di rete di appartenenza.	▪ **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** ▪ **ALLEGATO - MATRICE RACI** ▪ *PROCEDURA PER LA GESTIONE DELL'INVENTARIO DEI SISTEMI INFORMATIVI DI RETE*
Art. 21 §2(i)	**Art. c.2(i)**	**24**	**ID.AM-04**	**Gli inventari dei servizi erogati da fornitori esterni sono mantenuti.**	
				1. È mantenuto un inventario aggiornato dei servizi informatici acquistati da fornitori esterni rilevanti per i sistemi informativi e di rete, che comprende almeno: a) la tipologia di servizio; b) il fornitore del servizio; c) il riferimento al sistema informativo e di rete di appartenenza.	▪ **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** ▪ **ALLEGATO - MATRICE RACI** ▪ *PROCEDURA PER LA SICUREZZA INFORMATICA DELLA CATENA DI APPROVVIGIONAMENTO E RELATIVI ALLEGATI* ▪ *PROCEDURA PER LA GESTIONE DELL'INVENTARIO DEI SISTEMI INFORMATIVI DI RETE*

				ID.RA	**Le minacce informatiche all'organizzazione, i vettori di minaccia, le vulnerabilità e la loro potenziale influenza sono compresi e utilizzati per informare le attività di gestione del rischio.**	
Art. §2(e)	**21**	**Art. c.2(e)**	**24**	**ID.RA-01**	**Le vulnerabilità degli asset sono identificate, validate e registrate.** 1. Le informazioni di cui al punto 1 della misura ID.RA-08 sono utilizzate per individuare le vulnerabilità applicabili ai sistemi informativi e di rete. 2. Per almeno i sistemi informativi e di rete rilevanti, in accordo al piano di gestione delle vulnerabilità di cui al punto 3 della misura ID.RA-08, sono eseguite attività di analisi delle vulnerabilità (vulnerability assessment). 3. Le attività di cui al punto 2 sono documentate tramite appositi report.	▪ **PIANO DI GESTIONE DELLE VULNERABILITÀ** ▪ *PRO004 - PROCEDURA VULNERABILITY ASSESSMENT* ▪ *PRO003 - PROCEDURA PER I CONTATTI CON LE AUTORITÀ ED I GRUPPI SPECIALISTICI*
Art. §2(e)	**21**	**Art. c.2(e)**	**24**	**ID.RA-05**	**Le minacce, le vulnerabilità, le probabilità e gli impatti sono utilizzati per comprendere il rischio inerente e informare le risposte ai rischi.**	▪ **VALUTAZIONE DEL RISCHIO POSTO ALLA SICUREZZA DEI SISTEMI INFORMATIVI E DI RETE** ▪ **PIANO DI GESTIONE DELLE VULNERABILITÀ** ▪ **ALL004 - ELENCO RISCHI INDIVIDUATI E RISK OWNER** ▪ *PRO004 - PROCEDURA VULNERABILITY ASSESSMENT*

				1. In accordo al piano di gestione dei rischi per la sicurezza informatica di cui alla misura GV.RM-03, è definita, documentata ed eseguita una valutazione del rischio per la sicurezza informatica. A tal fine, la valutazione del rischio comprende almeno: a) l'identificazione dei sistemi informativi e di rete e dei relativi asset; b) l'identificazione delle minacce applicabili; c) l'identificazione delle vulnerabilità applicabili; d) la valutazione della probabilità di accadimento delle minacce e del loro impatto sull'organizzazione; e) la determinazione del livello di rischio. 2. La valutazione del rischio di cui al punto 1 è eseguita a intervalli pianificati, comunque almeno annualmente, e in occasione di variazioni significative del contesto organizzativo o di sicurezza informatica. 3. La valutazione del rischio di cui al punto 1 è approvata dagli organi di amministrazione e direttivi.	
Art. 21 §2(a)	**Art. 24 c.2(a)**	**ID.RA-06**	**Le risposte ai rischi sono scelte, prioritizzate, pianificate, monitorate e comunicate.** 1. È definito, documentato, eseguito e monitorato un piano di trattamento dei rischi per la sicurezza informatica, che comprende almeno: a) i rischi da trattare e le relative opzioni di trattamento (riduzione, accettazione, trasferimento o eliminazione del rischio); b) le azioni di trattamento previste	▪ **VALUTAZIONE DEL RISCHIO POSTO ALLA SICUREZZA DEI SISTEMI INFORMATIVI E DI RETE** ▪ **PIANO DI TRATTAMENTO DEL RISCHIO E DI GESTIONE DELLE CRISI** ▪ **ALL004 - ELENCO RISCHI INDIVIDUATI E RISK OWNER**

				con indicazione dei tempi di attuazione e dei responsabili; c) lo stato di attuazione delle azioni di trattamento. 2. Qualora per motivate e documentate ragioni normative o tecniche non sia possibile applicare le misure di sicurezza previste, sono adottate misure di mitigazione compensative e incluse nel Piano di trattamento del rischio e di gestione delle crisi la descrizione delle misure e dell'eventuale rischio residuo. 3. Il piano di cui al punto 1, ivi compresa l'accettazione di eventuali rischi residui, è approvato dagli organi di amministrazione e direttivi.	
Art. 21 §2(e)	**Art. 24 c.2(e)**	**ID.RA-08**	**I processi per ricevere, analizzare e rispondere alle vulnerabilità divulgate dall'organizzazione, dai suoi fornitori e da altre parti interessate sono stabiliti.** 1. Sono monitorati almeno i canali di comunicazione del CSIRT Italia, nonché di eventuali CERT e Information Sharing and Analysis Centre (ISAC) settoriali, al fine di acquisire, analizzare e rispondere alle informazioni sulle vulnerabilità. 2. Le vulnerabilità, ivi comprese quelle identificate ai sensi della misura ID.RA-01, sono tempestivamente risolte mediante aggiornamenti di sicurezza o misure di mitigazione, ove disponibili, oppure mediante	▪ **PIANO DI GESTIONE DELLE VULNERABILITÀ** ▪ *PRO004 - PROCEDURA VULNERABILITY ASSESSMENT* ▪ *PRO003 - PROCEDURA PER I CONTATTI CON LE AUTORITÀ ED I GRUPPI SPECIALISTICI*

				accettazione e documentazione del rischio residuo in accordo al piano di trattamento del rischio di cui alla misura ID.RA-06. 3. È definito, attuato, aggiornato e documentato un piano di gestione delle vulnerabilità che comprende almeno: a) le modalità per l'identificazione delle vulnerabilità di cui alla misura ID.RA-01 e la relativa pianificazione delle attività; b) le modalità per monitorare, ricevere, analizzare e rispondere alle informazioni sulle vulnerabilità; c) le procedure, i ruoli e le responsabilità per lo svolgimento delle attività di cui alle lettere a) e b). 4. Il piano di cui al punto 3 è approvato dagli organi di amministrazione e direttivi. Nota di applicabilità: l'ulteriore requisito relativo al monitoraggio dei canali dei fornitori del software ritenuto critico è previsto dalle specifiche di base per i soggetti essenziali; l'Ateneo può adottarlo come misura ulteriore ove pertinente e proporzionata al rischio.	
			ID.IM	**I miglioramenti alle pratiche di cybersecurity dell'organizzazione sono identificati sulla base di valutazioni continue delle attività di cybersecurity.**	
Art. 21 §2(f)	**Art. 24 c.2(f)**		**ID.IM-01**	**I miglioramenti sono identificati sulla base delle revisioni degli eventi di sicurezza.**	• **PIANO DI ADEGUAMENTO DELLE MISURE DI SICUREZZA** • *PRO028 - PROCEDURA DI AUDITING* • *ALL024 - REPORT AUDIT INTERNO 2026*

					• *PROGRAMMA DI AUDIT E RIESAME DELLA DIREZIONE (evidenze SGSI)*
				1. In accordo agli esiti del riesame di cui al punto 1 della misura GV.PO-02, è definito, approvato dagli organi di amministrazione e direttivi, attuato e monitorato un piano di adeguamento delle misure di sicurezza. Il piano comprende almeno: a) le azioni di adeguamento previste, con indicazione dei tempi di attuazione e dei responsabili; b) lo stato di attuazione delle azioni di adeguamento. 2. Gli organi di amministrazione e direttivi sono informati mediante apposite relazioni sullo stato di attuazione del piano di adeguamento di cui al punto 1.	
Art. 21 §2(c)		**Art. 24 c.2(c)**	**ID.IM-04**	**I piani di risposta agli incidenti e di ripristino sono testati.** 1. Per almeno i sistemi informativi e di rete rilevanti è definito, documentato e attuato un piano di business continuity, contenente almeno: a) i servizi critici da ripristinare in via prioritaria e i relativi obiettivi di ripristino; b) le procedure di ripristino dei servizi critici. 2. Per almeno i sistemi informativi e di rete rilevanti è definito, documentato e attuato un piano di disaster recovery, contenente almeno:	• **PIANO DI TRATTAMENTO DEL RISCHIO E DI GESTIONE DELLE CRISI** • **PIANO DI CONTINUITÀ OPERATIVA E DI RIPRISTINO IN CASO DI DISASTRO** • *ALL009 - BUSINESS IMPACT ANALYSIS* • *PRO029 - PIANO DI BUSINESS CONTINUITY E DISASTER RECOVERY*

	a) le procedure di ripristino dei sistemi informativi e di rete; b) gli obiettivi di ripristino (RTO – Recovery Time Objective e RPO – Recovery Point Objective). 3. Per almeno i sistemi informativi e di rete rilevanti è definito, documentato e attuato un piano di gestione delle crisi, contenente almeno: a) i ruoli e le responsabilità nella gestione delle crisi; b) le modalità di comunicazione interna ed esterna in caso di crisi. 4. I piani di cui ai punti 1, 2 e 3 sono approvati dagli organi di amministrazione e direttivi. 5. I piani di cui ai punti 1, 2 e 3 sono riesaminati e, se opportuno, aggiornati periodicamente e comunque almeno ogni due anni, nonché qualora si verifichino incidenti significativi o mutamenti dell'esposizione alle minacce e ai relativi rischi.	
3. PROTEZIONE (PROTECT)		
PR.AA	**L'accesso agli asset fisici e logici è limitato agli utenti, ai servizi e all'hardware autorizzati, e gestito in misura appropriata alla valutazione del rischio di accesso non autorizzato.**	

Art. 21 §2(i)	**Art. c.2(i)**	**24**	**PR.AA-01**	**Le identità e le credenziali degli utenti, dei servizi e dell'hardware autorizzati sono gestite dall'organizzazione.** 1. Tutte le utenze, ivi incluse quelle con privilegi amministrativi e quelle utilizzate per l'accesso remoto, sono censite, approvate da attori interni al soggetto NIS e, fatte salve motivate e documentate ragioni tecniche, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono individuali per gli utenti. 2. Le credenziali (ad esempio nome utente e password) relative alle utenze sono robuste e aggiornate in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05. 3. Per almeno i sistemi informativi e di rete rilevanti, sono verificate periodicamente le utenze e le relative autorizzazioni, aggiornandole/revocandole in caso di variazioni (ad esempio trasferimento o cessazione di personale).	• **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** • **ALLEGATO - MATRICE RACI** • *PROCEDURA PER LA GESTIONE DELLE UTENZE AMMINISTRATIVE* • *PROCEDURA PER LA GESTIONE DELLE UTENZE FUNZIONALI* • *PROCEDURA ATTIVAZIONE SSO* • *PROCEDURA GESTIONE ACCESSI LOGICI*
Art. 21 §2(l)	**Art. c.2(l)**	**24**	**PR.AA-03**	**Utenti, servizi e hardware sono autenticati.**	▪ **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** ▪ **ALLEGATO - MATRICE RACI** ▪ *PROCEDURA PER LA GESTIONE DELLE UTENZE AMMINISTRATIVE*

					▪ *PROCEDURA PER LA GESTIONE DELLE UTENZE FUNZIONALI* ▪ *PROCEDURA ATTIVAZIONE SSO* ▪ *PROCEDURA GESTIONE ACCESSI LOGICI*
				1. Le modalità di autenticazione delle utenze per accedere ai sistemi informativi e di rete sono commisurate al rischio. A tal fine sono valutati almeno i rischi connessi: a) ai privilegi delle utenze; b) alla criticità dei sistemi informativi e di rete; c) alla tipologia di operazioni che le utenze possono effettuare sui sistemi informativi e di rete. 2. Per almeno i sistemi informativi e di rete rilevanti e in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono impiegate modalità di autenticazione multifattore.	
Art. 21 §2(i)	**Art. 24 c.2(i)**		**PR.AA-05**	**I permessi, i diritti e le autorizzazioni di accesso sono definiti in una politica, gestiti, applicati e rivisti e incorporano i principi del minimo privilegio e della separazione dei compiti.** 1. I permessi sono assegnati alle utenze in accordo ai principi del minimo privilegio e della separazione delle funzioni, tenuto anche conto della necessità di conoscere (need to know).	▪ **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** ▪ **ALLEGATO - MATRICE RACI** ▪ *PROCEDURA PER LA GESTIONE DELLE UTENZE AMMINISTRATIVE* ▪ *PROCEDURA PER LA GESTIONE DELLE UTENZE FUNZIONALI* ▪ *PROCEDURA GESTIONE ACCESSI LOGICI*

				2. È assicurata la completa distinzione tra utenze con e senza privilegi degli amministratori di sistema alle quali devono corrispondere credenziali diverse.	
Art. 21 §2(i)	**Art. 24 c.2(i)**		**PR.AA-06**	**L'accesso fisico agli asset è gestito, monitorato e applicato in misura appropriata al rischio.** 1. Per almeno i sistemi informativi e di rete rilevanti, l'accesso fisico è protetto.	▪ **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** ▪ **ALLEGATO - MATRICE RACI** ▪ *PROCEDURA DI GESTIONE DEGLI ACCESSI FISICI*
			PR.AT	**Il personale dell'organizzazione è sensibilizzato e formato sulla cybersecurity in modo da poter svolgere i propri compiti inerenti alla cybersecurity.**	
Art. 21 §2(g)	**Art. 24 c.2(g)**		**PR.AT-01**	**Il personale è sensibilizzato e formato in modo da possedere le conoscenze e le competenze per svolgere compiti di carattere generale tenendo conto dei rischi di cybersecurity.** 1. È definito, attuato, aggiornato e documentato un piano di formazione in materia di sicurezza informatica del personale, ivi inclusi gli organi di amministrazione e direttivi, che comprende almeno: a) la pianificazione delle attività di formazione previste con l'indicazione dei contenuti della	▪ **PIANO DI FORMAZIONE IN MATERIA DI SICUREZZA INFORMATICA** ▪ **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA (cap. 11)** ▪ *PRO017 - PROCEDURA DI SELEZIONE E FORMAZIONE DEL PERSONALE*

				formazione fornita; b) le eventuali modalità di verifica dell'acquisizione dei contenuti. 2. Il piano di formazione di cui al punto 1 è approvato dagli organi di amministrazione e direttivi. 3. È mantenuto un registro aggiornato recante l'elenco dei dipendenti che hanno ricevuto la formazione di cui al punto 1, i relativi contenuti e l'elenco delle verifiche svolte laddove previste.	
			PR.DS	**I dati sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni.**	
Art. 21 §2(h)		**Art. 24 c.2(h)**	**PR.DS-01**	**La riservatezza, l'integrità e la disponibilità dei dati a riposo (data-at-rest) sono protette.** 1. Per almeno i sistemi informativi e di rete rilevanti, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05 e fatte salve motivate e documentate ragioni normative o tecniche, i dati in essi conservati sono protetti con tecniche di cifratura o con adeguate protezioni fisiche dei supporti.	• **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** • **ALLEGATO - MATRICE RACI** • *PROCEDURA PER LA SICUREZZA DEI DATI* • *LINEE GUIDA SULL'UTILIZZO DI STRUMENTI E SERVIZI INFORMATICI, DI INTERNET E DELLA POSTA ELETTRONICA*

					2. Fatte salve motivate e documentate ragioni normative o tecniche, i dati conservati su dispositivi rimovibili sono protetti con tecniche di cifratura.	
Art. 21 §2(h)		**Art. 24 c.2(h)**	**PR.DS-02**	**La riservatezza, l'integrità e la disponibilità dei dati in transito (data-in-transit) sono protette.**	1. Per almeno i sistemi informativi e di rete rilevanti, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05 e fatte salve motivate e documentate ragioni normative o tecniche, i dati trasmessi attraverso reti pubbliche o non fidate sono protetti con tecniche di cifratura.	• **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** • **ALLEGATO - MATRICE RACI** • *PROCEDURA PER LA SICUREZZA DEI DATI* • *LINEE GUIDA SULL'UTILIZZO DI STRUMENTI E SERVIZI INFORMATICI, DI INTERNET E DELLA POSTA ELETTRONICA*
Art. 21 §2(c)		**Art. 24 c.2(c)**	**PR.DS-11**	**I backup dei dati sono creati, protetti, mantenuti e verificati.**	1. In accordo alle esigenze di continuità operativa e di ripristino in caso di disastro individuate nei piani di cui alla misura ID.IM-04, sono effettuati periodicamente i backup dei dati e delle configurazioni e, per almeno i sistemi informativi e di rete rilevanti, sono anche conservate copie di backup offline.	▪ **PIANO DI CONTINUITÀ OPERATIVA E DI RIPRISTINO IN CASO DI DISASTRO** ▪ *PRO029 - PIANO DI BUSINESS CONTINUITY E DISASTER RECOVERY* ▪ *PROCEDURA PER LA GESTIONE DEI BACKUP/RESTORE*

				2. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.	
			PR.PS	**La tecnologia hardware e software è gestita in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità degli asset.**	
Art. 21 §2(e)		**Art. 24 c.2(e)**	**PR.PS-02**	**Il software è mantenuto in modo da ridurre al minimo i rischi di cybersecurity.** 1. Fatte salve motivate e documentate ragioni normative o tecniche, i sistemi operativi, le applicazioni e i firmware dei sistemi informativi e di rete sono aggiornati con le patch di sicurezza rilasciate dai produttori o da fonti attendibili. 2. Fatte salve motivate e documentate ragioni normative o tecniche, sono rimossi o disattivati i software e i servizi non necessari al funzionamento dei sistemi informativi e di rete. 3. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1 e 2.	▪ **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** ▪ **ALLEGATO - MATRICE RACI** ▪ *PROCEDURA PER IL PATCH MANAGEMENT* ▪ *PROCEDURA PER L'INSTALLAZIONE E DISMISSIONE DI UN SERVER O APPARATO GESTITO*

Art. 21 §2(b)	**Art. 24 c.2(b)**	**PR.PS-04**	**I registri di log sono generati e resi disponibili per il monitoraggio continuo.** 1. Tutti gli accessi eseguiti da remoto e quelli effettuati con utenze con privilegi amministrativi sono registrati. 2. Per almeno i sistemi informativi e di rete rilevanti, sono acquisiti e, in modo sicuro e possibilmente centralizzato, conservati almeno i log necessari ai fini del monitoraggio degli eventi di sicurezza, ivi compresi quelli relativi agli accessi di cui al punto 1. 3. In accordo agli esiti della valutazione rischio di cui alla misura ID.RA-05, sono definite e documentate le tempistiche di conservazione dei log di cui al punto 2. 4. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1 e 2.	▪ **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** ▪ **ALLEGATO - MATRICE RACI** ▪ *PROCEDURA PER LA CONSERVAZIONE DEI LOG* ▪ *PROCEDURA DI MONITORAGGIO, MISURAZIONE, ANALISI E VALUTAZIONE*
Art. 21 §2(e)	**Art. 24 c.2(e)**	**PR.PS-06**	**Le pratiche di sviluppo sicuro del codice sono integrate e le relative performance sono valutate.**	▪ **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** ▪ **ALLEGATO - MATRICE RACI** ▪ *PROCEDURA PER LO SVILUPPO SICURO DEL SOFTWARE*

				1. Sono adottate e documentate pratiche di sviluppo sicuro del codice per i sistemi informativi e di rete sviluppati internamente o su commessa, che comprendono almeno: a) un processo per la gestione dei difetti di sicurezza del codice che include le modalità di segnalazione delle vulnerabilità e di rilascio degli aggiornamenti di sicurezza; b) in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, l'esecuzione di test di sicurezza del codice sviluppato.	
		PR.IR		**Misure di sicurezza per proteggere le reti e l'infrastruttura tecnologica dell'organizzazione sono gestite.**	
Art. 21 §2(i)	**Art. 24 c.2(i)**	**PR.IR-01**		**Le reti e gli ambienti sono protetti dall'accesso logico e dall'uso non autorizzati.** 1. Per almeno i sistemi informativi e di rete rilevanti, sono definite e documentate le eventuali attività consentite da remoto e implementate adeguate misure di sicurezza per l'accesso. 2. È mantenuto un elenco aggiornato dei sistemi informativi e di rete ai quali è possibile accedere da remoto e delle relative modalità di accesso.	▪ **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** ▪ **ALLEGATO - MATRICE RACI** ▪ *PROCEDURA PER LA PROTEZIONE DELLE RETI E DELLE COMUNICAZIONI* ▪ *PROCEDURE DI GESTIONE DEGLI ACCESSI LOGICI E DELLE UTENZE PERTINENTI*

				3. Sono presenti, aggiornati, mantenuti e configurati in modo adeguato strumenti per la protezione perimetrale della rete (quali firewall, sistemi di rilevamento e prevenzione delle intrusioni). 4. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1 e 2.	
4. RILEVAMENTO (DETECT)					
			DE.CM	**Gli asset sono monitorati per individuare anomalie, indicatori di compromissione e altri eventi potenzialmente avversi.**	
Art. 21 §2(b)		**Art. 24 c.2(b)**	**DE.CM-01**	**Le reti e le infrastrutture di rete sono monitorate per individuare potenziali eventi avversi di cybersecurity.** 1. Per almeno i sistemi informativi e di rete rilevanti, sono presenti, aggiornati, mantenuti e configurati in modo adeguato strumenti tecnici per rilevare tempestivamente gli incidenti significativi, quali sistemi di rilevamento delle intrusioni (IDS/IPS).	▪ **PIANO PER LA GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA** ▪ *PROCEDURA DI MONITORAGGIO, MISURAZIONE, ANALISI E VALUTAZIONE* ▪ *PROCEDURA PER LA CONSERVAZIONE DEI LOG*

				2. Sono definiti e documentati i livelli di servizio attesi (SL) dei servizi e delle attività, ai fini del rilevamento di anomalie. 3. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1 e 2.	
Art. 21 §2(b)	**Art. 24 c.2(b)**	**DE.CM-09**	**Il computing hardware e software, i servizi di runtime dell'ambiente operativo sono monitorati per individuare potenziali eventi avversi di cybersecurity.**	1. Fatte salve motivate e documentate ragioni normative o tecniche, sono presenti, aggiornati, mantenuti e configurati in modo adeguato sistemi di protezione dei punti terminali (endpoint) per il rilevamento del codice malevolo. 2. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.	▪ **PIANO PER LA GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA** ▪ *PROCEDURA DI MONITORAGGIO, MISURAZIONE, ANALISI E VALUTAZIONE*
5. RISPOSTA (RESPOND)					
		RS.MA	**Le risposte agli incidenti rilevati sono gestite.**		

Art. 23	**Art. 25**	**RS.MA-01**	**Il piano di risposta agli incidenti è eseguito in coordinamento con le terze parti pertinenti, una volta che un incidente è stato dichiarato.** 1. È definito, attuato, aggiornato e documentato un piano per la gestione degli incidenti di sicurezza informatica, che comprende almeno: a) il processo per la rilevazione, l'analisi, il contenimento, l'eradicazione e il ripristino a seguito di un incidente; b) i ruoli e le responsabilità nella gestione degli incidenti; c) le modalità di comunicazione interna nella gestione degli incidenti; d) le modalità di notifica degli incidenti al CSIRT Italia ai sensi dell'articolo 25 del decreto NIS. 2. Il piano di cui al punto 1 è approvato dagli organi di amministrazione e direttivi. 3. Il piano di cui al punto 1 è riesaminato e, se opportuno, aggiornato periodicamente e comunque almeno ogni due anni, nonché a seguito di incidenti significativi o variazioni organizzative.	▪ **PIANO PER LA GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA** ▪ **PIANO DI TRATTAMENTO DEL RISCHIO E DI GESTIONE DELLE CRISI** ▪ **PIANO DI CONTINUITÀ OPERATIVA E DI RIPRISTINO IN CASO DI DISASTRO** ▪ **MOD_001 - GESTIONE EVENTO - SOGGETTI IMPORTANTI**
		RS.CO	**Le attività di risposta sono coordinate con le parti interne ed esterne.**	

Art. 23	**Art. 25**	**RS.CO-02**	**Gli incidenti vengono segnalati in base ai criteri stabiliti.** 1. In accordo al piano per la gestione degli incidenti di cui alla misura RS.MA-01, sono adottate e documentate procedure per comunicare ai destinatari dei propri servizi gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura dei servizi, le minacce significative cui sono potenzialmente interessati e le relative misure correttive o di mitigazione da adottare. 2. Sono documentate e adottate procedure per informare il pubblico sugli incidenti occorsi, ove necessario.	▪ **PIANO PER LA GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA** ▪ **PIANO DI TRATTAMENTO DEL RISCHIO E DI GESTIONE DELLE CRISI** ▪ **MOD_001 - GESTIONE EVENTO - SOGGETTI IMPORTANTI**
6. RIPRISTINO (RECOVER)				
		RC.RP	**Il ripristino delle attività colpite da un incidente di cybersecurity avviene in modo tempestivo.**	
Art. 21 §2(c)	**Art. 24 c.2(c)**	**RC.RP-01**	**Il piano di ripristino è eseguito durante o dopo un incidente di cybersecurity.**	▪ **PIANO PER LA GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA** ▪ **PIANO DI CONTINUITÀ OPERATIVA E DI RIPRISTINO IN CASO DI DISASTRO**

- **PIANO DI TRATTAMENTO DEL RISCHIO E DI GESTIONE DELLE CRISI**
- *PRO029 - PIANO DI BUSINESS CONTINUITY E DISASTER RECOVERY*

1. Nell'ambito del piano per la gestione degli incidenti di cui alla misura RS.MA-01 e dei piani di business continuity e disaster recovery di cui alla misura ID.IM-04, sono definite le procedure per il ripristino del normale funzionamento dei sistemi informativi e di rete coinvolti da incidenti di sicurezza informatica.

Matrice dei documenti NIS e dei livelli di approvazione

Ai fini dell'attuazione della presente Politica, l'Ateneo distingue tra documenti di indirizzo, governo e pianificazione strategica NIS, approvati dal Consiglio di Amministrazione quale organo competente ai fini dell'art. 23 del D.Lgs. 138/2024, e procedure tecniche o operative, approvate dalla Direttrice/Direttore Generale o dai dirigenti competenti secondo l'assetto organizzativo interno. La seguente matrice individua, per ciascun documento, natura, soggetto predisponente, livello di supervisione, livello di approvazione e periodicità di riesame. Fermo restando l'aggiornamento costante delle procedure, alcune di esse hanno vincoli periodici:

Documento	Natura	Predispone	Supervisiona	Approva	Riesame
Politica per la sicurezza dei sistemi informativi e di rete	Strategica	Direzione IT / DG	Consiglio di Amministrazione	Consiglio di Amministrazione	almeno annuale o in caso di incidenti/rilevanti variazioni dei sistemi informativi di Ateneo

Documento	Natura	Predispone	Supervisiona	Approva	Riesame
Organizzazione per la sicurezza informatica	Strategica	Direzione IT / DG	Consiglio di Amministrazione	Consiglio di Amministrazione	almeno annuale o in caso di incidenti/rilevanti variazioni dei sistemi informativi di Ateneo
Valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete	Strategica	Direzione IT / RSGSI, con Risk Owner e Responsabili SIR secondo perimetro	Consiglio di Amministrazione	Consiglio di Amministrazione	almeno annuale o in caso di incidenti/rilevanti variazioni dei sistemi informativi di Ateneo
Piano di trattamento del rischio e di gestione delle crisi	Strategica	Direzione IT / RSGSI, con Risk Owner e Responsabili SIR secondo perimetro	Consiglio di Amministrazione	Consiglio di Amministrazione	almeno annuale o in caso di incidenti/rilevanti variazioni dei sistemi informativi di Ateneo
Piano di gestione delle vulnerabilità	Strategica/operativa	Direzione IT / RSGSI, con Responsabili SIR e Gestori tecnici secondo perimetro	Consiglio di Amministrazione	Consiglio di Amministrazione	almeno biennale o in caso di incidenti, variazioni organizzative o mutamenti dell’esposizione alle minacce

Documento	Natura	Predispone	Supervisiona	Approva	Riesame
Piano di adeguamento	Strategica e programmatoria	Direzione IT / RSGSI, con i responsabili delle strutture interessate	Consiglio di Amministrazione	Consiglio di Amministrazione	almeno annuale o in caso di incidenti/rilevanti variazioni dei sistemi informativi di Ateneo
Piano di continuità operativa e di ripristino in caso di disastro	Strategica	Direzione IT / Responsabili SIR / Process-Service Owner secondo perimetro	Consiglio di Amministrazione	Consiglio di Amministrazione	almeno annuale o in caso di incidenti significativi o mutamenti dell'esposizione alle minacce e ai relativi rischi
Piano per la gestione degli incidenti di sicurezza informatica	Strategica	Direzione IT, con Responsabili SIR e Gestori tecnici secondo perimetro	Consiglio di Amministrazione	Consiglio di Amministrazione	almeno biennale o a seguito di incidenti significativi o variazioni organizzative
Piano di formazione	Strategica	Direzione IT in raccordo con DG e strutture HR	Consiglio di Amministrazione	Consiglio di Amministrazione	Annuale
Procedure tecniche attuative	Operativa	Strutture competenti	Direzione IT / DG	DG o dirigente competente	secondo procedura

La matrice è aggiornata in occasione di modifiche organizzative, variazioni normative, incidenti significativi o riesami del sistema di gestione della sicurezza informatica.

3 Ruoli e responsabilità

La Direttiva NIS2 e il D.Lgs. 138/2024 attribuiscono agli organi di vertice dei soggetti obbligati un ruolo centrale e non delegabile nella governance della sicurezza informatica. Ai sensi dell'art. 23 del Decreto, gli organi di amministrazione e direttivi sono responsabili dell'approvazione delle misure di gestione dei rischi, della supervisione della loro attuazione e della formazione propria e del personale, al fine di garantire competenze adeguate per individuare i rischi, valutarne la gestione e il loro impatto sulle attività e sui servizi dell'Ateneo.

L'art. 38 stabilisce il regime sanzionatorio per le violazioni degli obblighi di governance, prevedendo sanzioni pecuniarie e accessorie, commisurate alla gravità della violazione, alle misure preventive adottate, alla cooperazione con le Autorità e a eventuali violazioni pregresse.

Ai fini della presente Politica, l'Ateneo distingue tra:

a) organi di amministrazione e direttivi secondo ACN cui competono gli obblighi di approvazione, supervisione e formazione ai sensi dell'art. 23 del D.Lgs. 138/2024, nonché le responsabilità e gli adempimenti informativi previsti dagli artt. 7 e 38 del medesimo decreto;

b) organi di governo e organi istituzionali dell'Ateneo che concorrono, secondo le rispettive competenze statutarie e regolamentari, alla definizione degli indirizzi dell'Ateneo in materia di sicurezza informatica

c) strutture, ruoli e soggetti che collaborano all'attuazione delle misure tecniche, operative e organizzative previste dalla normativa NIS e dalla presente Politica.

Ai fini dell'art. 23 del D.Lgs. 138/2024, gli organi di amministrazione e direttivi dell'Ateneo sono individuati negli organi che, secondo lo Statuto e i regolamenti di Ateneo, esercitano funzioni di indirizzo strategico, approvazione degli atti di programmazione, allocazione delle risorse, supervisione e accettazione del rischio. In tale prospettiva, le funzioni di approvazione e supervisione previste dalla normativa NIS sono esercitate dal **Consiglio di Amministrazione**, presieduto dalla Rettrice, ferma restando la distinzione tra tali funzioni e i ruoli di indirizzo propri del Senato Accademico, e quelli operativi, istruttori e di raccordo svolti dalla Direttrice Generale, dal Delegato rettorale competente, dalla Direzione Informatica e Tecnologie, dal Punto di Contatto NIS e dal Referente CSIRT.

Nello specifico:

Figura	Ruolo

Consiglio di Amministrazione, presieduto dalla Rettrice	Organo collegiale che, nell'ambito delle competenze statutarie e regolamentari, esercita le funzioni di approvazione, indirizzo strategico, allocazione delle risorse, supervisione e accettazione dei rischi residui riservati secondo i criteri e le deleghe vigenti, ai fini dell'art. 23 del D.Lgs. 138/2024. Ha obblighi di approvazione, supervisione e formazione ai sensi dell'art. 23 del D.Lgs. 138/2024, nonché le responsabilità e gli adempimenti informativi previsti dalla normativa NIS applicabile.
Rettrice	Rappresentante legale dell'Ateneo e Presidente degli organi collegiali, assicura il raccordo istituzionale tra indirizzo politico-istituzionale, proposta degli atti e approvazione da parte degli organi competenti.
Senato Accademico	Organo collegiale che concorre, nei limiti delle proprie competenze statutarie e regolamentari, alla definizione degli indirizzi istituzionali dell'Ateneo nelle materie che possono incidere sul profilo di rischio informatico, esprimendo il parere previsto nell'ambito del procedimento interno di approvazione della Politica. Tale ruolo resta distinto dall'individuazione degli organi di amministrazione e direttivi ai fini degli obblighi di cui all'art. 23 del D.Lgs. 138/2024 e delle comunicazioni previste dalla normativa NIS applicabile, salvo diversa ed espressa individuazione.
Direttrice/Direttore Generale	Cura il coordinamento gestionale e amministrativo dell'attuazione degli indirizzi approvati dagli organi competenti e assicura il raccordo con le strutture tecnico-amministrative interessate. In particolare, approva le procedure attuative derivanti dalla Politica e cura l'attuazione degli indirizzi e delle risorse approvati dagli organi competenti
Delegato/a rettorale competente	Svolge funzioni di indirizzo, raccordo e supporto nell'ambito della delega conferita dalla Rettrice, senza che tale ruolo comporti autonoma assunzione delle responsabilità non delegabili attribuite agli organi ex art. 23.
Direttrice/Direttore Direzione IT	Cura l'istruttoria tecnica, il coordinamento operativo, la predisposizione delle proposte

	documentali, il supporto tecnico all'attuazione delle misure di sicurezza NIS e la predisposizione della documentazione strategica e del Piano di Formazione in materia di sicurezza informatica
Punto di Contatto NIS e Referente CSIRT	Curano, secondo le rispettive attribuzioni, l'interlocuzione operativa con ACN/CSIRT e gli adempimenti di piattaforma e notifica, senza che tali funzioni costituiscano delega delle responsabilità ex art. 23.

Con l'approvazione della presente Politica, il Consiglio di Amministrazione, quale organo competente ai fini delle funzioni di cui all'art. 23 del D.Lgs. 138/2024, assume formalmente l'impegno a garantire la supervisione strategica delle misure di sicurezza, l'approvazione dei documenti NIS di alto livello, l'allocazione delle risorse necessarie e il riesame periodico dell'assetto di governance. Le strutture amministrative, tecniche e operative competenti curano l'istruttoria, la proposta, l'attuazione e la rendicontazione delle misure, secondo quanto previsto dalla presente Politica e dalle procedure attuative.L'individuazione degli organi di amministrazione e direttivi ai fini dell'art. 23 del D.Lgs. 138/2024 è coordinata con le informazioni comunicate e aggiornate sulla piattaforma ACN ai sensi dell'art. 7 del medesimo decreto e delle determinazioni ACN applicabili. Prima dell'approvazione definitiva della presente Politica, e successivamente in occasione degli aggiornamenti previsti, l'Ateneo verifica la coerenza tra l'assetto di governance rappresentato nel presente documento e le informazioni risultanti dalla piattaforma ACN

3.1 Supervisione e coordinamento della Sicurezza

Fermo restando il ruolo e la responsabilità degli Organi di Governo, il Dirigente della Direzione IT viene designato quale responsabile del coordinamento per l'adeguamento agli obblighi derivanti dal Decreto NIS.

Il Dirigente ha la responsabilità di garantire la coerenza, l'efficacia nonché la proposta di aggiornamento delle politiche, delle procedure e dei processi rilevanti per il mantenimento della conformità agli obblighi NIS, assicurando che questi siano allineati con le esigenze istituzionali dell'Ateneo.

L'Ateneo deve assicurare l'aggiornamento annuale e continuo delle informazioni relative al soggetto NIS secondo le modalità e i termini previsti dall'art. 7 del D.Lgs. 138/2024 e dalle determinazioni ACN applicabili.

Il Punto di Contatto NIS cura, per gli aspetti operativi, la raccolta, la verifica e la trasmissione delle informazioni richieste sulla piattaforma ACN, avvalendosi delle strutture competenti. Gli organi di amministrazione e direttivi individuati ai fini dell'art. 23 del D.Lgs. 138/2024 sovrintendono al processo di registrazione, comunicazione e aggiornamento delle informazioni, ferma restando la responsabilità operativa dei soggetti incaricati della raccolta e verifica dei dati.

Le variazioni rilevanti relative a organi, punti di contatto, servizi, domini, indirizzi IP, accordi di condivisione, asset o ulteriori informazioni richieste dalla normativa sono comunicate tempestivamente dalle strutture competenti alla Direzione Informatica e Tecnologie, affinché siano valutati gli eventuali aggiornamenti sulla piattaforma ACN.

A seguito dell'approvazione della presente Politica, il Punto di Contatto NIS cura, per gli aspetti operativi e secondo le modalità previste dalle determinazioni ACN applicabili, l'aggiornamento delle informazioni presenti sulla piattaforma ACN, al fine di renderle coerenti con l'assetto di governance NIS definito dall'Ateneo.

3.2 Cultura della sicurezza e consapevolezza

La sicurezza dei sistemi informativi e di rete rappresenta una responsabilità trasversale che interessa l'intera struttura dell'Ateneo.

L'Organizzazione, pertanto, si impegna a definire chiaramente le responsabilità specifiche in materia di sicurezza per tutte le funzioni e le strutture coinvolte, assicurando al contempo l'assenza di sovrapposizioni o lacune operative.

A supporto di questo impegno, l'Ateneo, anche tramite atti organizzativi, promuove una collaborazione strutturata tra la Direzione IT, le altre Direzioni e Aree amministrative, i Dipartimenti e i Centri di ricerca, in modo da garantire un approccio integrato e coerente alla gestione della sicurezza.

Parallelamente, l'Ateneo, nell'ambito delle responsabilità che derivano dalle strutture organizzative, stabilisce meccanismi di coordinamento con soggetti esterni rilevanti, quali fornitori di servizi critici, autorità competenti e il CSIRT nazionale, in conformità con quanto previsto dal Decreto NIS2, e si assicura che le esigenze di sicurezza siano considerate fin dalla fase di progettazione di nuovi servizi, sistemi o processi, applicando il principio di *security by design*.

3.3 Formazione e sensibilizzazione

I membri degli Organi di amministrazione e direttivi (ex art. 23 c.2 D.Lgs. 138/2024) sono tenuti a partecipare a iniziative formative periodiche in materia di sicurezza informatica, finalizzate all'acquisizione e al mantenimento delle conoscenze e competenze necessarie per comprendere i rischi relativi ai sistemi informativi e di rete dell'Ateneo, nonché le pratiche idonee alla loro gestione. Tali iniziative consentono ai membri di esercitare con consapevolezza le proprie responsabilità di indirizzo, approvazione e supervisione in materia di sicurezza, nel rispetto degli obblighi di responsabilità personale previsti dal Decreto NIS2.

L’Ateneo promuove l’offerta periodica di una formazione obbligatoria in materia di sicurezza informatica rivolta a tutto il personale dell'Ateneo che accede ai sistemi informativi e di rete. Il Piano è proposto dal Dirigente della Direzione IT, in raccordo con le strutture competenti in materia di gestione delle risorse umane, ed è strutturato secondo un approccio basato sul rischio.

Il Piano definisce obiettivi, contenuti, modalità di erogazione, frequenza e criteri di verifica dell'efficacia delle iniziative formative. È sottoposto a revisione almeno annuale, ovvero al verificarsi di cambiamenti significativi nel contesto delle minacce, nell'organizzazione o nel quadro normativo di riferimento. I risultati delle attività formative sono documentati e tenuti in considerazione nell'ambito della valutazione complessiva della postura di sicurezza dell'Ateneo.

4 Misure tecniche e organizzative

In conformità con quanto previsto dall'art. 21 della Direttiva (UE) 2022/2555 e dal relativo Decreto Legislativo di recepimento, l'Ateneo si impegna ad adottare misure tecniche e organizzative adeguate e proporzionate, volte a gestire i rischi per la sicurezza dei sistemi informativi e di rete e a prevenire o ridurre al minimo l'impatto di eventuali incidenti sui destinatari dei servizi erogati e sui servizi interconnessi.

La tabella seguente illustra la mappatura tra gli ambiti di intervento previsti, i relativi requisiti ACN e la documentazione di Ateneo. Per ciascun ambito sono richiamati anzitutto i documenti NIS di governo o pianificazione sottoposti all'approvazione del Consiglio di Amministrazione e, successivamente, le procedure e le evidenze attuative del SGSI ISO/IEC 27001. I due livelli sono complementari: i documenti NIS definiscono governo, responsabilità, criteri e piani; le procedure SGSI ne disciplinano o comprovano l'attuazione operativa nel perimetro applicabile. Nella colonna «Documenti NIS primari / Procedure ed evidenze attuative UNIVR», il **neretto** identifica i documenti del framework NIS, inclusi i piani e gli allegati sottoposti all'approvazione del Consiglio di Amministrazione; il *corsivo* identifica le procedure, i registri, le linee guida e le evidenze attuative del SGSI ISO/IEC 27001. L'ordine delle voci segue la medesima gerarchia: prima NIS, quindi SGSI/ISO.

Ambiti	**Requisiti ACN**	Documenti NIS primari / Procedure ed evidenze attuative UNIVR
a) Gestione del rischio	GV.PO-02: punto 1. GV.RM-03: punto 1. ID.RA-05: punti 1, 2 e 3. ID.RA-06: punti 1, 2 e 3.	• **VALUTAZIONE DEL RISCHIO POSTO ALLA SICUREZZA DEI SISTEMI INFORMATIVI E DI RETE** • **PIANO DI TRATTAMENTO DEL RISCHIO E DI GESTIONE DELLE CRISI** • **ALL004 - ELENCO RISCHI INDIVIDUATI E RISK OWNER**
b) Ruoli e responsabilità	GV.RR-02: punti 1, 2, 3 e 4.	• **POLITICA PER LA SICUREZZA DEI SISTEMI INFORMATIVI E DI RETE** • **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** • **ALLEGATO - MATRICE RACI** • **REGISTRO CONTROLLATO DEI RUOLI NIS E ATTI DI ATTRIBUZIONE**
c) Affidabilità delle risorse umane	GV.RR-04: punti 1 e 2.	• **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA (cap. 12)** • *PRO017 - PROCEDURA DI SELEZIONE E FORMAZIONE DEL PERSONALE* • *PROCEDURA PER LA GESTIONE DELLA ATTIVAZIONE, VARIAZIONE E CESSAZIONE DEL RAPPORTO DI LAVORO*
d) Conformità e audit di sicurezza	GV.PO-01: punti 1, 2 e 3. GV.PO-02: punti 1 e 2.	• **PIANO DI ADEGUAMENTO DELLE MISURE DI SICUREZZA**

	ID.IM-01: punti 1 e 2.	• *PRO028 - PROCEDURA DI AUDITING* • *ALL024 - REPORT AUDIT INTERNO 2026* • *PROGRAMMA DI AUDIT E RIESAME DELLA DIREZIONE (evidenze SGSI)*
e) Gestione dei rischi per la sicurezza informatica della catena di approvvigionamento	GV.SC-01: punto 1. GV.SC-02: punto 1. GV.SC-04: punto 1. GV.SC-05: punto 1. GV.SC-07: punti 1 e 2.	• **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** • **ALLEGATO - MATRICE RACI** • *PROCEDURA PER LA SICUREZZA INFORMATICA DELLA CATENA DI APPROVVIGIONAMENTO E RELATIVI ALLEGATI*
f) Gestione degli asset	ID.AM-01: punto 1. ID.AM-02: punto 1. ID.AM-04: punto 1.	• **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** • **ALLEGATO - MATRICE RACI** • *PROCEDURA PER LA GESTIONE DELL'INVENTARIO DEI SISTEMI INFORMATIVI DI RETE* • *PROCEDURA CONSEGNA E RESTITUZIONE ASSET* • *PROCEDURA DISMISSIONE DEI SUPPORTI* • *PROCEDURA TRASPORTO SUPPORTI FISICI*
g) Gestione delle vulnerabilità	ID.RA-01: punto 1. ID.RA-08: punti 1, 2, 3 e 4.	• **PIANO DI GESTIONE DELLE VULNERABILITÀ** • *PRO004 - PROCEDURA VULNERABILITY ASSESSMENT* • *PRO003 - PROCEDURA PER I CONTATTI CON LE AUTORITÀ ED I GRUPPI SPECIALISTICI*
h) Continuità operativa, ripristino in caso di disastro e gestione delle crisi informatiche	ID.IM-04: punti 1, 2, 3, 4 e 5.	• **PIANO DI TRATTAMENTO DEL RISCHIO E DI GESTIONE DELLE CRISI** • **PIANO DI CONTINUITÀ OPERATIVA E DI RIPRISTINO IN CASO DI DISASTRO** • *ALL009 - BUSINESS IMPACT ANALYSIS* • *PRO029 - PIANO DI BUSINESS CONTINUITY E DISASTER RECOVERY*
i) Gestione dell'autenticazione, delle identità digitali e del controllo accessi	PR.AA-01: punti 1, 2 e 3. PR.AA-03: punti 1 e 2. PR.AA-05: punti 1 e 2. PR.IR-01: punti 1 e 2.	• **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** • **ALLEGATO - MATRICE RACI** • *PROCEDURA PER LA GESTIONE DELLE UTENZE AMMINISTRATIVE* • *PROCEDURA PER LA GESTIONE DELLE UTENZE FUNZIONALI* • *PROCEDURA ATTIVAZIONE SSO* • *PROCEDURA GESTIONE ACCESSI LOGICI* • *ULTERIORI PROCEDURE APPLICATIVE IAM DEL SGSI*
j) Sicurezza fisica	PR.AA-06: punto 1.	• **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** • **ALLEGATO - MATRICE RACI** • *PROCEDURA DI GESTIONE DEGLI ACCESSI FISICI*

k) Formazione del personale e consapevolezza	PR.AT-01: punti 1, 2 e 3.	• **PIANO DI FORMAZIONE IN MATERIA DI SICUREZZA INFORMATICA** • **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA (cap. 11)** • *PRO017 - PROCEDURA DI SELEZIONE E FORMAZIONE DEL PERSONALE*
l) Sicurezza dei dati	PR.DS-01: punti 1 e 2. PR.DS-02: punto 1. PR.DS-11: punto 1.	• **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** • **ALLEGATO - MATRICE RACI** • *PROCEDURA PER LA SICUREZZA DEI DATI* • *PROCEDURA PER LA GESTIONE DEI BACKUP/RESTORE* • *LINEE GUIDA E REGOLAMENTI DI ATENEO PERTINENTI*
m) Sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete	PR.PS-02: punti 1 e 2. PR.PS-04: punti 1, 2 e 3. PR.PS-06: punto 1.	• **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** • **ALLEGATO - MATRICE RACI** • *PROCEDURA PER LO SVILUPPO SICURO DEL SOFTWARE* • *PROCEDURA INSTALLAZIONE E DISMISSIONE SERVER E APPARATI* • *PROCEDURA PER IL PATCH MANAGEMENT* • *PROCEDURA PER LA CONSERVAZIONE DEI LOG*
n) Protezione delle reti e delle comunicazioni	PR.IR-01: punto 3.	• **ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA** • **ALLEGATO - MATRICE RACI** • *PROCEDURA PER LA PROTEZIONE DELLE RETI E DELLE COMUNICAZIONI*
o) Monitoraggio degli eventi di sicurezza	DE.CM-01: punti 1 e 2. DE.CM-09: punto 1.	• **PIANO PER LA GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA** • *PROCEDURA DI MONITORAGGIO, MISURAZIONE, ANALISI E VALUTAZIONE* • *PROCEDURA PER LA CONSERVAZIONE DEI LOG*
p) Gestione degli incidenti, ivi inclusi la risposta e ripristino	RS.MA-01: punti 1, 2 e 3. RS.CO-02: punti 1 e 2. RC.RP-01: punto 1.	• **PIANO PER LA GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA** • **PIANO DI TRATTAMENTO DEL RISCHIO E DI GESTIONE DELLE CRISI** • **PIANO DI CONTINUITÀ OPERATIVA E DI RIPRISTINO IN CASO DI DISASTRO** • **MOD_001 - GESTIONE EVENTO - SOGGETTI IMPORTANTI**

4.1.1 Gestione del rischio

L'Ateneo adotta un processo strutturato di gestione del rischio per la sicurezza informatica, esteso all'intera organizzazione. Il processo include l'identificazione dei sistemi informativi e di rete rilevanti, la valutazione delle minacce e delle vulnerabilità applicabili, la determinazione del livello di rischio e la definizione di un Piano di trattamento del rischio e di gestione delle crisi predisposto dalla Direzione Informatica e Tecnologie con il coinvolgimento delle strutture competenti e sottoposto all'approvazione del Consiglio di Amministrazione. La valutazione del rischio è riesaminata almeno annualmente e comunque in occasione di cambiamenti significativi nell'organizzazione, nelle infrastrutture tecnologiche, nel contesto normativo o nel panorama delle minacce.

Il processo di valutazione del rischio segue la metodologia consolidata del Framework della ISO/IEC 27005. Viene considerato un panorama di minacce rilevanti, la verosimiglianza di accadimento degli eventi avversi e la gravità del loro potenziale impatto sulla riservatezza, integrità e disponibilità delle informazioni dell'Ateneo.

Sulla base dell'analisi del contesto di Ateneo è definito un Piano di trattamento del rischio e di gestione delle crisi che include le misure di sicurezza tecniche e organizzative necessarie a mitigare le vulnerabilità che permetterebbero alla minaccia di concretizzarsi, al fine di ridurre il livello di rischio. L'Ateneo si propone di garantire un equilibrio efficace tra il livello di protezione assicurato e la sostenibilità organizzativa ed economica degli interventi, privilegiando quelli con maggiore efficacia nella riduzione del rischio residuo.

4.1.2 Gestione dei ruoli e delle responsabilità

L'Ateneo definisce e formalizza l'organizzazione per la sicurezza informatica, stabilendo con chiarezza ruoli, responsabilità e poteri a tutti i livelli istituzionali. L'organizzazione include il Punto di Contatto NIS e il suo sostituto, il Referente CSIRT e gli eventuali sostituti, il Dirigente della Direzione IT, il RSGSI e gli ulteriori ruoli previsti dal modello organizzativo. Per i singoli SIR, inclusi quelli gestiti al di fuori del perimetro della Direzione IT, sono individuati, ove applicabile, il Responsabile del SIR (SIR Owner) e il Gestore tecnico del SIR. I ruoli sono riesaminati almeno annualmente e comunque in occasione di incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.

Il documento "Organizzazione per la sicurezza informatica" costituisce la fonte autoritativa per ruoli, responsabilità e criteri di attribuzione; la relativa Matrice RACI applica tali criteri alle singole attività. Gli atti di attribuzione e il registro nominativo dei ruoli NIS identificano le persone che ricoprono le funzioni previste, senza sovrapporre la funzione organizzativa alla persona fisica che la esercita.

La valutazione del rischio per la sicurezza informatica e il Piano di trattamento del rischio e di gestione delle crisi sono predisposti dalla Direzione Informatica e Tecnologie e dal RSGSI, con il coinvolgimento delle strutture competenti, dei Responsabili SIR e dei Risk Owner individuati secondo il rispettivo perimetro, e sono sottoposti all'approvazione del Consiglio di Amministrazione. Le decisioni sui singoli rischi residui sono assunte secondo le deleghe e i criteri di escalation definiti nella valutazione e nel

Piano di trattamento; sono riservati al Consiglio di Amministrazione il rischio residuo effettivo di classe "Molto alto" (12–16) e i casi fuori delega, di deroga sostanziale o di rilevanza strategica o finanziaria.

4.1.3 Affidabilità delle risorse umane

L'Ateneo adotta misure volte a garantire che il personale autorizzato ad accedere ai sistemi informativi e di rete rilevanti, nonché gli amministratori di sistema, siano individuati previa valutazione dell'esperienza e delle capacità. Sono definiti i profili di competenza per i ruoli individuati, comprensivi di requisiti specifici relativi alla sicurezza delle informazioni e alla cybersecurity, calibrati anche in funzione della tipologia, della sensibilità e del volume delle informazioni gestite da ciascuna mansione.

Viene approvato un piano di formazione specifico per la sicurezza delle informazioni che definisce le modalità di definizione dei requisiti di formazione, i principi e le indicazioni sulle modalità di programmazione, i destinatari e le tempistiche previste per l'erogazione.

4.1.4 Conformità e audit di sicurezza

L'Ateneo, nell'ambito delle responsabilità che derivano dalle strutture organizzative, programma un riesame annuale della propria conformità agli obblighi NIS2 e alle politiche di sicurezza informatica adottate.

L'attività di verifica è affidata a un soggetto terzo indipendente che elabora un rapporto di audit.

La/il Dirigente della Direzione Informatica e Tecnologie presenta gli esiti al Consiglio di Amministrazione, che ne valuta i contenuti e delibera sulle azioni correttive da intraprendere, traducendole in un piano di adeguamento con responsabili e tempi di attuazione definiti.

4.1.5 Gestione dei rischi per la sicurezza informatica della catena di approvvigionamento

La gestione del rischio nella catena di approvvigionamento richiede che anche gli aspetti di sicurezza informatica siano presi in considerazione sin dalle fasi iniziali dei processi di acquisto, in coerenza con quanto richiesto dalla direttiva NIS2 e dal D.Lgs. 138/2024.

L'Ateneo adotta linee guida in materia di sicurezza della catena di approvvigionamento, applicabili a tutte le strutture, in conformità ai requisiti della Direttiva NIS2 e del D.Lgs. 138/2024.

Gli acquisti di forniture che possono avere un impatto sulla sicurezza dei sistemi informativi e di rete rilevanti avvengono ordinariamente attraverso piattaforme di mercato elettronico qualificato — MEPA, CONSIP, UBUY — ovvero mediante dati e servizi erogati da consorzi istituzionali come CINECA e GARR. Il ricorso a piattaforme qualificate e a fornitori istituzionali costituisce criterio preferenziale e fattore di mitigazione del rischio, ma non determina una presunzione automatica di conformità. Resta ferma la necessità di valutare la rilevanza NIS della specifica fornitura, il livello di accesso del fornitore

ai sistemi, i dati trattati, la dipendenza operativa, gli impatti sulla continuità dei servizi e l'eventuale necessità di requisiti contrattuali di sicurezza proporzionati al rischio.

Le forniture con potenziale impatto sui sistemi informativi e di rete rilevanti sono sottoposte a valutazione del rischio secondo le procedure definite dalla Direzione Informatica e Tecnologie, con il coinvolgimento delle strutture richiedenti e dei referenti tecnici competenti.

Qualora un docente o una struttura decentrata intenda selezionare un fornitore appartenente alla categoria di cui sopra al di fuori di tali canali, è tenuto a motivare documentalmente la scelta. I Tecnici Informatici presenti nei dipartimenti e gli altri referenti tecnici competenti supportano la valutazione del rischio informatico e formulano il relativo parere tecnico; la decisione e l'eventuale approvazione restano attribuite al Responsabile del SIR o alla struttura competente secondo il perimetro, le deleghe e le procedure di Ateneo.

Le strutture decentrate che gestiscono autonomamente processi di acquisto sono in ogni caso tenute ad applicare i criteri di valutazione del rischio fornitore, i requisiti contrattuali minimi e le procedure di verifica della conformità definiti dalla Direzione IT.

4.1.6 Procedura per la gestione degli asset

La corretta gestione del rischio e delle vulnerabilità, come richiesto dalla normativa e indicato nella presente Politica, presuppone una conoscenza puntuale e aggiornata di tutti gli asset hardware e software in uso presso l'Ateneo.

A tal fine, l'Ateneo ritiene necessario, laddove tecnicamente possibile e di norma, procedere all'installazione di agenti software su tutti i dispositivi di proprietà dell'Ateneo, al fine di garantire una mappatura completa, aggiornata e centralizzata degli asset, condizione indispensabile per qualsiasi attività successiva di valutazione del rischio e gestione delle vulnerabilità.

Nel caso non sia installato l'agente sul dispositivo, è comunque necessario mantenere aggiornate le caratteristiche del sistema che integra la mappatura di cui sopra. La responsabilità del mantenimento di dette informazioni è del proprietario dell'asset e/o dell'affidatario preposto alla gestione dello stesso.

Fermi restando, per i sistemi informativi e di rete rilevanti, i termini cogenti stabiliti dalla normativa e dalle determinazioni ACN applicabili, e senza che il presente termine possa differirli, entro dodici mesi dall'approvazione della presente Politica gli asset non mappati nell'inventario generale saranno considerati dispositivi non riconosciuti e inseriti in un profilo di rete analogo a quello offerto agli utenti ospiti dell'Ateneo, salvo deroghe motivate e governate secondo la valutazione del rischio.

Nei casi in cui l'installazione dell'agente software non sia tecnicamente possibile o risulti incompatibile con specifiche esigenze relative al funzionamento del dispositivo, la struttura interessata richiede una deroga motivata alla Direzione Informatica e Tecnologie. La deroga è accompagnata da una valutazione del rischio, dall'indicazione delle misure compensative applicabili e da un termine di riesame periodico. Gli asset oggetto di deroga sono comunque censiti nell'inventario, classificati in base al rischio e soggetti a misure alternative di monitoraggio, segregazione o limitazione, ove necessarie.

L'eventuale collocazione in profili di rete limitati è disposta secondo criteri proporzionati al rischio, tenendo conto della criticità dell'asset, della sua funzione istituzionale, dell'esposizione a minacce e delle misure compensative effettivamente adottate.

4.1.7 Gestione delle vulnerabilità

L'Ateneo estende il perimetro delle attività di gestione delle vulnerabilità già in essere per la Direzione Informatica e Tecnologie ai sistemi rilevanti NIS dell'intera organizzazione.

Le attività comprendono il monitoraggio sistematico dei canali di comunicazione del CSIRT Italia e degli eventuali CERT e Information Sharing and Analysis Centre (ISAC) settoriali, nonché, quali ulteriori fonti pertinenti, CERT-AgID, CVCN, fonti OSINT e canali dei produttori. Le vulnerabilità sono analizzate e gestite tempestivamente mediante aggiornamenti o misure di mitigazione ove disponibili oppure, quando il rimedio non sia applicabile, mediante valutazione e accettazione documentata del rischio residuo secondo il Piano di trattamento del rischio. Il Piano di gestione delle vulnerabilità definisce modalità di identificazione e pianificazione, monitoraggio/ricezione/analisi/risposta, nonché procedure, ruoli e responsabilità, con evidenze delle attività svolte.

4.1.8 Procedura per la continuità operativa, il ripristino in caso di disastro e la gestione delle crisi informatiche

L'Ateneo, nell'ambito delle responsabilità che derivano dalle strutture organizzative, estende il perimetro dell'analisi di impatto (Business Impact Analysis) e dei piani di Business Continuity e Disaster Recovery ai sistemi rilevanti NIS, inclusi quelli eventualmente al di fuori della Direzione Informatica e Tecnologie.

I piani definiscono gli obiettivi di ripristino (RTO e RPO), le procedure di ripristino dei servizi critici e le priorità di intervento. La procedura di gestione delle crisi informatiche è estesa e adeguata ai sistemi rilevanti NIS.

4.1.9 Procedura per la gestione dell'autenticazione, delle identità digitali e del controllo degli accessi

La Direzione IT definisce, con adeguato preavviso, un piano di transizione finalizzato alla progressiva razionalizzazione dei privilegi di amministratore locale sui dispositivi assegnati. In tale ambito, l'Ateneo adotta un approccio differenziato, coerente con la specificità dei ruoli:

Personale docente, ricercatori, dottorandi, cultori della materia, assegnisti di ricerca – in ragione delle attività di ricerca e didattica che possono richiedere autonomia nella scelta degli strumenti – possono mantenere, ove necessario e secondo le procedure e la valutazione del rischio applicabili, i privilegi di amministratore locale sul dispositivo assegnato, distinguendo l'utenza per l'uso ordinario (non privilegiata) da quella per le attività amministrative. La Direzione Informatica e Tecnologie può richiedere informazioni sul software installato, indicare misure di mitigazione, limitarne l'utilizzo o disporne la rimozione qualora emergano vulnerabilità, incompatibilità o rischi non accettabili per i sistemi informativi e di rete dell'Ateneo.

- Personale tecnico-amministrativo, CEL e studenti utilizzano dispositivi privi di privilegi di amministratore di sistema. L'accesso con diritti amministrativi, oltre che al personale della Direzione IT, è consentito esclusivamente in via eccezionale, a fronte di comprovate esigenze lavorative, previa formale richiesta e autorizzazione della Direzione IT. Eventuali concessioni hanno carattere strettamente personale, sono limitate nel tempo e soggette a revisione periodica. Qualsiasi uso improprio o non autorizzato dei privilegi amministrativi costituisce violazione della presente Politica e comporta responsabilità personali a carico dell'utente.

Il controllo degli accessi e l'autenticazione forte sono individuati tra le misure tecniche prioritarie per garantire un'adeguata sicurezza dei sistemi informatici dell'Ateneo. L'Ateneo ha già consolidato il sistema GIA (Gestione delle Identità e degli Accessi) come unico centro di autenticazione federata per tutti i software e i servizi istituzionali, consentendo di monitorare con precisione gli accessi, revocare tempestivamente le autorizzazioni in caso di cessazione del rapporto o di incidente di sicurezza e applicare in maniera uniforme politiche di autenticazione forte.

L'accesso ai sistemi istituzionali tramite credenziali diverse da GIA non è previsto, di norma, in favore di un'infrastruttura uniforme e centralizzata per la gestione delle identità digitali.

4.1.10 Procedura per la sicurezza fisica

L'Ateneo estende e integra le misure di protezione fisica degli spazi, delle infrastrutture e delle apparecchiature che ospitano o supportano i sistemi informativi e di rete per ricomprendere esplicitamente i sistemi rilevanti NIS, inclusi quelli collocati al di fuori dei locali della Direzione Informatica e Tecnologie.

L'accesso fisico ai sistemi rilevanti è protetto e monitorato, in coerenza con quanto previsto dalla valutazione del rischio.

4.1.11 Procedura per la formazione del personale e la consapevolezza

L'Ateneo promuove una cultura della sicurezza informatica diffusa attraverso un programma strutturato di formazione obbligatoria rivolto a tutto il personale che accede ai sistemi informativi e di rete, inclusi gli organi di amministrazione e direttivi, in conformità con quanto previsto dall'art. 23 del Decreto NIS2. Il Piano di Formazione in materia di sicurezza informatica, predisposto annualmente dalla Direzione Informatica e Tecnologie in raccordo con le strutture competenti per la gestione delle risorse umane, è sottoposto all'approvazione del Consiglio di Amministrazione. Il Piano include specifici percorsi formativi per i componenti del Consiglio di Amministrazione, compresi i componenti di nuova nomina e la componente studentesca, al fine di assicurare la piena consapevolezza delle responsabilità di indirizzo, approvazione e supervisione previste dalla normativa NIS. La/Il Direttrice/Direttore Generale attua il Piano per quanto di competenza.

4.1.12 Procedura per la sicurezza dei dati

L'Ateneo adotta misure tecniche e organizzative per proteggere i dati trattati, garantendone riservatezza, integrità e disponibilità nel rispetto della normativa applicabile. Per i sistemi rilevanti NIS, i dati conservati sono protetti con tecniche di cifratura o con adeguate protezioni fisiche; i dati trasmessi su reti pubbliche o non fidate sono protetti con tecniche di cifratura. Le disposizioni in materia di sicurezza delle comunicazioni sono recepite e integrate nella documentazione operativa di riferimento.

4.1.13 Procedura per lo sviluppo, la configurazione, la manutenzione e la dismissione dei sistemi informativi e di rete

L'Ateneo, per l'implementazione dei propri servizi, utilizza software valutati e ritenuti sicuri dalla Direzione IT, messi a disposizione dell'intera comunità accademica.

L'utilizzo di software non previamente analizzato dalla Direzione IT per esigenze di ricerca o didattica è disciplinato dalle procedure interne e avviene secondo criteri proporzionati al rischio, ferma restando la responsabilità dell'Ateneo quale soggetto NIS per la governance complessiva del rischio e gli obblighi operativi di collaborazione, diligenza, segnalazione e aggiornamento in capo al richiedente o utilizzatore. Linee guida e informazioni su come gestire questa casistica sono illustrate nel piano formativo che coinvolge il personale di ateneo.

L'Ateneo assicura che l'intero ciclo di vita dei sistemi informativi e di rete sia gestito secondo principi di security by design e by default, dalla progettazione fino alla dismissione. Sono definite linee guida per le configurazioni di riferimento (baseline) dei sistemi rilevanti NIS. I sistemi operativi, le applicazioni e i firmware sono aggiornati con le patch di sicurezza; i software e i servizi non necessari sono rimossi o disattivati. Per i sistemi sviluppati internamente o su commessa sono adottate pratiche di sviluppo sicuro del codice.

4.1.14 Procedura per la protezione delle reti e delle comunicazioni

L'Ateneo protegge la propria infrastruttura di rete attraverso strumenti di sicurezza perimetrale e interna (firewall, IDS/IPS) presenti, aggiornati e configurati in modo adeguato. Le attività consentite da remoto

sono definite e documentate; è mantenuto un elenco aggiornato dei sistemi accessibili da remoto e delle relative modalità di accesso autorizzate. L'inventario dei flussi di rete interni, comprensivo dei flussi autorizzati tra i sistemi NIS e l'esterno, costituisce riferimento per il controllo degli accessi di rete.

4.1.15 Procedura per il monitoraggio degli eventi di sicurezza

L'Ateneo garantisce la rilevazione tempestiva di eventi anomali tramite strumenti tecnici per il rilevamento delle intrusioni (IDS/IPS) e sistemi di protezione degli endpoint, presenti, aggiornati e configurati in modo adeguato. I log degli accessi da remoto e di quelli effettuati con utenze privilegiate sono registrati e conservati in modo sicuro e centralizzato. Sono definiti e documentati i livelli di servizio attesi (SL) dei servizi e delle attività, ai fini del rilevamento di anomalie e della qualificazione degli incidenti significativi.

4.1.16 Procedura per la risposta agli incidenti e il ripristino

L'Ateneo definisce, attua e mantiene aggiornato un piano strutturato per la gestione degli incidenti di sicurezza informatica, sviluppato in conformità con il modello di processo articolato nelle fasi di preparazione, rilevamento, risposta, ripristino e miglioramento continuo.

Le procedure adottate comprendono le fasi di gestione e notifica degli incidenti, con l'indicazione dei relativi ruoli e responsabilità; le procedure per la predisposizione e la trasmissione delle relazioni a CSIRT Italia; le informazioni di contatto per la segnalazione; le modalità di comunicazione interna, incluso il tempestivo coinvolgimento della Rettrice, della Direttrice/Direttore Generale, del Punto di Contatto NIS, del Referente CSIRT, della Direzione Informatica e Tecnologie e, nei casi di maggiore rilevanza strategica o istituzionale, del Consiglio di Amministrazione quale organo competente ai fini dell'art. 23 del D.Lgs. 138/2024. Il processo di notifica al CSIRT Italia, ai sensi dell'art. 25 del D.Lgs. 138/2024, è affidato al Referente CSIRT designato e ai suoi sostituti.

A supporto della risposta e del ripristino, l'Ateneo predispone una Business Impact Analysis (BIA) estesa ai sistemi rilevanti NIS, che consente di identificare i servizi critici, stimare l'impatto di una loro interruzione e definire le priorità di ripristino con i relativi obiettivi di RTO e RPO.

Sulla base degli esiti della BIA è elaborato e mantenuto aggiornato un Piano di Disaster Recovery, che disciplina le procedure tecniche e organizzative per il ripristino dei sistemi informativi e di rete compromessi.

5 Revisione della politica e miglioramento continuo

L'Ateneo si impegna a sottoporre la presente Politica a revisione formale almeno con cadenza annuale, tenendo conto degli aggiornamenti della valutazione del rischio, delle modifiche normative, delle raccomandazioni dell'ACN o dell'ENISA, delle buone pratiche di settore, dei risultati degli audit e degli incidenti occorsi. Gli aggiornamenti sono approvati conformemente a quanto finora descritto e comunicati a tutti i soggetti interessati.

6 Comunicazione, diffusione e riconoscimento

L'Ateneo si impegna a pubblicare la presente Politica nella intranet istituzionale, a inserire il richiamo alla Politica nei nuovi contratti di lavoro e nei contratti con i fornitori rilevanti.

La Politica non deve necessariamente essere distribuita nella sua interezza: a seconda del ruolo, può essere comunicato un estratto contenente le sole informazioni pertinenti, senza divulgare informazioni confidenziali.

7 Entrata in vigore

La presente Politica entra in vigore dalla data della sua approvazione e sostituisce ogni precedente documento avente analoga finalità.

8 Riferimenti normativi e di indirizzo

La presente Politica è redatta in conformità al seguente quadro normativo e di indirizzo, che ne costituisce il fondamento giuridico e metodologico:

Normativa europea

- Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (c.d. "Direttiva NIS2"), e in particolare l'art. 21, par. 2, lett. a);

- Regolamento di esecuzione (UE) 2024/2690 della Commissione, del 17 ottobre 2024, recante requisiti tecnici e metodologici per specifiche categorie di soggetti individuate dalla Direttiva NIS2; assunto dalla presente Politica quale riferimento tecnico-metodologico ove pertinente, ferma restando la verifica della sua diretta applicabilità al caso concreto;

Normativa nazionale di recepimento

- Decreto Legislativo 4 settembre 2024, n. 138, recante il recepimento della Direttiva (UE) 2022/2555 nell'ordinamento italiano, e in particolare gli artt. 23 (*Obblighi degli organi di amministrazione e direttivi*), 24 (*Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica*), 25–26 (*Obblighi in materia di notifica di incidente*);

Atti delle Autorità competenti

- Determinazione del Direttore Generale dell'ACN n. 379907 del 19 dicembre 2025, recante le specifiche di base per l'adempimento agli obblighi di cui agli artt. 23, 24, 25, 29 e 32 del D.Lgs. 138/2024 e, per l'Ateneo quale soggetto importante, il relativo Allegato 1 sulle misure di sicurezza di base;

- Determinazione del Direttore Generale dell'ACN n. 127437 del 13 aprile 2026, adottata ai sensi dell'art. 7, comma 6, del D.Lgs. 138/2024, relativa alla piattaforma digitale, all'aggiornamento delle informazioni, al Punto di contatto e agli ulteriori adempimenti previsti dal provvedimento;

- Determinazione del Direttore Generale dell'ACN n. 155238 del 20 aprile 2026, adottata ai sensi dell'art. 30, comma 2, del D.Lgs. 138/2024, recante le categorie di rilevanza nonché il processo, le modalità e i criteri per l'elencazione, la caratterizzazione e la categorizzazione delle attività e dei servizi del soggetto NIS;

  Linee guida ACN, dicembre 2025, per la definizione del processo di gestione degli incidenti di sicurezza informatica, contenenti indicazioni non vincolanti per l'attuazione delle misure di sicurezza di base;

Linee guida e standard di riferimento

- ENISA, Technical Implementation Guidance on Cybersecurity Risk Management Measures, versione 1.0, giugno 2025, con particolare riferimento al Capitolo I (Policy on the security of network and information systems);
- ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements;
- NIST Cybersecurity Framework (CSF) 2.0, quale ulteriore riferimento metodologico per l'approccio basato sulle funzioni Govern, Identify, Protect, Detect, Respond, Recover.