



Modello organizzativo

Modello organizzativo per la Sicurezza delle Informazioni

Azienda	Università degli Studi di Padova
Redatto da	Responsabile Settore Sicurezza delle Informazioni
Verificato da	Dirigente Area Servizi Informatici e Telematici
Approvato da	Direttore Generale
Versione	1.0

Modello organizzativo

Revisioni

Revisione	Data	Descrizione della revisione
1.0	11/03/2026	Prima stesura

Redazione

Azione	Data	Nominativo	Funzione
Redazione	11/03/2026	Dott. Giorgio Paolucci	Resp. Settore Sicurezza delle Informazioni
Verifica	11/03/2026	Ing. Andrea Baraldo	Dirigente ASIT
Approvazione		Ing Alberto Scuttari	Direttore Generale

Modello organizzativo

Sommario

1 Scopo	4
2 Campo di Applicazione	4
3 Termini e Definizioni	5
4 Modello Organizzativo	6
4.1 Organo nazionale: Centro Nazionale per la Sicurezza e Integrità della Ricerca	6
4.2 Organi direttivi	7
4.2.1 Magnifico Rettore	7
4.2.2 Direttore Generale	8
4.3 Consiglio di Amministrazione	9
4.4 Senato Accademico	9
4.5 Area Servizi Informatici e Telematici (ASIT)	10
4.5.1 Dirigente dell'Area Servizi Informatici e Telematici	11
4.6 Punto di contatto	11
4.7 Sostituto Punto di contatto	12
4.8 Referente CSIRT	12
4.9 Referente ICT di Struttura (Dipartimento/Scuola/Centro/Polo)	12
4.10 Referente per la Sicurezza e Integrità della Ricerca	12
4.11 Responsabile Progetto di Ricerca	13
4.12 Area Risorse Umane	14
4.13 Ulteriori ruoli in materia di sicurezza informatica esterni all'Ateneo	14
4.13.1 Fornitori strategici per l'Ateneo: Cineca Consorzio Interuniversitario	15
5 Procedura di Approvazione delle Misure di Sicurezza	15
5.1 Il Processo di Approvazione	15
5.2 Il sistema di Monitoraggio e Controllo	17
5.3 L'aggiornamento e la revisione	17
6 Allegati	17

Modello organizzativo

1 Scopo

La Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 (di seguito “*Direttiva*” o “*NIS2*”) ha introdotto un quadro normativo più rigoroso e armonizzato per la sicurezza delle reti e dei sistemi informativi nell'Unione Europea.

In Italia, la Direttiva è stata recepita con il Decreto Legislativo 4 settembre 2024, n. 138 (di seguito “*Decreto NIS*”).

L'Agenzia per la Cybersicurezza nazionale (“ACN”), quale autorità di settore competente, ha pubblicato, tramite la [Determinazione 164179 del 14 aprile 2025](#), le specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del Decreto NIS, contenute negli allegati 1, 2, 3 e 4.

Tra queste, la GV.RR-02 stabilisce che: “*I ruoli, le responsabilità e le autorità relative alla gestione del rischio di Cybersecurity sono stabiliti, comunicati, compresi e applicati.*” In particolare:

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 almeno un suo sostituto, di cui alla determina adottata ai sensi dell'articolo 7, comma 6 del Decreto NIS.*”
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 verificano incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.*”

Infine, con l'obiettivo di fornire alle istituzioni di ricerca, tra cui gli Atenei, indicazioni operative per rafforzare la sicurezza della ricerca, il Ministero dell'Università e della Ricerca ha emesso nel mese di agosto 2025 le “*Linee Guida per le Istituzioni di Ricerca*” e il “*Modello nazionale per l'Integrità e la Sicurezza della Ricerca*”.

L'Università degli Studi di Padova, (di seguito “*Ateneo*”) tramite il presente documento, ha definito e adottato, con l'obiettivo di ottemperare alle disposizioni sopraindicate, un modello organizzativo per la sicurezza delle informazioni (di seguito “*Modello Organizzativo*”).

2 Campo di Applicazione

Il presente documento si applica a tutti i soggetti, interni ed esterni, che si occupano di sicurezza delle Informazioni per conto dell'Ateneo, ricoprendo uno o più ruoli previsti all'interno del Modello Organizzativo.

Modello organizzativo

3 Termini e Definizioni

Termine	Definizione
Ministero dell'Università e della Ricerca ("MUR")	Il Ministero dell'Università e della Ricerca avente il compito di promuovere e sviluppare l'attività di ricerca scientifica e tecnologica italiana, in collegamento con le altre amministrazioni dello stato, centrali e regionali, che hanno competenze analoghe in materia.
Autorità di controllo ("ACN")	L'Agenzia per la Cybersicurezza Nazionale (ACN) è l'Autorità nazionale competente NIS di cui all'articolo 8, paragrafo 1, della Direttiva (UE) 2022/2555 e svolge numerose funzioni ai sensi dell'articolo 10 del Decreto NIS
Centro europeo per la sicurezza e integrità della ricerca	Il Centro di competenza <i>europeo</i> per la sicurezza informatica della ricerca, finalizzato allo sviluppo di pratiche comuni e alla creazione di una base di conoscenze per l'elaborazione di politiche condivise a livello europeo.
Centro nazionale per la sicurezza e integrità della ricerca	Il Centro di competenza <i>nazionale</i> per la sicurezza informatica della ricerca, finalizzato a interagire con il Centro di competenza europeo allo scopo di sviluppare e attuare pratiche comuni a livello nazionale.
Organi di amministrazione e direttivi	Gli organi di amministrazione e direttivi di cui all'articolo 23 del Decreto NIS
Punto di contatto ("PdC")	La persona fisica designata dal Soggetto NIS ai sensi dell'articolo 7, comma 1, lettera c), del Decreto NIS
Sostituto Punto di Contatto ("Sostituto PdC")	La persona fisica designata dal Soggetto NIS ai sensi dell'articolo 7, comma 4, lettera d), del Decreto NIS
Referente CSIRT e sostituti	Le persone fisiche designate dal Punto di contatto, ai sensi dell'articolo 7, della Determinazione di ACN n. 333017/2025, per interloquire con lo CSIRT Italia, di cui all'articolo 2, comma 1, lettera i) del decreto NIS, ed effettuare le notifiche di cui agli articoli 25 e 26 del medesimo decreto
Segreteria	La persona fisica che svolge funzioni di supporto al punto di contatto e al sostituto punto di contatto per promuovere l'efficace interlocuzione con l'Autorità nazionale competente NIS
Utenti	Il punto di contatto, il sostituto punto di contatto, la segreteria e gli operatori che accedono al Portale ACN e, in particolare, accedono ai Servizi NIS

Modello organizzativo

4 Modello Organizzativo

L'Ateneo ha definito le responsabilità e i livelli di coinvolgimento di una serie di ruoli volti a garantire un'adeguata Sicurezza delle Informazioni, nel rispetto degli obblighi derivanti da normative e prassi in materia applicabili.

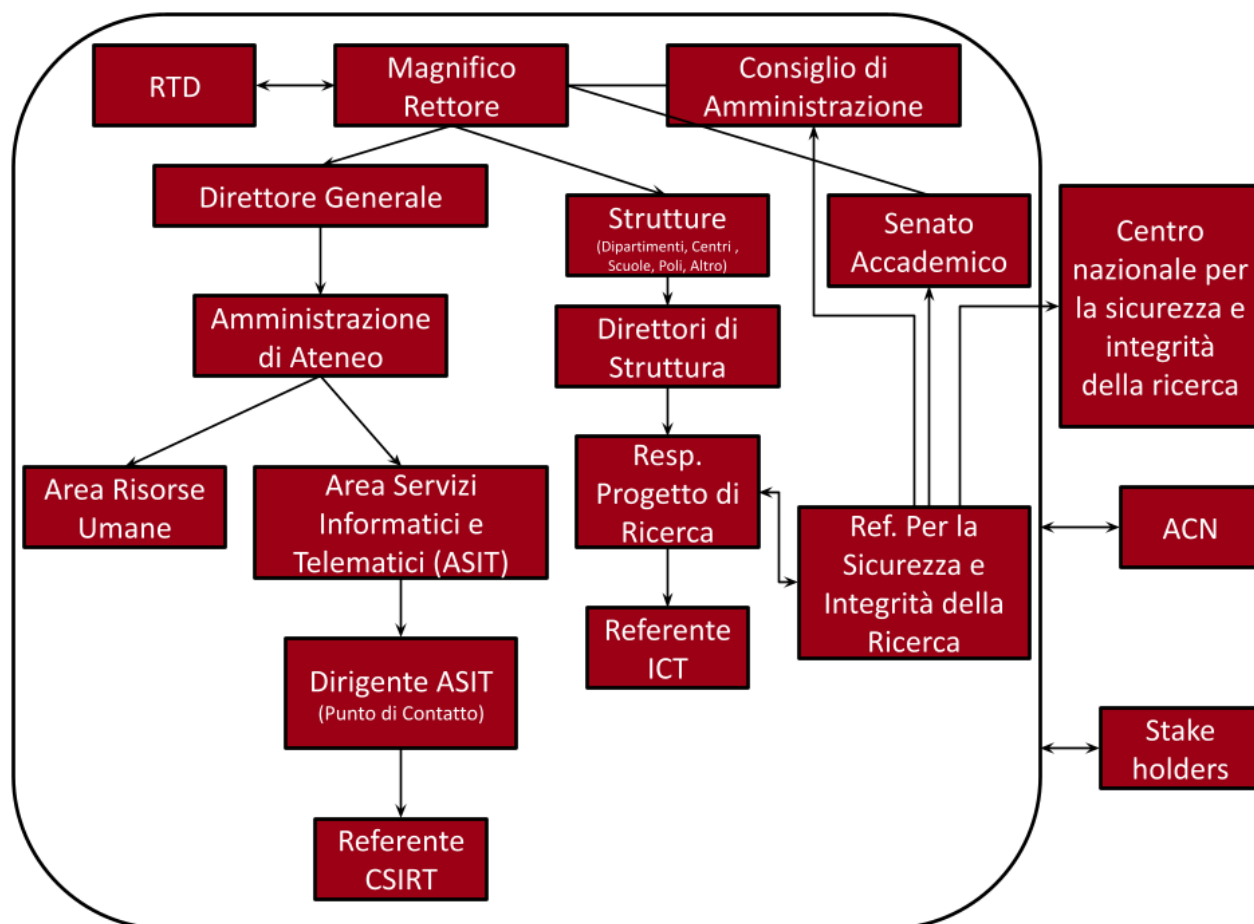


Figura 1 - Modello organizzativo

Nei paragrafi successivi sono approfondite le responsabilità attribuite a ciascuna struttura/ruolo previsto all'interno del Modello organizzativo.

4.1 Organo nazionale: Centro Nazionale per la Sicurezza e Integrità della Ricerca

Il Ministero dell'Università e della Ricerca in raccordo con altri Ministeri interessati, con l'Agenzia Nazionale di Cybersicurezza, nonché il Consiglio dell'Unione Europea¹, istituisce a livello nazionale un *Centro Nazionale per la Sicurezza e Integrità della Ricerca* (di seguito "Centro").

¹ Si veda la [Raccomandazione del Consiglio dell'Unione Europea del 23 maggio 2024](#).

Modello organizzativo

Il Centro Nazionale per la Sicurezza e Integrità della Ricerca operando in coordinamento con il MUR svolge principalmente *funzioni di coordinamento, indirizzo e supporto specialistico* agli enti di ricerca nazionali. Nello specifico, al Centro sono affidati i seguenti compiti:

- svolgere la funzione di raccordo e coordinamento con i Ministeri (ie. MUR) e le agenzie nazionali competenti in materia di sicurezza informatica (ie. ACN);
- coordinare i tavoli e gruppi di lavoro tecnici per l'emissione e aggiornamento periodico di raccomandazioni, linee guida, politiche, procedure e matrici di rischio in ambito di sicurezza informatica della ricerca;
- formulare, previa richiesta da parte degli Atenei, supporto nella classificazione del livello di rischio associato allo svolgimento di attività di ricerca e nell'adozione di idonee misure di mitigazione;
- fornire supporto e assistere, previa richiesta da parte degli Atenei, nel monitoraggio di criticità, al fine di rendere omogenee e trasparenti le procedure di trasmissione e le informazioni pertinenti alla sicurezza ed integrità della ricerca associate alle domande di finanziamento;
- promuovere momenti di confronto tra gli operatori del sistema della ricerca per condividere criticità, buone pratiche e casi di studio, migliorando costantemente il supporto alle misure di sicurezza e integrità della ricerca;
- realizzare e promuovere attività formativa destinata ai referenti e agli operatori del settore ricerca;
- sviluppare un modello di interazione efficiente tra istituzioni di ricerca, enti finanziatori e organi governativi, prevedendo un sistema di autovalutazione che consenta di adeguare le attività di ricerca in relazione ai profili di rischio rilevati.

4.2 Organi direttivi

L'Ateneo ha individuato come Organi direttivi la Magnifica Rettrice, il Prorettore con delega alle Tecnologie dell'informazione e della comunicazione, il Direttore Generale, il Dirigente dell'Area Servizi Informatici e Telematici, nonché, in considerazione della diretta responsabilità nella gestione dell'Internet Exchange VSIX, il Presidente e il Direttore Tecnico del Centro di Ateneo per la Connettività e i Servizi al Territorio – VSIX.

Come stabilito dalla delibera del CdA di Ateneo n.152 del 27/5/2025 al punto 6, fanno parte degli Organi direttivi anche i Direttori e, se presenti, i Responsabili della Gestione Tecnica (RGT) delle strutture dotate di infrastrutture ICT locali la cui eventuale compromissione potrebbe pregiudicare l'erogazione dei servizi universitari, in conformità a quanto previsto dal D.Lgs. 138/2024.

4.2.1 Magnifico Rettore

Il Magnifico Rettore ha la rappresentanza legale dell'Università ed esercita la funzione di indirizzo, di iniziativa e di coordinamento delle attività scientifiche e didattiche.

Modello organizzativo

Il Magnifico Rettore è provvisto di ogni altra funzione non espressamente attribuita ad altri organi dallo statuto così come previsto dall'art. 2 Legge 30 dicembre 2010, n. 240.

In quanto rappresentante legale con l'autorità di rappresentare l'Ateneo:

- assicura il rispetto delle disposizioni del Decreto NIS e può essere ritenuto responsabile dell'inadempimento in caso di violazione del Decreto NIS da parte dell'Ateneo.
- è informato tempestivamente in merito agli incidenti di sicurezza con impatto significativo e alle notifiche allo CSIRT Italia;
- è informato periodicamente sullo stato complessivo della sicurezza informatica dell'Ateneo;
- è tenuto a seguire adeguata formazione in materia di sicurezza informatica ai sensi della normativa vigente.

4.2.2 Direttore Generale

Il Direttore Generale ha la responsabilità in merito alla gestione complessiva e all'organizzazione dei servizi, delle risorse strumentali e del personale tecnico-amministrativo dell'Ateneo, nonché dei compiti, in quanto compatibili, di cui all'articolo 16 del decreto legislativo 30 marzo 2001, n. 165.

Il Direttore Generale partecipa, senza diritto di voto, alle sedute del Consiglio di Amministrazione.

Il Direttore Generale è responsabile della definizione della strategia di Cybersecurity e della gestione della sicurezza delle informazioni e degli asset aziendali, con l'obiettivo di garantirne la protezione in termini di riservatezza, integrità, disponibilità, verificabilità e accountability.

Il Direttore Generale è responsabile:

- dell'approvazione della valutazione dei rischi posta alla sicurezza dei sistemi informativi e di rete nonché del piano di trattamento dei rischi e delle modalità di implementazione di misure di gestione dei rischi per la sicurezza informatica e della verifica circa l'implementazione delle stesse (Art. 23 Decreto NIS e Misure ID.RA-05 punto 3 e ID.RA-06 punto 3);
- della verifica circa l'implementazione degli obblighi di registrazione e autovalutazione alla piattaforma di ACN di cui all'art. 7 e al capo IV del Decreto NIS;
- della promozione e dell'approvazione dell'offerta periodica di formazione in materia di sicurezza al personale aziendale (Art. 23 Decreto NIS e Misura PR.AT-01 punto 2);
- delle violazioni di cui al Decreto NIS.

Il Direttore Generale, inoltre, è:

- informato e coinvolto tempestivamente in caso di incidenti con impatto significativo e di notifiche allo CSIRT Italia (Art. 23 Decreto NIS);

Modello organizzativo

- tenuto a seguire una formazione in materia di sicurezza informatica (Art. 23 Decreto NIS e Misura PR.AT-01 punto 1).

Il Direttore Generale approva:

- l'organizzazione per la sicurezza informatica, stabilendone ruoli e responsabilità (Misura GV.RR-02 punto 1);
- le politiche di sicurezza per almeno gli ambiti indicati nella misura GV.PO-01 (Misura GV.PO-01 punto 3) e afferenti ai seguenti ambiti: gestione del rischio, ruoli e responsabilità, affidabilità delle risorse umane, conformità e audit di sicurezza, gestione dei rischi per la sicurezza informatica della catena di approvvigionamento, gestione degli asset, gestione delle vulnerabilità, continuità operativa, ripristino in caso di disastro e gestione delle crisi, gestione dell'autenticazione, delle identità digitali e del controllo accessi, sicurezza fisica, formazione del personale e consapevolezza, sicurezza dei dati, sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete, protezione delle reti e delle comunicazioni, monitoraggio degli eventi di sicurezza, risposta agli incidenti e ripristino;
- il piano di adeguamento relativo alle politiche di sicurezza in caso di necessità di revisione o aggiornamento delle politiche medesime (Misura ID.IM-01 punto 1);
- il piano di gestione delle vulnerabilità (Misura ID.RA-08 punto 4);
- il piano di continuità operativa, il piano di ripristino in caso di disastro e un piano per la gestione delle crisi per i sistemi informativi e di rete rilevanti (Misura ID.IM-04 punto 4);
- il piano per la gestione degli incidenti di sicurezza informatica e la notifica allo CSIRT Italia, in accordo a quanto previsto dall'art. 25 del Decreto NIS (Misura RS.MA-01 punto 2);
- i piani di risposta agli incidenti e gli altri piani di Cybersecurity che impattano le operazioni (Misura ID.IM-04 punto 4).

4.3 Consiglio di Amministrazione

Il Consiglio di Amministrazione esercita le funzioni di indirizzo strategico e di approvazione della programmazione finanziaria e del personale.

In materia di sicurezza informatica:

- è informato con periodicità almeno annuale sullo stato di attuazione delle politiche e dei piani di sicurezza;
- delibera esclusivamente nei casi in cui siano richiesti interventi con impatto significativo sul piano economico-finanziario o organizzativo.

4.4 Senato Accademico

Il Senato Accademico esercita le funzioni previste dallo Statuto in materia di didattica, ricerca e servizi agli studenti.

In materia di sicurezza informatica:

Modello organizzativo

- è informato periodicamente sullo stato generale della sicurezza informatica dell'Ateneo;
- può esprimere pareri su aspetti organizzativi che impattino direttamente le attività di didattica, ricerca e terza missione.

Non rientra tra le competenze del Senato l'approvazione delle politiche o dei piani operativi di cybersecurity.

4.5 Area Servizi Informatici e Telematici (ASIT)

L'Area Servizi Informatici e Telematici (ASIT) definisce e adotta misure tecniche, operative e organizzative adeguate, in conformità agli articoli 24 e 25 del Decreto NIS, alle Determinazioni di ACN.

All'Area sono attribuiti i seguenti compiti per la gestione della Cybersecurity all'interno dell'Ateneo per le *aree di propria competenza e pertinenza*:

- sviluppare e gestire il budget per la sicurezza informatica e supervisionare le spese IT e ICT (*ad esclusione di quelle relative ai dipartimenti*);
- supportare l'Ateneo nel mantenimento della conformità alle normative in materia di Cybersecurity applicabili;
- eseguire la valutazione e la gestione dei rischi informatici;
- monitorare minacce e vulnerabilità emergenti e proporre contromisure adeguate;
- implementare misure di sicurezza per proteggere reti, dati e sistemi in termini di riservatezza, integrità e disponibilità;
- supervisionare politiche, procedure e iniziative di sicurezza informatica, inclusi crittografia e cifratura;
- implementare sistemi di autenticazione multi-fattore e canali di comunicazione sicuri;
- valutare i fornitori con impatti sulla Cybersecurity e verificarne la conformità contrattuale;
- gestire l'inventario delle risorse IT;
- predisporre e gestire i piani di risposta agli incidenti di sicurezza;
- assicurare la corretta segnalazione degli incidenti significativi allo CSIRT e all'ACN;
- garantire la continuità operativa, inclusi backup e disaster recovery;
- gestire la sicurezza nello sviluppo e manutenzione dei sistemi informativi;
- supportare, ove richiesto, la Direzione Risorse Umane nella selezione e valutazione del personale dedicato alla cybersecurity;

Modello organizzativo

- supportare la Direzione Risorse Umane nella definizione dei piani formativi in materia di sicurezza informatica, differenziandone i contenuti in relazione al personale coinvolto.

L'Area Servizi Informatici e Telematici fornisce inoltre supporto:

- al Direttore Generale per la definizione e implementazione della strategia di sicurezza informatica e per l'invio di informazioni periodiche sugli incidenti significativi;
- ai Referenti ICT dei Dipartimenti/Strutture per la gestione di incidenti significativi e, ove richiesto, supporto della gestione dei sistemi informativi di dipartimento;
- al Referente per la Sicurezza e Integrità della Ricerca e ai Responsabili Progetti di Ricerca per la gestione degli incidenti significativi e, ove richiesto, per la gestione degli adempimenti connessi alla sicurezza della ricerca richiesti dal Centro Nazionale per la Sicurezza e Integrità della Ricerca.

4.5.1 Dirigente dell'Area Servizi Informatici e Telematici

Il Dirigente dell'Area Servizi Informatici e Telematici coordina e supervisiona l'attuazione delle misure tecniche, operative e organizzative definite dalla Direzione Sistemi Informativi, in conformità agli articoli 24 e 25 del Decreto NIS, alle Determinazioni di ACN.

Al Dirigente ASIT sono attribuiti i seguenti compiti:

- sviluppare il budget per la sicurezza informatica e supervisionare le spese IT e ICT;
- attuare operativamente la valutazione e gestione dei rischi informatici;
- verificare la corretta implementazione delle misure di sicurezza per proteggere reti, dati e sistemi;
- definire e applicare le politiche e procedure di sicurezza informatica, incluse crittografia e cifratura;
- monitorare la corretta gestione dell'inventario delle risorse IT;
- attuare i piani di risposta agli incidenti e favorire una corretta segnalazione allo CSIRT degli incidenti significativi;
- garantire la continuità operativa, inclusi backup e disaster recovery;
- gestire la sicurezza nello sviluppo e manutenzione dei sistemi informativi.

Il Dirigente ASIT fornisce inoltre supporto al Direttore Generale per la definizione e implementazione della strategia di sicurezza informatica e per l'invio di informazioni periodiche sugli incidenti significativi.

4.6 Punto di contatto

Il Dirigente ASIT è stato individuato come Punto di Contatto e, in quanto tale, è responsabile (Artt. 7, 30 e 42 Decreto NIS):

Modello organizzativo

- della registrazione dell'Ateneo e dell'aggiornamento della stessa presso la piattaforma ACN (dal 01/01/2025 al 28/02/2025) e della successiva integrazione con informazioni aggiuntive (dal 15/04/2025 al 31/05/2025);
- dell'aggiornamento delle informazioni su attività e servizi (dal 01/05 al 30/06 a partire dal 2026);
- di fornire eventuali informazioni e chiarimenti richiesti dall'ACN;
- di designare il Referente CSIRT e, ove necessario, i suoi sostituti.

Il Punto di contatto, infine, è informato e coinvolto tempestivamente in caso di incidenti con impatto significativo.

Il Punto di contatto si avvale nello svolgimento dei propri compiti del supporto operativo dei suoi collaboratori.

4.7 Sostituto Punto di contatto

Il Responsabile del Settore Sicurezza delle Informazioni di ASIT, è stato individuato e delegato come Sostituto Punto di contatto e fornisce supporto operativo al Punto di contatto:

- nell'aggiornamento dei dati dell'Ateneo con informazioni aggiuntive (dal 15/04 al 31/05 di ogni anno), nonché tramite il periodico aggiornamento delle informazioni medesime;
- nell'aggiornamento delle informazioni su attività e servizi (dal 01/05 al 30/06 di ogni anno);
- nel fornire eventuali informazioni e chiarimenti richiesti dall'ACN.

4.8 Referente CSIRT

Il Responsabile del Settore Sicurezza delle Informazioni di ASIT, è stato individuato e nominato dal Punto di Contatto quale Referente CSIRT. In tale ruolo assolve ai seguenti compiti:

- effettuare le notifiche di incidenti con impatto significativo allo CSIRT Italia di cui all'art.25 del D.lgs. 138/2024 nonché di informazioni pertinenti di cui all'art. 26 del D.lgs. 138/2024
- interloquire con lo CSIRT Italia in relazione agli incidenti notificati.

Il Referente CSIRT si avvale nello svolgimento dei propri compiti del supporto dei suoi sostituti.

Il Referente CSIRT, inoltre, possiede competenze in materia di sicurezza informatica e di gestione degli incidenti informatici, nonché una conoscenza approfondita dei sistemi informativi e di rete dell'Ateneo.

Modello organizzativo

4.9 Referente ICT di Struttura (Dipartimento/Scuola/Centro/Polo)

Al Referente ICT di Struttura (Dipartimento/Scuola/Centro/Polo) in qualità di funzione di supporto alla propria struttura e al Responsabile di Struttura (Direttore/Presidente) sono affidati i seguenti compiti:

- svolgere il ruolo di interfaccia di collegamento operativo tra la propria Struttura ed ASIT per la gestione dei sistemi informativi della struttura, la risoluzione di malfunzionamenti dei sistemi e il coordinamento delle attività informatiche di struttura;
- supportare il Responsabile di Struttura negli adempimenti relativi alla sicurezza informatica, monitorando i sistemi di struttura e collaborando con l'Area Servizi Informatici e Telematici nell'implementazione delle misure di sicurezza e nella gestione degli incidenti significativi.

4.10 Referente per la Sicurezza e Integrità della Ricerca

Il Referente per la Sicurezza e Integrità della Ricerca individuato all'interno dell'Area Ricerca dell'Ateneo in qualità di punto di raccordo tra l'Ateneo e il Centro Nazionale per la Sicurezza e l'Integrità della Ricerca ha in carico i seguenti compiti in materia di sicurezza e integrità della ricerca:

- richiedere supporto al Centro Nazionale per la Sicurezza e l'Integrità della Ricerca per criticità specifiche o situazioni di particolare complessità;
- supportare il Responsabili dei Progetti di Ricerca nella gestione del rischio delle attività di ricerca al fine di garantire la sicurezza e l'integrità della ricerca medesima;
- esaminare le risultanze delle autovalutazioni delle attività di ricerca per identificare il rischio di cybersicurezza compilate dai Responsabili dei Progetti di Ricerca ove il risultato del rischio fosse sopra soglia;
- garantire supporto e collaborazione con la Direzione Sistemi Informativi per la gestione di incidenti significativi;
- comunicare al Senato Accademico e al Consiglio di Amministrazione eventuali criticità in merito alla gestione dell'area ricerca circa la sicurezza e l'integrità della ricerca medesima.

Nelle more della definizione di un'apposita nomina, tale funzione viene espletata dal Prorettore alla Ricerca o da personale incaricato dallo stesso.

4.11 Responsabile Progetto di Ricerca

Al Responsabile Progetto di Ricerca, individuato per ciascun gruppo di ricerca, nell'ambito della propria area di competenza sono affidati i seguenti compiti in materia di sicurezza e integrità della ricerca:

Modello organizzativo

- effettuare l'autovalutazione delle attività di ricerca per identificare il rischio del progetto e le relative misure di sicurezza da applicare;
- consultare il report generato dalla scheda di autovalutazione e implementare le misure di mitigazione indicate, coinvolgendo, quando necessario e comunque in caso di risultato del rischio sopra soglia, il Referente per la Sicurezza e l'Integrità della Ricerca;
- analizzare le criticità relative all'ambito scientifico/tecnologico, ai partner coinvolti e agli enti finanziatori, dichiarando eventuali assenze di partner o finanziamenti esterni;
- aggiornare tempestivamente l'autovalutazione in caso di modifiche relative a collaborazioni, finanziamenti o altri elementi che alterino il profilo di rischio dell'attività;
- partecipare alle attività formative promosse dall'Ateneo in materia di sicurezza della ricerca;
- rivolgersi al Referente per la Sicurezza e l'Integrità della Ricerca per valutazioni preventive, chiarimenti o situazioni di dubbio;
- assicurare il rispetto delle politiche e procedure in materia di sicurezza informativa, emesse dall'Ateneo, che possano incidere sulla sicurezza e integrità della ricerca;
- garantire supporto e collaborazione con il Referente per la Sicurezza e l'Integrità della Ricerca alla Direzione Sistemi Informativi per la gestione di incidenti significativi;
- rispettare le politiche e i codici di condotta dell'Ateneo in materia di conflitto di interessi, dichiarando tempestivamente eventuali interessi esterni rilevanti di natura scientifica, finanziaria, didattica o derivanti da ruoli ricoperti presso altri enti.

4.12 Area Risorse Umane

Nell'ambito del Modello organizzativo di cybersecurity all'Area Risorse Umane, tramite l'Ufficio Sviluppo Organizzativo, settore Formazione, sono affidate le sue competenze e responsabilità:

- Garantire che il personale da impiegare in ambito cybersecurity rispetti i requisiti e le competenze tecniche necessarie previste dalla normativa in materia, prevedendo, ove ritenuto necessario, l'intervento della Direzione competente per la valutazione tecnica;
- pianificare, organizzare e coordinare le attività di formazione e aggiornamento in materia di cybersecurity rivolte al personale dell'Ateneo, differenziandone i contenuti in relazione ai ruoli, alle responsabilità e al livello di esposizione ai rischi informatici;
- collaborare con la Direzione Sistemi Informativi e il Referente per la Sicurezza e l'Integrità della Ricerca nella definizione e realizzazione dei programmi formativi, assicurandone la coerenza con le strategie e le politiche di sicurezza dell'Ateneo;

Modello organizzativo

- monitorare l'erogazione delle attività formative e verificare l'effettivo apprendimento del personale, al fine di garantire un costante livello di competenza e consapevolezza in materia di sicurezza informatica.

All'Area Risorse Umane sono inoltre affidate le attività di selezione del personale previa valutazione dell'esperienza, capacità e affidabilità che devono fornire idonea garanzia del pieno rispetto della normativa in materia di sicurezza informatica. Analoghe garanzie devono essere raggiunte definendo a livello contrattuale gli eventuali obblighi, in materia di sicurezza informatica, che rimangono validi dopo la cessazione o la modifica del rapporto di lavoro dei dipendenti (ad esempio prevedendo clausole in materia di riservatezza).

4.13 Ulteriori ruoli in materia di sicurezza informatica esterni all'Ateneo

L'Ateneo può avvalersi di fornitori esterni per lo svolgimento di attività con impatto sulla sicurezza informatica, quali:

- Managed Security Service Provider (MSSP) per servizi di sicurezza gestita
- SOC (Security Operations Center) esterno
- Consulenti per valutazioni di sicurezza, penetration test e vulnerability assessment
- Fornitori di servizi cloud e infrastruttura
- Data Center e provider di hosting

4.13.1 Fornitori strategici per l'Ateneo: Cineca Consorzio Interuniversitario

All'interno del panorama nazionale Cineca Consorzio Interuniversitario è stato individuato come fornitore strategico di servizi ICT e di infrastrutture di calcolo per gli Atenei. In particolare, in relazione al supporto fornito all'Ateneo, sono attribuite a Cineca le seguenti principali competenze e responsabilità:

- garantire la gestione sicura e la continuità operativa delle piattaforme applicative e dei sistemi in hosting utilizzati dall'Ateneo;
- adottare e mantenere misure tecniche e organizzative adeguate di sicurezza in coerenza con la normativa vigente e la tipologia di servizio o prodotto reso;
- assicurare la protezione dei dati trattati per conto dell'Ateneo, nel rispetto dei ruoli e degli obblighi previsti dagli accordi contrattuali e dalla disciplina sulla protezione dei dati personali;
- monitorare i sistemi forniti all'Ateneo per individuare eventi di sicurezza e vulnerabilità, attivare le opportune azioni di contenimento e ripristino e informare senza ritardo le strutture competenti di Ateneo in caso di incidenti che possano impattare su riservatezza, integrità o disponibilità dei servizi;
- collaborare con le funzioni interne dell'Ateneo nella valutazione dei rischi, nella definizione delle misure di mitigazione e nella gestione degli incidenti e delle crisi;

Modello organizzativo

- ove previsto contrattualmente, fornire reportistica periodica e informative sullo stato dei servizi, livelli di sicurezza, interventi evolutivi e correttivi, nonché supporto specialistico per audit, verifiche e adempimenti verso autorità e organismi nazionali competenti in materia di sicurezza informatica e ricerca.

5 Procedura di Approvazione delle Misure di Sicurezza

In ottemperanza agli obblighi derivanti da normative e prassi in materia di sicurezza delle informazioni, tra cui il Decreto NIS e le Determinazioni di ACN, nonché alle responsabilità indicate, di seguito si fornisce la descrizione del processo di approvazione delle misure di sicurezza.

5.1 Il Processo di Approvazione

Il processo di approvazione si articola attraverso una sequenza logica e progressiva che garantisce la completezza dell'istruttoria e l'adequatezza delle decisioni assunte dal Magnifico Rettore e dal Direttore Generale.

La *fase preparatoria e istruttoria* prevede che il Dirigente dell'Area Servizi Informatici e Telematici, nell'adempimento delle proprie responsabilità, conduca un'analisi preliminare dei rischi e delle misure di sicurezza attuali e sviluppi le politiche di Cybersecurity da sottoporre all'approvazione del Direttore Generale, le quali sono predisposte in conformità alle normative vigenti e alle Determinazioni ACN.

Successivamente, il Direttore Generale procede alla valutazione e verifica della documentazione prodotta e proposta dal Dirigente ASIT, analizzando l'adequatezza delle misure rispetto al profilo di rischio dell'Ateneo e verificandone la sostenibilità e l'operatività delle iniziative. Particolare attenzione viene dedicata alla valutazione dell'impatto organizzativo e delle risorse necessarie per l'implementazione, al fine di formulare proposte di miglioramento e di mantenimento del sistema atto a prevenire le minacce informatiche.

La *fase deliberativa* implica l'approvazione formale del Direttore Generale della seguente documentazione:

- Organizzazione per la sicurezza informatica;
- Politiche di sicurezza informatica;
- Valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete;
- Piano di trattamento del rischio;
- Piano di gestione delle vulnerabilità;
- Piano di adeguamento;
- Piano di continuità operativa;
- Piano di ripristino in caso di disastro;
- Piano di gestione delle crisi;

Modello organizzativo

- Piano di formazione;
- Piano di gestione degli incidenti di sicurezza informatica.

Il Decreto di approvazione del Direttore Generale, oltre a identificare le fonti normative applicabili tra cui il D.lgs. 4 settembre 2024 n. 138 di recepimento della Direttiva NIS2 con specifico riferimento all'art.23 che attribuisce specifiche responsabilità agli organi di amministrazione e direttivi, nonché l'art.24 circa gli obblighi in materia di misure di gestione dei rischi per la sicurezza informatica e le Determinazioni di ACN, identifica ASIT come funzione deputata alla gestione operativa della cybersicurezza curando l'attuazione della normativa applicabile, identificando pertanto anche il Punto di Contatto e conferendo specifico mandato al Dirigente ASIT per l'implementazione delle misure e le politiche approvate e la comunicazione alle strutture impattate, nonché ove necessario a tutta la popolazione dell'Ateneo, prevedendo al contempo una revisione periodica almeno biennale o in occasione di eventi significativi quali incidenti di sicurezza, variazioni organizzative o mutamenti dell'esposizione ai rischi.

5.2 Il sistema di Monitoraggio e Controllo

L'efficacia del sistema di governance richiede un costante monitoraggio delle misure implementate e una verifica periodica del loro adeguamento ai rischi emergenti. Il Dirigente ASIT assicura il monitoraggio periodico dell'efficacia delle misure adottate, valutando i tempi di risposta agli incidenti di sicurezza e di risoluzione dei medesimi, il livello di copertura formativa del personale e il grado di conformità complessivo alle normative vigenti.

Il reporting periodico al Magnifico Rettore, al Direttore Generale, al Consiglio di Amministrazione e al Senato Accademico sullo stato di implementazione delle politiche e dei principi ivi definiti garantisce che questi mantengano piena visibilità sull'evoluzione del sistema di sicurezza, mentre la segnalazione tempestiva di incidenti significativi, criticità o necessità di aggiornamento delle politiche consente interventi correttivi tempestivi. Il coordinamento delle attività di verifica e audit completa il quadro dei controlli, assicurando che il sistema mantenga nel tempo la propria efficacia e adeguatezza.

5.3 L'aggiornamento e la revisione

La natura evolutiva delle minacce informatiche e del contesto normativo richiede che il sistema di governance mantenga caratteristiche di flessibilità e adattabilità; pertanto, il sistema adottato per la gestione della cybersicurezza è soggetta a revisione periodica, oltre che a revisioni straordinarie in caso di modifiche normative significative, incidenti di sicurezza di particolare rilevanza, riorganizzazioni aziendali sostanziali o variazioni significative del profilo di rischio di Cybersecurity.

In particolare, il Modello organizzativo è soggetto a revisione:

1. nel caso in cui si verifichino:
 - Incidenti significativi;



Modello organizzativo

- Variazioni organizzative;
- Mutamenti dell'esposizione alle minacce e ai relativi rischi;
- Mutamenti del contesto normativo applicabile (es. nuove determinazioni ACN con ulteriori misure);

2. In ogni caso almeno ogni due anni dall'approvazione.

Il processo di aggiornamento segue il medesimo iter di approvazione definito per l'adozione iniziale, garantendo la continuità e la coerenza del sistema di governance della Cybersecurity. Questo approccio assicura che il framework rimanga sempre aggiornato per garantire la stabilità necessaria per un'efficace implementazione operativa delle misure di sicurezza a livello di Ateneo.