Organizzazione per la sicurezza informatica

Autore: DIREZIONE IT

Tipo Documento: Aziendale

Versione	Data	Descrizione
1.0	28 – 06 – 2026	Creazione documento
2.0	30 – 08 – 2026	Riorganizzazione complessiva del modello di ruoli e responsabilità NIS2
2.1	30 – 08 – 2026	Integrazione requisiti GV.RR-02, ambiti ACN e presidi applicabili
2.2	30 – 08 – 2026	Incorporazione delle discipline su persone, formazione e ciclo di vita dei rapporti e degli accessi
2.3	30 – 08 – 2026	Allineamento alle Determinazioni ACN 379907/2025 e 127437/2026; disciplina operativa di Punto di contatto, Referente CSIRT e sostituti
2.4	30 – 08 – 2026	Uniformazione della denominazione della Politica per la sicurezza dei sistemi informativi e di rete

Il documento definisce il modello organizzativo con cui l'Ateneo governa la sicurezza dei sistemi informativi e di rete, raccordando gli obblighi NIS2 con il SGSI ISO 27001 della Direzione IT.

EXECUTIVE SUMMARY

Il contesto. La NIS2 non considera la cybersicurezza una responsabilità esclusivamente tecnica. Il D.lgs. 138/2024 e le specifiche di base ACN richiedono che l'organizzazione stabilisca ruoli, responsabilità e poteri, che gli organi di amministrazione e direttivi approvino l'assetto e ne sorveglino l'attuazione. Questo documento traduce tali obblighi nella realtà dell'Università degli Studi di Verona, evitando che la responsabilità complessiva venga confusa con la sola gestione operativa della Direzione IT.

Il punto di partenza dell'Ateneo. L'Università non parte da zero. La Direzione IT dispone di un Sistema di Gestione per la Sicurezza delle Informazioni certificato ISO/IEC 27001 e governa, secondo la ricognizione attuale, circa il 95–98% dei sistemi informativi e di rete rilevanti. Il perimetro NIS assunto alla data di emissione coincide pertanto con quello del SGSI. Tale coincidenza costituisce una solida base organizzativa e documentale, ma non è considerata definitiva: la ricognizione continua può individuare SIR gestiti da altre strutture dell'Ateneo, per i quali devono essere formalizzati un Responsabile del SIR e un Gestore tecnico.

La funzione del documento. Il documento non sostituisce la Matrice RACI, le procedure tecniche o gli atti di nomina. Esso definisce il modello organizzativo comune: distingue l'indirizzo e la supervisione del Consiglio di Amministrazione, l'interlocuzione istituzionale con ACN e CSIRT Italia, il coordinamento del Dirigente IT e del RSGSI, la responsabilità sui singoli SIR e l'esecuzione tecnica. La RACI applica poi questi criteri alle singole attività; gli atti e il registro nominativo identificano le persone che ricoprono i ruoli.

Il governo dei diversi ambiti di sicurezza. Le misure ACN interessano l'intera organizzazione: rischio, risorse umane, audit, fornitori, asset, vulnerabilità, continuità, identità, sicurezza fisica, formazione, dati, ciclo di vita dei sistemi, reti, monitoraggio e incidenti. Il documento assegna tali ambiti secondo competenza e perimetro. Strumenti quali SIEM, SOC, MFA, PAM, VPN, firewall o penetration test sono indicati come possibili presidi applicativi: non costituiscono automaticamente obblighi tecnologici autonomi e si applicano secondo la valutazione del rischio e le caratteristiche dei SIR effettivamente presenti.

Le persone e il ciclo degli accessi. Il modello comprende direttamente anche: affidabilità e adeguatezza delle persone, formazione e consapevolezza, attivazione e variazione dei rapporti, attribuzione e revisione degli accessi, cessazione e restituzione degli asset. Tali regole sono ricondotte all'intero perimetro NIS dell'Ateneo e collegate ai ruoli e ai SIR descritti nel presente documento.

Implicazioni per il Consiglio di Amministrazione. L'approvazione non attribuisce al Consiglio la gestione operativa dei sistemi o degli incidenti. Il Consiglio esercita indirizzo e supervisione: riceve informazioni comprensibili sui rischi e sull'efficacia delle misure, verifica che responsabilità e risorse siano adeguate, decide sulle questioni che eccedono l'autorità delle funzioni operative e richiede il riesame dell'assetto quando il contesto cambia.

Decisioni richieste al Consiglio di Amministrazione

Ai fini dell'adozione del modello, al Consiglio è richiesto di:

- approvare il modello organizzativo descritto nel presente documento;
- prendere atto della Matrice RACI e della regola di attribuzione applicabile ai SIR centrali e ai SIR esterni al perimetro ISO;
- dare mandato alle strutture competenti di formalizzare i titolari dei ruoli e mantenere il relativo elenco nominativo;
- approvare le regole comuni su affidabilità, competenze, formazione e ciclo di vita dei rapporti e degli accessi;
- richiedere reporting periodico e riesame almeno annuale dell'assetto organizzativo.

1 SCOPO E NECESSITÀ DEL DOCUMENTO

Il presente documento definisce l'organizzazione adottata dall'Ateneo per governare la sicurezza informatica e per attribuire in modo chiaro, coerente e verificabile ruoli e responsabilità relativi ai sistemi informativi e di rete. Esso risponde alla necessità di rendere comprensibile chi esercita indirizzo e supervisione, chi coordina gli adempimenti NIS2, chi governa i singoli SIR, chi esegue le attività tecniche e chi effettua verifiche e controlli.

Le Determinazioni ACN vigenti individuano gli ambiti, i risultati di sicurezza e le modalità di interlocuzione che l'organizzazione deve presidiare; non assegnano automaticamente tali compiti a una specifica struttura dell'Ateneo. L'attribuzione organizzativa è effettuata dall'Università tenendo conto del proprio contesto, del modello ISO 27001 esistente, della titolarità dei servizi e della concreta capacità di decisione e intervento. Ai fini del presente modello si assumono, in particolare, la Determinazione ACN n. 379907 del 19 dicembre 2025 e la Determinazione ACN n. 127437 del 13 aprile 2026, nelle rispettive versioni vigenti.

> **Principio di lettura:** Il presente documento descrive il modello e i criteri di attribuzione. La Matrice RACI allegata assegna puntualmente, per ciascuna attività, i ruoli Responsible, Accountable, Consulted e Informed. I due documenti sono complementari e non duplicativi.

1.1 Risultati attesi

L'assetto organizzativo deve assicurare che:

- ogni ambito di sicurezza abbia responsabilità riconoscibili e formalizzate;
- per ciascuna attività e perimetro sia individuato un solo Accountable;
- le attività tecniche siano distinte dalle attività di controllo e supervisione;
- i rischi, gli incidenti e gli scostamenti siano comunicati al livello decisionale appropriato;
- l'attribuzione delle responsabilità segua l'evoluzione del perimetro dei SIR;
- le evidenze prodotte dal SGSI ISO 27001 siano riutilizzate anche ai fini NIS2.

1.2 Adempimenti assicurati ai sensi della misura GV.RR-02

La misura GV.RR-02 non richiede un semplice organigramma, ma un assetto effettivamente approvato, conosciuto e mantenuto. Il presente documento costituisce l'atto di riferimento per il primo requisito; la conformità complessiva è completata dagli atti di attribuzione, dal registro nominativo, dalla comunicazione interna e dalle evidenze di riesame.

Requisito ACN	Attuazione nell'Ateneo	Evidenza principale
Organizzazione definita, approvata e resa nota	Il CdA approva il modello; RSGSI e strutture competenti ne curano la diffusione ai destinatari	Documento approvato, comunicazioni e pubblicazione interna
Elenco aggiornato delle persone con ruoli specifici	RSGSI mantiene il registro nominativo con il supporto di Risorse Umane e delle strutture titolari	Registro dei ruoli NIS e atti di attribuzione
Punto di contatto e almeno un sostituto	I soggetti sono inclusi nel modello e individuati con apposito atto	Nomine e registrazioni sulla piattaforma ACN
Riesame periodico e al verificarsi di eventi rilevanti	Il riesame è svolto almeno annualmente e dopo incidenti, variazioni organizzative o mutamenti del rischio	Verbali, Riesame della Direzione e aggiornamenti documentali

2 CAMPO DI APPLICAZIONE E PERIMETRO

Il documento si applica agli organi di amministrazione e direzione, al personale dell'Università, ai responsabili e gestori dei SIR, alle strutture di supporto e controllo e ai soggetti esterni che partecipano alla gestione o alla sicurezza dei sistemi e dei servizi dell'Ateneo.

Definizione di SIR. Ai fini del presente documento, un sistema informativo e di rete è l'insieme organizzato di applicazioni, infrastrutture, reti, dispositivi, dati, flussi, servizi cloud o esternalizzati, persone e procedure utilizzato per erogare o supportare un servizio dell'Ateneo. Un SIR non coincide necessariamente con un singolo software o apparato: può comprendere più componenti e dipendenze, interne ed esterne, il cui funzionamento concorre alla disponibilità, autenticità, integrità o riservatezza del servizio.

Alla data di emissione, il perimetro NIS assunto dall'Ateneo coincide con il perimetro del SGSI ISO 27001 della Direzione IT. Tale perimetro comprende, secondo la ricognizione disponibile, circa il 95–98% dei sistemi rilevanti di Ateneo. La Direzione IT costituisce quindi il principale presidio tecnico e organizzativo, ma la coincidenza corrente non è considerata definitiva.

L'Ateneo mantiene una ricognizione continua dei SIR. Quando viene individuato un sistema rilevante gestito al di fuori del perimetro ISO, sono formalmente identificati almeno il Responsabile del SIR e il Gestore tecnico; il sistema viene quindi sottoposto alla valutazione del rischio e ricondotto ai processi di trattamento, adeguamento, monitoraggio e gestione degli incidenti.

> **Conseguenza organizzativa:** Il Dirigente IT risponde dei SIR e dei servizi centrali governati dalla Direzione IT. Per i SIR esterni al perimetro ISO, la responsabilità sul sistema è attribuita al relativo Responsabile del SIR, secondo la RACI.

3 QUADRO DI RIFERIMENTO E SISTEMA DOCUMENTALE

Il modello è definito in coerenza con:

- Direttiva (UE) 2022/2555 (NIS2);
- D.lgs. 4 settembre 2024, n. 138;
- Determinazione ACN n. 379907 del 19 dicembre 2025, applicabile dal 15 gennaio 2026, e relativi allegati tecnici;
- Determinazione ACN n. 127437 del 13 aprile 2026, per le modalità di accesso al Portale ACN e la designazione/operatività dei soggetti incaricati delle interlocuzioni NIS;
- Sistema di Gestione per la Sicurezza delle Informazioni ISO 27001 della Direzione IT;
- atti organizzativi, deleghe, nomine e procedure interne dell'Ateneo.

3.1 Relazione con gli altri documenti

Documento	Funzione nel sistema	Rapporto con l'organizzazione
Politica per la sicurezza dei sistemi informativi e di rete	Definisce principi, indirizzi e impegni	È approvata e supervisionata dagli organi competenti
Valutazione del rischio e ALL004	Identifica e valuta gli scenari di rischio	Associa rischi, Risk Owner, controllori e misure
Piano di trattamento del rischio e di gestione delle crisi	Governa trattamento, responsabilità ed escalation	Utilizza ruoli e flussi definiti nel presente documento
Piano di adeguamento	Coordina azioni derivanti da audit, riesami e scostamenti	Attribuisce owner, tempi, risorse ed evidenze
Matrice RACI	Assegna R, A, C e I alle attività	Costituisce l'allegato operativo del presente documento
Audit e Riesame della Direzione	Verificano adeguatezza ed efficacia	Producono rilievi, decisioni e azioni di miglioramento

4 PRINCIPI DI ATTRIBUZIONE DELLE RESPONSABILITÀ

Responsabilità degli organi di vertice. L'approvazione, l'indirizzo e la supervisione non sono trasferiti alle funzioni tecniche o ai fornitori.

Un solo Accountable. Per ciascuna attività e perimetro deve essere individuato un unico soggetto che risponde del risultato.

Separazione dei compiti. Chi realizza o modifica un controllo non deve essere l'unico soggetto che ne verifica efficacia e conformità.

Autorità coerente con la responsabilità. Un ruolo può essere Accountable solo se dispone di autorità, informazioni e possibilità di escalation adeguate.

Responsabilità interna non trasferibile. L'affidamento a un fornitore può trasferire attività operative, non la responsabilità dell'Ateneo.

Approccio per perimetro. Le attribuzioni cambiano a seconda che il SIR sia governato dalla Direzione IT o da un'altra struttura.

Tracciabilità. Nomine, decisioni, accettazioni, verifiche ed escalation devono essere documentate.

4.1 Significato degli indicatori RACI

Indicatore	Significato	Regola
R – Responsible	Esegue o coordina l'esecuzione operativa	Possono essere presenti più R se le attività sono ripartite
A – Accountable	Risponde del risultato e assume la decisione	Uno solo per attività e perimetro
C – Consulted	Fornisce contributi prima della decisione o dell'esecuzione	Il confronto deve essere effettivo e tempestivo
I – Informed	Riceve comunicazione di decisioni, avanzamento o esiti	Non partecipa necessariamente alla decisione operativa

4.2 Regola per SIR centrali e SIR esterni

Perimetro	Responsible	Accountable	Consulted/Informed
SIR e servizi centrali governati dalla Direzione IT	Direzione IT o area tecnica competente	Dirigente IT, salvo attribuzioni specifiche	RSGSI, Process Owner, DPO e altre funzioni pertinenti
SIR gestiti al di fuori del perimetro ISO	Gestore tecnico del SIR	Responsabile del SIR formalmente individuato	Direzione IT, RSGSI e responsabile della struttura titolare
Controlli centralizzati applicati a SIR esterni	Direzione IT per il controllo centrale; Gestore del SIR per le attività locali	Responsabile del SIR per il proprio sistema	RSGSI e funzioni specialistiche

5 MODELLO ORGANIZZATIVO PER LA SICUREZZA INFORMATICA

Il modello è articolato in livelli complementari. Ogni livello svolge una funzione diversa e nessun ruolo di interlocuzione o esecuzione tecnica assorbe le responsabilità degli altri livelli.

Livello	Soggetti principali	Funzione
1. Indirizzo e supervisione	CdA e organi di amministrazione e direzione	Approvano, indirizzano, assicurano risorse e verificano l'attuazione
2. Interlocuzione istituzionale	Punto di contatto, sostituto, Referente CSIRT	Curano rapporti e adempimenti verso ACN e CSIRT Italia
3. Governo centrale della sicurezza	Dirigente IT, Direzione IT, RSGSI	Coordinano SGSI, controlli centrali, rischio, reporting e miglioramento
4. Governo dei singoli SIR	Responsabile del SIR, Gestore tecnico, Process/Service Owner	Governano rischi, misure, funzionamento e continuità del sistema
5. Supporto, controllo ed esecuzione	DPO, HR, DTGAL, AdS, audit, fornitori	Forniscono competenze, eseguono attività e verificano i controlli

6 RUOLI ISTITUZIONALI E DI GOVERNO

I ruoli descritti in questo capitolo non costituiscono una catena gerarchica tecnica. Essi svolgono funzioni differenti: il Consiglio esercita indirizzo e supervisione; il Punto di contatto e il Referente CSIRT assicurano le interlocuzioni istituzionali; il Dirigente IT, la Direzione IT e il RSGSI rendono operativo e verificabile il sistema di governo. La presenza di un ruolo non sostituisce gli altri e ogni attribuzione deve essere letta insieme ai limiti indicati.

6.1 Consiglio di Amministrazione e organi di amministrazione e direzione

Esercitano indirizzo e supervisione sulla gestione dei rischi di cybersicurezza secondo le rispettive competenze istituzionali.

Responsabilità principali

- approvano politiche, modello organizzativo e principali indirizzi di sicurezza;
- esaminano periodicamente rischi, KPI, incidenti, scostamenti e stato dei piani;
- valutano risorse e decisioni che eccedono l'autorità delle funzioni operative;
- partecipano alla formazione prevista e verificano il riesame dell'assetto.

Limiti e raccordi

- non gestiscono operativamente sistemi o incidenti;
- la delega di attività tecniche non elimina la responsabilità di supervisione.

Evidenze e collegamenti: report periodici, verbali, delibere, Riesame della Direzione, Piano di adeguamento.

6.2 Punto di contatto e sostituto

Sono i riferimenti istituzionali dell'Ateneo per le interlocuzioni e gli adempimenti attribuiti nei confronti di ACN.

Responsabilità principali

- curano le comunicazioni e gli aggiornamenti richiesti tramite i canali previsti;
- assicurano il raccordo tra ACN, organi di vertice e funzioni interne;
- coordinano la disponibilità delle informazioni necessarie agli adempimenti;
- garantiscono continuità del ruolo attraverso il sostituto designato.

Limiti e raccordi

- non sostituiscono il CdA nella supervisione;
- non assumono automaticamente la gestione tecnica dei SIR o degli incidenti; in via eccezionale, quando il Referente CSIRT e tutti i suoi sostituti risultano indisponibili, il Punto di contatto può effettuare le notifiche previste dagli articoli 25 e 26 del D.lgs. 138/2024 nei casi e secondo le modalità stabilite dalla Determinazione ACN n. 127437/2026.

Evidenze e collegamenti: atto di designazione, registrazioni sulla piattaforma ACN, comunicazioni ufficiali.

6.3 Referente CSIRT e sostituti

Il Referente CSIRT e i sostituti designati assicurano l'interlocuzione operativa con CSIRT Italia e presidiano le notifiche degli incidenti secondo le modalità e i tempi applicabili. L'operatività del ruolo è assicurata secondo l'ordine e le condizioni risultanti dagli atti di designazione e dalle registrazioni sul Portale ACN.

Responsabilità principali

- raccolgono e consolidano le informazioni sull'incidente;
- curano alert, notifica e relazione finale, con il supporto delle funzioni coinvolte;
- mantengono il raccordo con il Punto di contatto e il team di risposta;
- assicurano continuità operativa tramite i sostituti.

Limiti e raccordi

- non coincidono necessariamente con chi contiene o risolve tecnicamente l'incidente;
- non decidono autonomamente comunicazioni istituzionali o accettazioni di rischio fuori dalla propria autorità.

Evidenze e collegamenti: atti di designazione e registro nominativo controllato; Portale ACN; registro incidenti; notifiche; Piano di crisi. I documenti di governo indicano i ruoli, mentre nominativi e recapiti restano nel registro controllato.

	Organizzazione per la sicurezza informatica	Ver. 2.4 del 30/08/2026
		Autore: DIT Approvato da: CDA Tipo Documento: Aziendale

6.4 Dirigente IT

È il principale responsabile organizzativo dei SIR e dei servizi centrali governati dalla Direzione IT e assicura il raccordo tra governo tecnico, SGSI e organi di vertice.

Responsabilità principali

- assicura l'attuazione delle politiche e delle misure nel perimetro di competenza;
- approva o propone priorità, interventi e fabbisogni di risorse;
- riceve il reporting da RSGSI, aree tecniche e responsabili interessati;
- effettua l'escalation di rischi, incidenti e scostamenti rilevanti;
- risponde dei controlli centrali e dei SIR assegnati secondo la RACI.

Limiti e raccordi

- non è automaticamente Accountable per SIR gestiti autonomamente da altre strutture;
- non assume le funzioni proprie del CdA, del Punto di contatto, del Referente CSIRT o del DPO.

Evidenze e collegamenti: Matrice RACI, SGSI ISO 27001, reporting, piani e Riesame della Direzione.

6.5 Direzione IT

È il presidio tecnico e organizzativo centrale dell'Ateneo e gestisce la quasi totalità dei SIR rilevanti attualmente censiti.

Responsabilità principali

- gestisce infrastrutture, reti, identità, servizi e controlli centralizzati;
- attua misure tecniche e organizzative nel proprio perimetro;
- supporta ricognizione dei SIR, valutazione dei rischi e gestione degli incidenti;
- fornisce supporto e raccordo ai Responsabili di SIR esterni;
- mantiene le evidenze tecniche e documentali di competenza.

Limiti e raccordi

- per i SIR esterni svolge supporto e coordinamento senza sostituirsi al relativo Responsabile o Gestore;
- le responsabilità affidate a fornitori restano presidiate da una funzione interna.

Evidenze e collegamenti: procedure ISO 27001, inventari, ALL004, registri tecnici, audit e piani.

6.6 RSGSI

Presidia il Sistema di Gestione per la Sicurezza delle Informazioni e assicura coerenza metodologica, documentale e di miglioramento continuo.

Responsabilità principali

- coordina aggiornamento della documentazione del SGSI e del sistema NIS2;
- supporta valutazione dei rischi, monitoraggio delle misure e definizione degli obiettivi;
- raccoglie evidenze, rilievi, non conformità e azioni di miglioramento;
- supporta audit e Riesame della Direzione;
- segnala scostamenti ed esigenze di aggiornamento al Dirigente IT.

Limiti e raccordi

- non sostituisce i Risk Owner, i Responsabili dei SIR o i gestori tecnici;
- il controllo metodologico deve restare distinguibile dall'esecuzione tecnica.

Evidenze e collegamenti: SGSI, audit, ALL004, Piano di adeguamento, Riesame della Direzione.

7 RUOLI RELATIVI AI SIR E FUNZIONI DI SUPPORTO

Quando si passa dal governo generale al singolo sistema, la responsabilità deve seguire il SIR e non soltanto l'organigramma della Direzione IT. Per i sistemi centrali l'assetto consolidato della DIT continua a operare; per un SIR esterno al perimetro ISO occorre invece individuare formalmente chi ne assicura il governo, chi lo gestisce tecnicamente e chi rappresenta le esigenze del processo o del servizio.

7.1 Responsabile del SIR (SIR Owner)

È il soggetto formalmente individuato che assicura il governo di un SIR, in particolare quando il sistema è gestito al di fuori del perimetro ISO della Direzione IT.

Responsabilità principali

- mantiene identificazione, finalità, dipendenze e criticità del SIR;
- coordina valutazione dei rischi e attuazione delle misure;
- verifica l'operato del Gestore tecnico e dei fornitori;
- assicura segnalazione tempestiva di incidenti, vulnerabilità e cambiamenti;
- propone risorse, priorità, trattamenti ed eventuali escalation;
- rende disponibili evidenze e informazioni per audit, reporting e riesami.

Limiti e raccordi

- non deve essere un referente meramente nominale; deve disporre di informazioni, autorità ed accesso ai canali di escalation;
- non può accettare rischi o assumere impegni economici oltre la propria competenza.

Evidenze e collegamenti: atto di individuazione, inventario SIR, ALL004, piani di trattamento e adeguamento.

7.2 Gestore tecnico del SIR

È il soggetto interno o esterno che esegue le attività tecniche sul SIR sotto il coordinamento del Responsabile del SIR.

Responsabilità principali

- configura, mantiene, aggiorna e monitora il sistema;
- attua backup, logging, protezione degli accessi e misure tecniche assegnate;
- gestisce vulnerabilità, patch e interventi di ripristino;
- conserva le evidenze tecniche e segnala tempestivamente anomalie e incidenti;
- collabora con Direzione IT, RSGSI e team di risposta agli incidenti.

Limiti e raccordi

- è normalmente Responsible e non Accountable;
- l'esecuzione affidata a un fornitore resta soggetta a controllo interno.

7.3 Responsabile della struttura titolare

Rappresenta la struttura cui afferisce il servizio o il SIR, senza assumere automaticamente la responsabilità tecnica o organizzativa del sistema.

Responsabilità principali

- è consultato per priorità, risorse, continuità e impatti sui servizi;
- è informato su rischi, incidenti, scostamenti ed esiti significativi;
- supporta le decisioni e le escalation che richiedono l'intervento della struttura.

Limiti e raccordi

- diventa Accountable soltanto quando un atto formale o la natura della decisione gli attribuiscono tale responsabilità.

7.4 Process Owner o Service Owner

Rappresenta le esigenze del processo o servizio supportato dal SIR e ne esprime impatti e priorità.

Responsabilità principali

- definisce requisiti di disponibilità, integrità, riservatezza e continuità;
- partecipa a BIA, RTO/RPO ed esercitazioni;
- valuta gli effetti organizzativi di interruzioni e cambiamenti.

Limiti e raccordi

- non coincide necessariamente con il Responsabile o il Gestore tecnico del SIR.

7.5 FUNZIONI SPECIALISTICHE E DI SUPPORTO

Funzione	Contributo principale	Limite/raccordo
DPO	Consulenza e sorveglianza in materia di protezione dei dati personali	Non assume la gestione tecnica dei SIR
Direzione Risorse Umane	Formazione, ciclo del rapporto di lavoro e registrazioni	Opera con DIT e responsabili dei ruoli
DTGAL	Sicurezza fisica, impianti e infrastrutture tecniche di competenza	Coordina fornitori e continuità delle infrastrutture
Amministratori di Sistema	Eseguono attività privilegiate formalmente assegnate	Sono nominati, formati, monitorati e verificati
Audit/controllori	Verificano conformità ed efficacia dei controlli	Devono mantenere adeguata indipendenza
Fornitori	Eseguono attività contrattualmente affidate	Non assorbono la responsabilità dell'Ateneo

8 AMBITI DI RESPONSABILITÀ DERIVANTI DALLE MISURE ACN

Le specifiche di base ACN richiedono che l'Ateneo governi un insieme coordinato di ambiti organizzativi e tecnici. L'elenco seguente riproduce separatamente i sedici ambiti indicati dalla misura relativa alle politiche di sicurezza, senza accorpare gestione del rischio, ruoli, risorse umane e audit nella sola nozione generale di governance. In questo modo il Consiglio di Amministrazione può verificare che nessuna area resti priva di un presidio riconoscibile.

Per ogni ambito la tabella indica il criterio di attribuzione delle responsabilità e, in una colonna subordinata, i principali presidi che possono concorrere all'attuazione. La colonna dei presidi non introduce automaticamente nuovi obblighi tecnologici: la concreta applicabilità dipende dalla valutazione del rischio, dal perimetro del SIR, dalle architetture effettivamente presenti e dalle specifiche ACN applicabili al soggetto.

> **Regola di attribuzione:** Per i servizi e i controlli centrali il governo fa capo alla Direzione IT secondo la RACI. Per un SIR gestito fuori dal perimetro ISO, la responsabilità organizzativa ricade sul Responsabile del SIR e l'esecuzione sul relativo Gestore tecnico; DIT e RSGSI assicurano raccordo, standard comuni e supporto.

8.1 Governo, persone, fornitori e conoscenza del perimetro

Ambito ACN	Responsabilità e raccordi	Principali presidi applicabili	Evidenze
1. Gestione del rischio	CdA: approvazione e supervisione. Dirigente IT o Responsabile SIR: governo nel rispettivo perimetro. RSGSI e Risk Owner: metodo, analisi e monitoraggio.	Metodologia di rischio, BIA ove necessaria, ALL004, valutazione, trattamento, accettazione e riesame.	Valutazione del rischio, ALL004, piani e verbali di approvazione
2. Ruoli e responsabilità	CdA: approva il modello. Dirigente IT e RSGSI: coordinano. Ciascun titolare esercita il ruolo formalmente attribuito.	Organigramma, RACI, atti di nomina, sostituzioni, registro nominativo e canali di escalation.	Documento organizzativo, RACI, nomine e registro dei ruoli NIS
3. Affidabilità delle risorse umane	Risorse Umane governa il ciclo del rapporto; responsabili organizzativi e dei SIR definiscono requisiti, segnalano variazioni e verificano l'adeguatezza.	Verifiche consentite dalla legge, riservatezza, onboarding, variazione, offboarding e revoca tempestiva degli accessi.	Capitoli 11 e 12, atti, registrazioni e revoche
4. Conformità e audit	Organi di vertice supervisionano. RSGSI pianifica e consolida; auditor e funzioni di controllo verificano con adeguata indipendenza; DPO è consultato per la protezione dati.	Programma di audit, verifiche di conformità, non conformità, azioni correttive e Riesame della Direzione.	Piani e rapporti di audit, rilievi, azioni e riesami
5. Catena di approvvigionamento	Titolare del contratto e struttura di acquisto governano la fornitura; DIT o Responsabile SIR definisce e verifica i requisiti di sicurezza applicabili.	Valutazione del fornitore, clausole, SLA, obblighi di notifica, controllo dei subfornitori, continuità ed exit strategy.	Valutazioni, contratti, SLA, verifiche e piani di uscita
6. Gestione degli asset	DIT per asset e servizi centrali; Responsabile e Gestore tecnico per SIR esterni. Process Owner contribuisce a finalità, criticità e dipendenze.	Inventari hardware, software, dati, flussi, cloud, fornitori, configurazioni e relazioni tra asset e servizi.	Inventari, registri, schemi e censimento SIR
7. Gestione delle vulnerabilità	Dirigente IT o Responsabile SIR governa priorità ed eccezioni; Gestore tecnico esegue analisi e remediation; RSGSI monitora gli scostamenti.	Vulnerability assessment, patch management, remediation, penetration test proporzionati al rischio e gestione delle eccezioni.	Report tecnici, ticket, piani di remediation ed eccezioni approvate
8. Continuità, disaster recovery e crisi	Process/Service Owner definisce esigenze di continuità; Dirigente IT o Responsabile SIR governa il ripristino; il Piano di crisi disciplina comando e comunicazioni.	BIA, RTO/RPO, backup e prove di restore, DR, alternative operative, esercitazioni e gestione della crisi.	Piani, test, verbali di esercitazione e azioni di miglioramento

8.2 Protezione, esercizio, rilevazione e risposta

Gli ambiti successivi riguardano soprattutto la protezione e l'esercizio dei SIR. Anche in questi casi l'esecuzione tecnica può essere centralizzata, locale o affidata a un fornitore, ma deve sempre restare riconducibile a un responsabile interno e produrre evidenze verificabili.

Ambito ACN	Responsabilità e raccordi	Principali presidi applicabili	Evidenze
9. Autenticazione, identità e accessi	DIT governa le identità centrali; per SIR esterni rispondono Responsabile e Gestore tecnico. Risorse Umane e responsabili di struttura attivano tempestivamente le variazioni.	IAM, MFA ove richiesta o appropriata, PAM, utenze nominative, revisioni periodiche, segregazione dei privilegi e accessi remoti protetti.	Richieste, autorizzazioni, revisioni, log e revoche
10. Sicurezza fisica	DTGAL governa sedi e impianti di competenza; DIT presidia datacenter e apparati; responsabili locali segnalano esigenze e anomalie.	Controllo degli accessi, registri, videosorveglianza ove prevista, UPS, climatizzazione, antincendio e protezione dei locali tecnici.	Registri, manutenzioni, test e rapporti di intervento
11. Formazione e consapevolezza	Risorse Umane e DIT pianificano; responsabili dei ruoli segnalano fabbisogni e verificano la partecipazione; gli organi di vertice seguono la formazione prevista.	Piano formativo, moduli per ruolo, awareness, comunicazioni periodiche e simulazioni di phishing proporzionate al rischio.	Capitolo 11, piano, registri, verifiche ed esiti delle campagne
12. Sicurezza dei dati	Responsabile SIR e Process Owner definiscono esigenze; DIT o Gestore tecnico attua i controlli; DPO è consultato quando sono coinvolti dati personali.	Classificazione, minimizzazione, cifratura, certificati, integrità, conservazione, cancellazione sicura e prevenzione delle perdite.	Regole, configurazioni, registri, test e autorizzazioni
13. Ciclo di vita dei SIR	DIT per sistemi centrali; Responsabile SIR per sistemi esterni; Gestore tecnico e fornitori eseguono secondo requisiti approvati.	Security by design, sviluppo sicuro, configurazioni di base, change management, manutenzione, aggiornamento e dismissione controllata.	Requisiti, collaudi, change, configurazioni e verbali di dismissione
14. Reti e comunicazioni	DIT governa le reti centrali; Responsabile SIR governa eventuali reti locali di propria competenza; DTGAL cura gli aspetti infrastrutturali fisici assegnati.	Segmentazione, apparati di rete, firewall, Wi-Fi, VPN, protezione dei protocolli, ridondanza, cablaggio e armadi ove pertinenti.	Schemi, configurazioni, regole, backup e registri di modifica
15. Monitoraggio degli eventi	DIT o Gestore tecnico assicura raccolta e analisi; RSGSI e funzioni di sicurezza ricevono il reporting; il Referente CSIRT è coinvolto quando emerge un incidente notificabile.	Logging, sincronizzazione temporale, SIEM o SOC ove adottati, protezione endpoint, rilevazione anomalie e threat intelligence pertinente.	Log, alert, dashboard, rapporti ed evidenze di presa in carico
16. Risposta agli incidenti e ripristino	Team di risposta, DIT e Gestori contengono e ripristinano; Responsabile SIR/Dirigente IT coordinano; Referente CSIRT cura le notifiche; vertici supervisionano e decidono sulla crisi.	Piano e playbook di risposta, reperibilità, triage, contenimento, eradicazione, comunicazioni, notifiche e lezioni apprese.	Registro incidenti, notifiche, relazioni finali, verbali e azioni correttive

I riferimenti a tecnologie o ambienti specifici, compresi OT/ICS, si applicano soltanto quando tali componenti sono effettivamente presenti nel perimetro dell'Ateneo. L'assenza di uno strumento nominativamente indicato non costituisce di per sé una non conformità, purché l'obiettivo di sicurezza sia raggiunto con misure adeguate, proporzionate e documentate.

9 PROCESSI DI ATTRIBUZIONE, REPORTING ED ESCALATION

L'attribuzione formale dei ruoli acquista efficacia soltanto quando è collegata a processi comprensibili e ripetibili. Questo capitolo descrive quindi come le responsabilità si attivano nei casi più rilevanti: l'emersione di un nuovo SIR, la gestione di un rischio o di uno scostamento, la risposta a un incidente e il reporting agli organi di vertice. I passaggi non sostituiscono le procedure specialistiche, ma ne chiariscono il raccordo organizzativo.

9.1 Individuazione di un nuovo SIR

Passaggio	Attività	Esito
1	Segnalazione o ricognizione del sistema e delle sue dipendenze	SIR candidato identificato
2	Verifica della rilevanza e del rapporto con il perimetro esistente	Decisione di inclusione e priorità
3	Individuazione del Responsabile del SIR e del Gestore tecnico	Responsabilità formalizzate
4	Censimento e valutazione del rischio	Aggiornamento degli inventari e di ALL004
5	Definizione di misure, tempi, risorse e controlli	Aggiornamento dei piani di trattamento/adeguamento
6	Integrazione nei flussi di monitoraggio, incidenti e reporting	SIR governato nel ciclo ordinario

9.2 Gestione di un rischio o di uno scostamento

Il soggetto che rileva il rischio o lo scostamento lo comunica al Responsabile competente. Il Gestore tecnico propone o attua le misure; il Responsabile del SIR o il Dirigente IT, secondo il perimetro, assume la decisione entro la propria autorità. Le esigenze che richiedono risorse ulteriori, accettazioni eccezionali o decisioni interstrutturali sono sottoposte agli organi competenti. Gli esiti alimentano ALL004, il Piano di trattamento e il Piano di adeguamento.

9.3 Gestione di un incidente

Fase	Responsabilità principale	Raccordo
Rilevazione e segnalazione	Gestori, utenti, SOC o altre funzioni rilevanti	Attivazione del team di risposta
Contenimento, eradicazione e ripristino	Team di risposta, DIT e Gestore del SIR	Responsabile SIR/Dirigente IT e fornitori
Valutazione della significatività	Funzioni designate con supporto tecnico e legale	Punto di contatto, Referente CSIRT, DPO se pertinente
Notifica	Referente CSIRT e sostituti	Informazioni fornite dalle strutture coinvolte
Comunicazione e crisi	Ruoli previsti dal Piano di gestione delle crisi	Organi di vertice e destinatari interessati
Chiusura e miglioramento	Responsabile dell'incidente e RSGSI	Riesame, ALL004, trattamento e adeguamento

9.4 Reporting agli organi di vertice

Contenuto	Responsabile del consolidamento	Periodicità/attivazione
Profilo di rischio e rischi residui rilevanti	Dirigente IT con RSGSI e Risk Owner	Periodica e in occasione del riesame
Stato delle misure e dei piani	Owner dei piani, coordinamento RSGSI	Secondo scadenze e reporting definito
Incidenti significativi e notifiche	Punto di contatto/Referente CSIRT con funzioni coinvolte	Secondo urgenza e obblighi applicabili
Audit, non conformità e miglioramenti	RSGSI e funzioni di controllo	Dopo verifiche e nel Riesame della Direzione
Esigenze di risorse o decisioni	Dirigente IT o Responsabile competente	Quando l'esigenza eccede l'autorità disponibile

10 FORMALIZZAZIONE, COMPETENZE E CICLO DI VITA DEI RUOLI

L'organizzazione descritta nei capitoli precedenti deve poter essere ricondotta, in ogni momento, a persone e unità organizzative effettivamente individuate. A tal fine, i ruoli sono formalizzati mediante atti, nomine, organigrammi, mansionari o registrazioni coerenti con la loro natura. La forma può quindi variare, ma deve sempre rendere verificabili responsabilità, autorità, sostituzioni e durata dell'incarico.

Per ciascuna attribuzione sono documentati, in misura proporzionata al ruolo:

- ambito e perimetro della responsabilità;
- compiti, autorità e canali di escalation;
- eventuali sostituti e modalità di attivazione;
- obblighi di comunicazione e mantenimento delle evidenze;
- competenze e formazione richieste;
- durata, riesame e condizioni di cessazione.

L'affidabilità, l'adeguatezza e il mantenimento delle competenze sono disciplinati dal capitolo 11. Il ciclo di attivazione, variazione e cessazione dei rapporti, dei ruoli e degli accessi è disciplinato dal capitolo 12. Le due discipline costituiscono parte integrante del modello organizzativo e si applicano secondo il perimetro e le responsabilità qui definiti.

La Direzione Risorse Umane mantiene le registrazioni formative di competenza; la Direzione IT e i responsabili organizzativi segnalano i fabbisogni specialistici e verificano che i soggetti assegnati a ruoli rilevanti dispongano delle competenze necessarie.

10.1 Registro nominativo dei ruoli NIS

In attuazione della misura GV.RR-02, l'Ateneo mantiene un registro nominativo aggiornato del personale cui sono attribuiti ruoli e responsabilità specifici per la sicurezza dei sistemi informativi e di rete. Il registro non replica la Matrice RACI: la RACI descrive il modello delle responsabilità, mentre il registro identifica chi, nel periodo considerato, ricopre concretamente ciascun ruolo.

Il registro riporta almeno il ruolo, il nominativo, la struttura di appartenenza, l'ambito o i SIR interessati, l'atto o la fonte dell'attribuzione, l'eventuale sostituto, la data di decorrenza, lo stato dell'incarico e la data dell'ultima verifica. Il RSGSI ne coordina il consolidamento con la Direzione Risorse Umane e con le strutture titolari dei SIR; i responsabili competenti comunicano tempestivamente nomine, variazioni e cessazioni. La diffusione avviene secondo necessità, applicando i principi di pertinenza e minimizzazione dei dati personali.

10.2 Amministratori di Sistema e fornitori

Gli Amministratori di Sistema sono nominati e verificati secondo le procedure applicabili. Le utenze privilegiate devono essere nominative o comunque riconducibili alle persone autorizzate. Per i fornitori, il contratto e le procedure di accesso definiscono responsabilità operative, obblighi di sicurezza, comunicazioni, evidenze e cessazione degli accessi.

11 AFFIDABILITÀ, COMPETENZE, FORMAZIONE E CONSAPEVOLEZZA

La sicurezza dei SIR dipende anche dall'affidabilità delle persone, dalla loro adeguatezza rispetto ai compiti assegnati e dalla capacità di riconoscere e gestire comportamenti ed eventi rilevanti. L'Ateneo applica pertanto un processo proporzionato al ruolo, al livello di privilegio, alla criticità del SIR e alle informazioni trattate. Il processo riguarda personale strutturato e non strutturato, collaboratori, consulenti, fornitori e ogni altro soggetto cui siano attribuiti compiti o accessi rilevanti ai fini NIS.

11.1 Responsabilità

Soggetto	Responsabilità principale
Direzione Risorse Umane	Governa i processi di reclutamento e rapporto di lavoro; conserva le registrazioni di competenza; concorre alla pianificazione della formazione e comunica le variazioni rilevanti.
Direzione IT e RSGSI	Definiscono i requisiti di sicurezza e i contenuti specialistici, coordinano il programma NIS, verificano le evidenze e propongono miglioramenti.
Responsabile del SIR / responsabile organizzativo	Definisce i requisiti del ruolo nel proprio perimetro, verifica l'adeguatezza della persona, segnala fabbisogni e assicura la partecipazione alle attività previste.
Gestore tecnico / responsabile operativo	Verifica le competenze tecniche necessarie, limita le attività alle persone abilitate e segnala scostamenti o necessità di aggiornamento.
Persona interessata	Partecipa alla formazione, rispetta le regole, mantiene le competenze richieste e segnala tempestivamente incidenti, errori, vulnerabilità o conflitti di interesse.

11.2 Definizione e verifica dei requisiti

Prima dell'attribuzione di un ruolo NIS o di un accesso rilevante, il responsabile competente definisce le conoscenze, le capacità, l'esperienza, l'eventuale formazione obbligatoria e, quando giustificato, le certificazioni o abilitazioni richieste. I requisiti sono descritti nell'atto di attribuzione, nel profilo professionale, nel contratto, nel capitolato o in altra registrazione appropriata.

L'adeguatezza è verificata utilizzando informazioni pertinenti e legittimamente disponibili, nel rispetto della disciplina sul lavoro e sulla protezione dei dati personali. Per personale esterno e fornitori la verifica comprende, secondo rischio, referenze, qualifiche, impegni di riservatezza, obblighi contrattuali, conflitti di interesse e capacità di garantire sostituzione e continuità. L'esito è documentato senza raccogliere dati eccedenti.

11.3 Formazione e consapevolezza

Il programma di formazione è annuale, aggiornabile durante l'anno e basato sui rischi, sugli incidenti, sulle vulnerabilità, sugli audit, sui cambiamenti normativi e tecnologici e sulle esigenze segnalate dai responsabili. Esso distingue almeno quattro livelli, evitando che una formazione generale sia considerata sufficiente per ruoli specialistici o di governo.

Destinatari	Contenuti minimi	Momento e verifica
Tutto il personale e collaboratori	Regole essenziali, phishing e social engineering, protezione delle credenziali e dei dati, uso sicuro degli strumenti, canali di segnalazione.	All'ingresso e aggiornamento periodico; verifica di fruizione e, ove opportuno, apprendimento.
Organi di amministrazione e direzione	Obblighi NIS, responsabilità di supervisione, rischio, decisioni, incidenti significativi, crisi e reporting.	Secondo obblighi applicabili e in occasione di cambiamenti rilevanti; evidenza della partecipazione.
Ruoli NIS, Responsabili SIR e owner	Responsabilità, RACI, rischio, fornitori, continuità, incidenti, escalation, evidenze e accettazione del rischio.	Prima o subito dopo l'attribuzione e almeno a ogni cambiamento sostanziale del ruolo.
Ruoli tecnici e privilegiati	Amministrazione sicura, logging, vulnerabilità, backup e restore, risposta agli incidenti, procedure e tecnologie di competenza.	Prima dell'abilitazione quando necessario; aggiornamento tecnico e prove pratiche proporzionate.

Campagne di awareness, comunicazioni mirate e simulazioni, incluse quelle di phishing quando appropriate, integrano la formazione formale. Gli esiti sono utilizzati per individuare esigenze collettive o individuali, non per sostituire i processi disciplinari o di valutazione del personale.

11.4 Registrazioni, efficacia e riesame

Per ogni attività sono conservati almeno destinatari, contenuti, data, modalità, partecipazione ed esito della verifica prevista. La Direzione Risorse Umane conserva le registrazioni di propria competenza; il RSGSI consolida il quadro NIS e segnala carenze ai responsabili. L'efficacia è valutata mediante test, simulazioni, indicatori, audit, osservazione degli incidenti e verifica dell'applicazione delle regole.

L'adeguatezza dei soggetti che ricoprono ruoli rilevanti è riesaminata almeno annualmente nell'ambito del riesame organizzativo e, inoltre, in caso di variazione del ruolo, accessi privilegiati nuovi o ampliati, incidente significativo, mancato rispetto delle regole, assenza prolungata, cambiamento del SIR o delle minacce. Per gli Amministratori di Sistema restano ferme le verifiche specifiche previste dalla disciplina applicabile e dagli atti dell'Ateneo.

12 ATTIVAZIONE, VARIAZIONE E CESSAZIONE DI RAPPORTI, RUOLI E ACCESSI

Il ciclo di vita delle identità e degli accessi deve seguire il ciclo effettivo del rapporto con l'Ateneo e delle responsabilità attribuite. Le automazioni centrali costituiscono il presidio ordinario, ma non esauriscono il processo: accessi locali, privilegi, dispositivi, certificati, token, account presso fornitori e conoscenze operative devono essere gestiti dai rispettivi titolari. La disciplina si applica al personale, ai collaboratori, agli studenti quando dotati di accessi ulteriori rispetto a quelli ordinari, ai fornitori e agli altri soggetti autorizzati.

12.1 Principi e responsabilità

- identità individuale e riconducibile al soggetto, salvo account tecnici espressamente autorizzati e controllati;
- minimo privilegio, necessità di conoscere, separazione dei compiti e durata limitata degli accessi temporanei;
- autorizzazione del responsabile competente e tracciabilità della richiesta, dell'approvazione e dell'esecuzione;
- allineamento tempestivo tra rapporto, struttura, ruolo, SIR, accessi, dispositivi e registri;
- revoca o modifica senza ingiustificato ritardo quando vengono meno le condizioni dell'autorizzazione.

Soggetto	Compito nel processo
Direzione Risorse Umane / struttura che governa il rapporto	Registra e comunica attivazione, variazione, sospensione e cessazione nelle fonti autoritative dell'Ateneo.
Responsabile organizzativo / Responsabile SIR	Determina necessità, ruolo, durata e livello degli accessi; approva variazioni; assicura passaggio di consegne e segnala urgenze.
Direzione IT / gestori delle identità centrali	Gestisce GIA/IDM e i sistemi centrali di autenticazione e autorizzazione; registra gli esiti e controlla anomalie e sincronizzazioni.
Gestore tecnico del SIR / fornitore	Attua, modifica e revoca gli accessi applicativi, locali o privilegiati; restituisce evidenza al responsabile e gestisce gli account tecnici.
Assegnatario	Usa credenziali e asset secondo le regole; protegge i fattori di autenticazione; restituisce beni e informazioni e collabora al passaggio di consegne.

12.2 Attivazione

Per il personale registrato nei sistemi centrali, l'inserimento nell'applicativo autoritativo di Ateneo alimenta GIA/IDM e i sistemi di autenticazione secondo regole predefinite. Prima dell'effettiva abilitazione, il responsabile competente deve tuttavia verificare che il rapporto sia attivo, che il ruolo sia definito e che gli accessi richiesti siano coerenti con le mansioni. Gli accessi non derivabili automaticamente, quelli locali e quelli privilegiati richiedono una richiesta e un'approvazione tracciate.

Quando pertinente, l'attivazione comprende accettazione delle regole, impegni di riservatezza, formazione iniziale, consegna dei dispositivi, configurazione sicura, MFA, registrazione dei recapiti operativi e attribuzione di un sostituto. Per i fornitori devono essere verificati contratto, referente interno, durata, sistemi autorizzati, modalità di assistenza e obblighi di segnalazione degli incidenti.

12.3 Variazione

Ogni cambiamento di struttura, funzione, mansione, contratto, responsabilità sul SIR o necessità operativa determina una rivalutazione degli accessi. Le autorizzazioni non sono semplicemente accumulate: quelle non più necessarie sono revocate, i privilegi sono adeguati al nuovo ruolo e gli accessi incompatibili sono rimossi. La variazione comprende, quando necessario, aggiornamento del registro dei ruoli NIS, RACI applicativa, contatti di emergenza, inventari, gruppi, account locali, dispositivi e responsabilità sui dati.

Gli accessi temporanei o eccezionali indicano motivazione, approvatore, ambito e scadenza e sono soggetti a revoca automatica o verifica alla scadenza. Gli accessi privilegiati e quelli relativi a SIR critici sono riesaminati con maggiore frequenza e dopo cambiamenti significativi.

12.4 Cessazione, sospensione e casi urgenti

Alla cessazione del rapporto o dell'incarico, le identità centrali sono disabilitate secondo le regole dell'Ateneo e i titolari dei sistemi revocano senza ingiustificato ritardo accessi locali, privilegi, VPN, token, certificati, chiavi, account cloud e accessi presso fornitori. Sono inoltre recuperati dispositivi e supporti, trasferite le informazioni di servizio, aggiornati i contatti e verificata la presenza di account condivisi o deleghe da rimuovere. La conservazione dei dati e della casella segue le regole applicabili e non mantiene accessi personali non necessari.

In caso di rischio immediato, sospensione cautelare, compromissione delle credenziali o cessazione non programmata, il responsabile competente attiva il canale urgente verso Risorse Umane, Direzione IT e gestori interessati. La protezione dei sistemi prevale sui tempi del flusso ordinario, fermo restando il rispetto delle competenze e la successiva formalizzazione delle azioni adottate. Per i fornitori, la cessazione o scadenza contrattuale comprende revoca degli accessi, restituzione o cancellazione dei dati, restituzione degli asset e attestazione delle operazioni previste.

12.5 Verifiche ed evidenze

Le evidenze comprendono almeno evento che ha originato il processo, richiesta e approvazione, identità e ruolo, SIR e privilegi interessati, data e ora di esecuzione, esecutore, eccezioni, restituzione degli asset e verifica conclusiva. Sono effettuate riconciliazioni periodiche tra fonti autoritative, IDM, directory, applicazioni, accessi privilegiati e registri degli asset. Anomalie, ritardi e account orfani sono registrati, corretti ed eventualmente trattati come non conformità, rischio o incidente.

13 COMUNICAZIONE INTERNA E COMPRENSIONE DEI RUOLI

L'organizzazione assicura che ciascun soggetto comprenda il proprio ruolo, le relazioni con gli altri ruoli e i limiti della propria autorità. Il presente documento, la Matrice RACI, gli atti di nomina, l'organigramma per la sicurezza e le procedure specialistiche sono resi disponibili ai destinatari secondo necessità.

La sola pubblicazione dei documenti non è sufficiente: la comunicazione deve essere calibrata sui destinatari e consentire loro di riconoscere le situazioni nelle quali devono agire, consultare un altro ruolo oppure attivare un'escalation. In particolare, essa deve assicurare:

- conoscenza dei canali per segnalare incidenti, rischi e vulnerabilità;
- comprensione dei casi in cui è necessaria l'escalation;
- tempestiva comunicazione dei cambiamenti organizzativi e tecnici;
- informazione ai soggetti consultati o informati secondo la RACI;
- tracciabilità delle decisioni e delle responsabilità assunte.

14 RIESAME E AGGIORNAMENTO

L'assetto organizzativo e la Matrice RACI sono riesaminati almeno annualmente e quando intervengono incidenti significativi, variazioni organizzative, modifiche del perimetro, nuovi SIR, cambiamenti normativi, esiti di audit o mutamenti rilevanti del rischio.

Il riesame non consiste in una conferma meramente formale. Deve verificare che l'assetto descritto continui a corrispondere all'organizzazione reale, che le responsabilità siano esercitabili e che le evidenze prodotte dai processi confermino il funzionamento del modello. Sono quindi esaminati almeno:

- completezza e attualità dei ruoli e delle nomine;
- presenza di un Accountable univoco per attività e perimetro;
- coerenza tra responsabilità, autorità, risorse e competenze;
- effettivo esercizio dei flussi di reporting ed escalation;
- coerenza con valutazione dei rischi, piani, audit e Riesame della Direzione;
- necessità di aggiornare procedure, formazione e accessi.

Il RSGSI coordina la raccolta delle proposte di aggiornamento; il Dirigente IT valuta gli impatti nel perimetro di competenza e sottopone agli organi appropriati le modifiche che richiedono approvazione o decisioni interstrutturali.

15 ALLEGATI E RIFERIMENTI OPERATIVI

- Allegato – Matrice RACI NIS2;
- Politica per la sicurezza dei sistemi informativi e di rete;
- Valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete e ALL004;
- Piano di trattamento del rischio e di gestione delle crisi;
- Piano di adeguamento;
- documentazione di audit, non conformità, azioni di miglioramento e Riesame della Direzione;
- Dichiarazione di Applicabilità e procedure del SGSI ISO 27001.

RACI – Responsabilità NIS2

R = Responsible (esegue) | A = Accountable (risponde) | C = Consulted (consultato) | I = Informed (informato)

Area NIS2	Rif. NIS2	Responsabilità	R			A			C			I		
a) Governance e responsabilità del management														
Governance e responsabilità del management	GV.PO-01 GV.RR-02	Approvazione e supervisione delle politiche di sicurezza delle informazioni	Dirigente IT			CdA			AdS, RSGSI	DPO, Delegato, DG	Senato Accademico	Tutto il personale dell'Ateneo	Studenti	
Governance e responsabilità del management	GV.PO-02	Reporting agli organi direttivi su rischi, KPI e stato di conformità	Dirigente IT			CdA			AdS, RSGSI			DPO	Delegato, DG	Senato Accademico
Governance e responsabilità del management	GV.RM-03	Gestione del rischio cyber (Risk Management)	RSGSI	Risk Owner	Direzione IT / Gestore tecnico del SIR	Dirigente IT / Responsabile del SIR (secondo perimetro)			Process/Service Owner	DPO, se pertinente	CdA per rischi riservati o fuori delega	Delegato, DG	Senato Accademico	Accettazione residuo: v. documenti 2–3 e sistema delle deleghe.
Governance e responsabilità del management	GV.PO-01 GV.PO-02	Gestione della conformità normativa e audit di sicurezza	Direzione IT - Area Sistemi di Calcolo			CdA			RSGSI	DPO				
Governance e responsabilità del management	GV.PO-02	Valutazione e revisione periodica delle misure di sicurezza e audit di sicurezza	Direzione IT - Area Sistemi di Calcolo	RSGSI	Soggetto esterno indipendente (solo per audit)	CdA			DPO					
b) Sicurezza della supply chain														
Sicurezza della supply chain	GV.SC-01 GV.SC-04 GV.SC-07	Coordinamento dei fornitori esterni e vendor risk management	Figura responsabile dell'acquisto / titolare del contratto	Direzione IT / Responsabile del SIR (requisiti di sicurezza)	RSGSI	Dirigente IT / Responsabile del SIR (secondo perimetro)			DTGAL / struttura acquisti	Process/Service Owner		DG		V. regola di perimetro nel foglio "Ruoli e definizioni".
c) Gestione degli asset														
Gestione degli asset	ID.AM-01 ID.AM-02 ID.AM-03 ID.AM-04	Gestione degli asset	Direzione IT - Area Servizi	Gestore tecnico del SIR (SIR esterni)		Dirigente IT / Responsabile del SIR (secondo perimetro)			Process/Service Owner	RSGSI				V. regola di perimetro.
d) Gestione della vulnerabilità														
Gestione delle vulnerabilità	ID.RA-05	Gestione delle vulnerabilità cyber	Direzione IT - Area Sistemi di Calcolo	Gestore tecnico del SIR		Dirigente IT / Responsabile del SIR (secondo perimetro)			RSGSI	Process/Service Owner, se pertinente				V. regola di perimetro.
Gestione delle vulnerabilità	ID.RA-05	Gestione delle vulnerabilità cyber — ambienti OT/ICS	Direzione IT - Area Sistemi di Calcolo	Gestore tecnico del SIR		Dirigente IT / Responsabile del SIR (secondo perimetro)			RSGSI	Process/Service Owner, se pertinente				V. regola di perimetro.
Gestione delle vulnerabilità	ID.RA-05	Penetration testing (IT e OT)	Direzione IT - Area Sistemi di Calcolo	Gestore tecnico del SIR	Soggetto esterno incaricato, se previsto	Dirigente IT / Responsabile del SIR (secondo perimetro)			RSGSI	Process/Service Owner, se pertinente				V. regola di perimetro.
e) Continuità operativa e ripristino														
Continuità operativa e ripristino	RC.RP-01	Business Continuity Plan (BCP)	Direzione IT - Area Sistemi di Calcolo / Gestore tecnico del SIR	Process/Service Owner		Dirigente IT / Responsabile del SIR (secondo perimetro)			RSGSI	Responsabile della struttura titolare, se pertinente				Process/Service Owner definisce esigenze di continuità.
Continuità operativa e ripristino	RC.RP-01	Disaster recovery — piano di ripristino IT	Direzione IT - Area Sistemi di Calcolo / Gestore tecnico del SIR	Process/Service Owner		Dirigente IT / Responsabile del SIR (secondo perimetro)			RSGSI	Fornitore, se pertinente				V. regola di perimetro.
Continuità operativa e ripristino	RC.RP-01	Backup e test periodici di ripristino	Direzione IT - Area Sistemi di Calcolo / Gestore tecnico del SIR			Dirigente IT / Responsabile del SIR (secondo perimetro)			RSGSI	Process/Service Owner				V. regola di perimetro.
f) Autenticazione, identità e controllo accessi														
Autenticazione, identità e controllo accessi	PR.AA	Gestione delle utenze	Direzione IT - Area Servizi	Gestore tecnico del SIR per utenze locali		Dirigente IT / Responsabile del SIR (secondo perimetro)			Responsabile organizzativo / Process Owner, se pertinente					Identità centrali DIT; utenze locali secondo perimetro.
Autenticazione, identità e controllo accessi	PR.AA	Gestione delle identità e degli accessi privilegiati (IAM/PAM)	Direzione IT - Area Sistemi di Calcolo	Gestore tecnico del SIR per accessi locali/privilegiati		Dirigente IT / Responsabile del SIR (secondo perimetro)			RSGSI	Responsabile organizzativo / Process Owner, se pertinente				Accessi locali/privilegiati secondo perimetro.
Autenticazione, identità e controllo accessi	PR.AA	Autenticazione multifattore (MFA) e autenticazione continua	Direzione IT - Area Sistemi di Calcolo	Gestore tecnico del SIR, se controllo locale		Dirigente IT / Responsabile del SIR (secondo perimetro)			RSGSI					Controlli locali secondo perimetro.
Autenticazione, identità e controllo accessi	PR.AA	Assegnazione e gestione dei device	Direzione IT - Area Servizi	Gestore tecnico / struttura che gestisce device in autonomia		Dirigente IT / Responsabile del SIR o struttura titolare (secondo perimetro)			RSGSI					Device locali/autonomi: v. regola di perimetro.
g) Sicurezza dei dati														
Sicurezza dei dati	PR.DS	Salvaguardia dei dati personali	Direzione IT	Gestore tecnico del SIR		Dirigente IT / Responsabile del SIR (secondo perimetro)			Process/Service Owner	DPO				DPO consultato per dati personali.
Sicurezza dei dati	PR.DS	Gestione della crittografia e dei certificati digitali	Direzione IT	Gestore tecnico del SIR		Dirigente IT / Responsabile del SIR (secondo perimetro)			Process/Service Owner	RSGSI				V. regola di perimetro.
h) Sviluppo, configurazione e manutenzione														
Sviluppo, configurazione e manutenzione	PR.PS	Sviluppo sicuro	Direzione IT - Area Sistemi Informativi	Gestore tecnico del SIR / struttura o fornitore che sviluppa		Dirigente IT / Responsabile del SIR (secondo perimetro)			RSGSI	Process/Service Owner				Sviluppo esterno/autonomo: v. regola di perimetro.
Sviluppo, configurazione e manutenzione	PR.PS	Coordinamento delle attività operative IT	Direzione IT - Area Sistemi Informativi	Gestore tecnico del SIR		Dirigente IT / Responsabile del SIR (secondo perimetro)			RSGSI	Process/Service Owner, se pertinente				V. regola di perimetro.
i) Protezione delle reti e delle comunicazioni														
Protezione delle reti e delle comunicazioni	PR.IR	Apparati di rete	Direzione IT - Area Networking	Gestore tecnico del SIR per reti locali esterne, se presenti		Dirigente IT / Responsabile del SIR (secondo perimetro)			RSGSI					Reti locali esterne: v. regola di perimetro.
Protezione delle reti e delle comunicazioni	PR.IR	Connettività e Wi-Fi	Direzione IT - Area Networking	Gestore tecnico del SIR per reti locali esterne, se presenti		Dirigente IT / Responsabile del SIR (secondo perimetro)			RSGSI					Reti locali esterne: v. regola di perimetro.
Protezione delle reti e delle comunicazioni	PR.IR	VPN (Virtual Private Network)	Direzione IT - Area Networking	Gestore tecnico del SIR per reti locali esterne, se presenti		Dirigente IT / Responsabile del SIR (secondo perimetro)			RSGSI					Reti locali esterne: v. regola di perimetro.
Protezione delle reti e delle comunicazioni	PR.IR	Firewall	Direzione IT - Area Networking	Gestore tecnico del SIR per reti locali esterne, se presenti		Dirigente IT / Responsabile del SIR (secondo perimetro)			RSGSI					Reti locali esterne: v. regola di perimetro.
Protezione delle reti e delle comunicazioni	PR.IR	Gestione del cablaggio e armadi di rete	DTGAL			DTGAL			Direzione IT	Responsabile del SIR / Gestore tecnico, se interessati				Infrastruttura fisica a DTGAL; SIR consultato se interessato.
j) Monitoraggio degli eventi di sicurezza														
Monitoraggio degli eventi di sicurezza	DE.CM	SIEM (Security Information and Event Management) — IT e OT	Direzione IT - Area Sistemi di Calcolo	Gestore tecnico del SIR		Dirigente IT / Responsabile del SIR (secondo perimetro)			RSGSI	Referente CSIRT, se emerge un incidente notificabile				Referente CSIRT coinvolto se emerge incidente notificabile.
Monitoraggio degli eventi di sicurezza	DE.CM	SOC (Security Operation Center) con copertura IT e OT/ICS	Direzione IT - Area Sistemi di Calcolo	Gestore tecnico del SIR		Dirigente IT / Responsabile del SIR (secondo perimetro)			RSGSI	Referente CSIRT, se emerge un incidente notificabile				Referente CSIRT coinvolto se emerge incidente notificabile.
Monitoraggio degli eventi di sicurezza	DE.CM	Threat intelligence (IT e OT/ICS)	Direzione IT - Area Sistemi di Calcolo	Gestore tecnico del SIR		Dirigente IT / Responsabile del SIR (secondo perimetro)			RSGSI	Referente CSIRT, se emerge un incidente notificabile				Referente CSIRT coinvolto se emerge incidente notificabile.
Monitoraggio degli eventi di sicurezza	DE.CM	Antivirus e protezione endpoint	Direzione IT - Area Servizi	Gestore tecnico del SIR		Dirigente IT / Responsabile del SIR (secondo perimetro)			RSGSI	Referente CSIRT, se emerge un incidente notificabile				Referente CSIRT coinvolto se emerge incidente notificabile.
k) Risposta agli incidenti e ripristino														
Risposta agli incidenti e ripristino	RS.MA	Gestione e risposta agli incidenti (Incident Response)	Team Cybersecurity I livello	Direzione IT / Gestore tecnico del SIR		Dirigente IT / Responsabile del SIR (secondo perimetro)			RSGSI	DPO, se pertinente	Referente CSIRT, se pertinente	CdA	DG	Gestione tecnica distinta dalla funzione di notifica CSIRT.
Risposta agli incidenti e ripristino	RS.CO	Notifica degli incidenti significativi al CSIRT e alle autorità competenti	Referente CSIRT e sostituti			Referente CSIRT			Punto di contatto	Team Cybersecurity I livello	Dirigente IT / Responsabile del SIR (secondo perimetro)	DPO e RSGSI, se pertinenti	CdA	Notifica a cura di Referente CSIRT e sostituti.
Risposta agli incidenti e ripristino	RS.CO	Comunicazione verso utenti e clienti in caso di incidente rilevante	Referente CSIRT / funzione di comunicazione competente	Process/Service Owner, se pertinente		Dirigente IT / Responsabile del SIR (secondo perimetro)			Team Cybersecurity I livello	DPO, RSGSI		CdA	DG	Coordinare con titolare del servizio/SIR.
l) Formazione del personale e consapevolezza														
Formazione del personale e consapevolezza	PR.AT	Formazione in cybersecurity per tutto il personale, inclusi gli organi direttivi	Direzione HR	Direzione IT		CdA			RSGSI			Tutto il personale dell'Ateneo		
Formazione del personale e consapevolezza	PR.AT	Programma di awareness e simulazioni (es. phishing)	Direzione IT			Dirigente IT			RSGSI	Direzione HR		Tutto il personale dell'Ateneo	CdA	
m) Sicurezza fisica														
Sicurezza fisica	PR.AA-06	Gestione accessi fisici	DTGAL			DTGAL			Direzione IT					
Sicurezza fisica	PR.PS	Gestione sistematica impianti di videosorveglianza	Direzione Informatica e Tecnologie / Gestore tecnico del SIR			Dirigente IT / Responsabile del SIR (secondo perimetro)			DTGAL	DPO, se pertinente				Aspetti sistemistici secondo perimetro; fisici alle strutture competenti.
Sicurezza fisica	PR.PS	Manutenzione infrastrutture tecniche (UPS, condizionatori, impianti elettrici e antincendio)	DTGAL	Fornitori esterni		DTGAL			Direzione IT					

Definizione dei ruoli – RACI NIS2	
Codice	**Significato**
R - Responsible	Esegue materialmente l'attività o coordina l'esecuzione operativa. Possono esservi più Responsible quando necessario.
A - Accountable	Risponde del risultato e assume o valida la decisione nel perimetro assegnato. Deve essercene uno solo per attività e perimetro.
C - Consulted	È consultato prima o durante l'attività e fornisce competenze, pareri o informazioni.
I - Informed	È informato sullo stato, sull'esito o sulle decisioni secondo necessità.
Fonte dei ruoli	Le definizioni, i limiti e i criteri di attribuzione dei ruoli organizzativi sono quelli del documento "Organizzazione per la sicurezza informatica"; questo foglio chiarisce soltanto la lettura della matrice.
Responsabile del SIR (SIR Owner)	Soggetto formalmente individuato che assicura il governo del SIR. Per i SIR esterni al perimetro ISO è normalmente Accountable; per i SIR centrali la funzione equivalente è esercitata dal Dirigente IT secondo la matrice.
Gestore tecnico del SIR	Soggetto interno o esterno che esegue le attività tecniche sul SIR sotto il coordinamento del Responsabile del SIR. È normalmente Responsible e non Accountable.
Risk Owner	Titolare della gestione/decisione sul singolo rischio entro le deleghe attribuite. Non coincide automaticamente con Responsabile del SIR, Gestore tecnico o Process/Service Owner.
Process/Service Owner	Rappresenta esigenze, impatti e priorità del processo o servizio supportato dal SIR; partecipa in particolare a criticità, BIA, RTO/RPO e requisiti di sicurezza/continuità.

Regola di perimetro	Le formule "Dirigente IT / Responsabile del SIR" e "Direzione IT / Gestore tecnico del SIR" indicano ruoli alternativi in funzione del perimetro, non una doppia responsabilità simultanea.
SIR esterno al perimetro ISO	Per un SIR gestito fuori dal perimetro ISO: Responsabile del SIR = Accountable del governo del sistema; Gestore tecnico = Responsible dell'esecuzione tecnica; DIT e RSGSI assicurano raccordo, standard comuni e supporto.