POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

(RIFERIMENTO ISO 27001:2022 – Punto norma 5.2)

INDICE

1. Premessa 3
2. Ambito di applicabilità e approvazione 3
3. Oggetto e finalità 3
4. Riferimenti normativi, definizioni e acronimi 4
5. Ruoli, responsabilità e autorità 5
   5.1. Organi di governo e Direzione 5
   5.2. Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni 6
   5.3. Funzioni operative nell'ambito della Sicurezza delle Informazioni 7
   5.4. Direttori di Dipartimento 9
   5.5. Responsabili di area a Perimetro SGSI 9
   5.5.1. Responsabile della Funzione Didattica 9
   5.5.2. Responsabile della Funzione di Ricerca 10
   5.6. Utenti 10
6. Disposizioni in materia di Sicurezza delle Informazioni 10
   6.1. Principi 11
   6.2. Obiettivi 12
7. Governo e organizzazione della sicurezza delle informazioni 13
   7.1. Organizzazione della sicurezza delle informazioni 13
   7.2. Sicurezza delle risorse umane 13
   7.3. Formazione, informazione e consapevolezza 14
8. Gestione della sicurezza delle informazioni 15
   8.1. Procedure operative di sicurezza 15
   8.2. Gestione delle risorse ICT 15
   8.3. Gestione Identità e accessi logici 16
   8.4. Misure di sicurezza fisica e ambientale 17
   8.5. Sicurezza delle reti 17
   8.6. Sviluppo, acquisizione e manutenzione delle risorse ICT 18
   8.7. Gestione dei progetti e dei cambiamenti ICT 19
   8.8. Gestione e sicurezza delle attività operative ICT 20

8.9. Gestione degli incidenti di sicurezza delle informazioni 21
8.10. Gestione della Continuità Operativa 21
8.11. Gestione della sicurezza delle informazioni nelle relazioni con i fornitori 22
8.12. Gestione della sicurezza delle informazioni nei rapporti con soggetti esterni 23
9. Monitoraggio, audit e miglioramento continuo 23
9.1. Monitoraggio e misurazione 24
9.2. Audit interni 24
9.3. Riesame della Direzione 24
9.4. Gestione delle non conformità e azioni correttive 24
10. Documentazione di supporto 25
11. Modalità di diffusione, recepimento e aggiornamento della Politica 25

1. Premessa

Il Politecnico di Bari, al fine di garantire una gestione efficace e coerente della sicurezza delle informazioni e della continuità operativa, in conformità e nell'adempimento di quanto descritto dallo Standard ISO/IEC 27001:2022, definisce nel presente documento i principi, i ruoli e le responsabilità del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI).

Quanto descritto nel presente documento, e in ogni altro elemento documentale o organizzativo del Sistema di Gestione per la Sicurezza delle Informazioni, non esaurisce gli obblighi, le responsabilità e gli adempimenti in capo al Politecnico di Bari per quanto riguarda normative, comunque applicabili all'ambito in oggetto (es. Reg EU/2016/679 – GDPR).

La declinazione operativa dei compiti e delle responsabilità è formalizzata nel documento di "Modello Organizzativo del Sistema di Gestione della Sicurezza delle Informazioni"[1] adottato dall'Ateneo, che ne assicura la chiara attribuzione e tracciabilità, anche mediante l'utilizzo di strumenti di rappresentazione, quali la matrice RACI ad esso allegata.

La struttura organizzativa del SGSI e la relativa assegnazione di ruoli e responsabilità sono sottoposte all'approvazione del Direttore Generale.

La presente Politica è elaborata in conformità ai principi e ai requisiti della norma ISO/IEC 27001:2022, è sviluppata in coerenza con il contesto normativo, istituzionale e organizzativo del Politecnico di Bari e si applica al perimetro del SGSI così come formalmente definito nel documento di "Campo di Applicazione e Perimetro" adottato dall'Ateneo.

2. Ambito di applicabilità e approvazione

La presente Politica per la Sicurezza delle Informazioni, nell'ambito del SGSI, si applica a tutte le informazioni trattate dal Politecnico di Bari, indipendentemente dal formato e dal supporto utilizzato, nonché alle risorse ICT e ai processi che ne consentono la gestione.

Essa si applica a tutto il personale dell'Ateneo, nonché a tutti i soggetti esterni che, a qualsiasi titolo, accedono o trattano informazioni e risorse ICT del Politecnico di Bari, inclusi fornitori, partner, clienti e altri soggetti terzi.

Nell'individuazione del perimetro del Sistema di Gestione per la Sicurezza delle Informazioni, il Politecnico ha definito il seguente Campo di Applicazione: "Erogazione dei servizi relativi alle attività di didattica e di ricerca, incluse la progettazione ed erogazione dell'offerta formativa, i servizi agli studenti e le attività di ricerca scientifica, e gestione delle informazioni e dei sistemi informativi a supporto delle strutture afferenti alla Direzione Servizi agli Studenti, Sistema Bibliotecario, Campus Life, Centro Linguistico di Ateneo e alla Direzione Ricerca, Internazionalizzazione e Interazione con il Territorio del Politecnico di Bari".

La presente Politica è approvata dal Consiglio di Amministrazione.

3. Oggetto e finalità

La presente politica definisce gli indirizzi e i principi adottati dal Politecnico di Bari al fine di garantire la sicurezza delle informazioni, in qualunque forma esse siano rappresentate e trattate, sia su supporto cartaceo sia su supporto elettronico.

La Politica è finalizzata ad assicurare un'adeguata protezione delle informazioni lungo l'intero ciclo di vita delle stesse, inclusi i processi di creazione, utilizzo, conservazione, trasmissione e archiviazione, attraverso misure idonee a tutelarne in particolare:

[1] Inserire Rif. Documento/Protocollo

- Riservatezza (o confidenzialità), intesa come la garanzia che le informazioni siano accessibili esclusivamente a soggetti e/o processi debitamente autorizzati;
- Integrità, intesa come la salvaguardia dell'accuratezza e della completezza delle informazioni e dei metodi di trattamento associati;
- Disponibilità, intesa come la garanzia che le informazioni e i servizi informativi siano accessibili e utilizzabili quando richiesto dai soggetti autorizzati;
- Autenticità, intesa come la garanzia dell'identità dei soggetti che accedono alle informazioni e dell'origine delle stesse;
- Accountability (responsabilità), intesa come la possibilità di attribuire in modo chiaro e tracciabile le azioni compiute sui sistemi e sulle informazioni ai soggetti responsabili.

I contenuti della presente Politica devono essere comunicati, conosciuti e adottati da tutti i soggetti interni ed esterni coinvolti, a qualsiasi titolo, nella gestione delle informazioni e dei sistemi informativi del Politecnico di Bari, incluse le parti interessate e i fornitori.

La violazione dei principi della presente Politica può comportare conseguenze in relazione alle responsabilità previste dalla normativa vigente, dai regolamenti interni dell'Ateneo e dagli obblighi contrattuali applicabili. Eventuali violazioni sono gestite secondo le modalità definite dal SGSI e dalle procedure interne del Politecnico di Bari.

4. Riferimenti normativi, definizioni e acronimi

La presente Politica è definita in conformità ai requisiti della normativa e degli standard applicabili in materia di sicurezza delle informazioni e, in particolare, fa riferimento a:

- ISO/IEC 27001:2022 - *Information security, cybersecurity and privacy protection – Information security management systems – Requirements*.
- ISO/IEC 27002:2022– *Information security, cybersecurity and privacy protection – Information security controls*.
- ISO/IEC 27005 – *Information security risk management*
- D.lgs. 196/2003 e s.m.i. – Codice in materia di protezione dei dati personali
- Direttiva (UE) 2022/2555 (NIS2) – Misure per un livello comune elevato di cibersicurezza nell'Unione europea
- Regolamento (UE) 2016/679 (GDPR) – Regolamento generale sulla protezione dei dati personali
- Linee guida e provvedimenti del Garante per la protezione dei dati personali
- Linee guida AgID in materia di sicurezza ICT
- Regolamenti, linee guida e disposizioni interne del Politecnico di Bari applicabili ai processi di didattica e ricerca

Eventuali ulteriori riferimenti normativi e documentali applicabili sono riportati nei documenti di supporto richiamati dalla presente Politica.

Ai fini della presente Politica si elencano le seguenti definizioni:

- **Dati personali:** Qualsiasi informazione riguardante una persona fisica identificata o identificabile, ai sensi dell'articolo 4 del Regolamento (UE) 2016/679 (GDPR).
- **Categorie particolari di dati personali:** Dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale, ai sensi dell'articolo 9 del Regolamento (UE) 2016/679 (GDPR).
- **Dati giudiziari:** Dati personali relativi a condanne penali e reati o a misure di sicurezza connesse a condanne penali, ai sensi dell'articolo 10 del Regolamento (UE) 2016/679 (GDPR).

- **Incidente di sicurezza delle informazioni:** Evento singolo o serie di eventi indesiderati o inattesi che compromettono, o possono compromettere, la riservatezza, l'integrità o la disponibilità delle informazioni.
- **Informazione:** Qualunque dato o insieme di dati, in qualsiasi forma o supporto, rilevante per le attività di didattica e ricerca del Politecnico di Bari.
- **Parte interessata:** Soggetto interno o esterno che può influenzare o essere influenzato dalla sicurezza delle informazioni.
- **Sicurezza delle informazioni:** Preservazione della riservatezza, dell'integrità e della disponibilità delle informazioni.
- **Sistema di Gestione per la Sicurezza delle Informazioni (SGSI / ISMS):** Insieme di politiche, processi, procedure, risorse e controlli adottati per gestire e migliorare la sicurezza delle informazioni.

Per i termini non espressamente definiti nel presente documento si applicano le definizioni contenute nella norma ISO/IEC 27001 e nei documenti di riferimento del Sistema di Gestione per la Sicurezza delle Informazioni.

Nel presente documento sono utilizzati i seguenti acronimi, il cui significati è riportato di seguito.

- **CIA** – Confidentiality, Integrity, Availability (Riservatezza, Integrità, Disponibilità)
- **GDPR** – General Data Protection Regulation
- **ICT** – Information and Communication Technology
- **SGSI / ISMS** –Sistema di Gestione per la Sicurezza delle Informazioni
- **RSGSI** – Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni
- **ISO** – International Organization for Standardization
- **IEC** – International Electrotechnical Commission

5. Ruoli, responsabilità e autorità

5.1. Organi di governo e Direzione

- **Consiglio di Amministrazione**

Definisce e approva la presente Politica per la Sicurezza delle Informazioni, nonché i suoi eventuali aggiornamenti e revisioni successive, assicurandone l'allineamento agli obiettivi strategici, organizzativi e di business del Politecnico di Bari. In tale ambito, ove lo ritenesse opportuno, il Consiglio di Amministrazione può richiedere, per quanto di competenza, il parere consultivo del Senato Accademico.

Il Consiglio di Amministrazione assicura inoltre l'applicazione della presente Politica e delle linee guida in essa contenute, promuovendone la diffusione all'interno dell'organizzazione e vigilando sulla sua effettiva attuazione. A tal fine, procede al riesame periodico della Politica e del relativo quadro di riferimento, con l'obiettivo di verificarne nel tempo l'adeguatezza, l'efficacia e la continua coerenza con il contesto interno ed esterno, con l'evoluzione dei rischi per la sicurezza delle informazioni e con gli indirizzi strategici del Politecnico di Bari.

- **Direttore Generale**

Sottopone la presente Politica per la Sicurezza delle Informazioni al Comitato Alta Direzione per le valutazioni di competenza e, successivamente, al Consiglio di Amministrazione per le relative deliberazioni e approvazioni.

Il Direttore Generale assicura inoltre che i contenuti del presente documento siano adeguatamente diffusi, comunicati e resi conoscibili a tutto il personale dell'Ateneo, promuovendone la comprensione e l'applicazione nell'ambito delle attività operative, nel rispetto dei ruoli e delle responsabilità assegnate.

Provvede, altresì, all'approvazione e all'introduzione delle linee guida operative a supporto della presente Politica, assicurandone la coerenza con gli obiettivi di sicurezza delle informazioni e con il sistema di gestione adottato.

- **Comitato Alta Direzione**

Il Comitato Alta Direzione è composto dal Direttore Generale e dai Direttori di Dipartimento.

Il Comitato, qualora emergano argomenti attinenti alla protezione dei dati personali, si avvale del supporto del Responsabile della Protezione dei Dati (DPO) per gli aspetti di competenza e ai fini della conformità alla normativa applicabile.

Il Responsabile del Sistema di Gestione della Sicurezza delle Informazioni (RSGSI) assicura il supporto tecnico e metodologico alle attività del Comitato, partecipando alle relative riunioni e fornendo elementi informativi, analisi e valutazione utili ai fini delle decisioni, in coerenza con il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) e con il contesto normativo e organizzativo dell'Ateneo.

Il Comitato è responsabile della valutazione dell'adeguatezza e dell'efficacia delle misure di protezione previste o ritenute necessarie al fine di garantire appropriati livelli di sicurezza delle informazioni, protezione dei dati personali e continuità operativa, in coerenza con il contesto organizzativo e con i rischi identificati.

Il Comitato svolge, inoltre, la funzione di riesame della direzione (Management Review) del SGSI, valutandone periodicamente le prestazioni e l'efficacia complessiva, nonché le opportunità di miglioramento e l'eventuale necessità di modifiche al sistema, in conformità ai requisiti della normativa applicabile e della norma ISO/IEC 27001.

5.2. Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni

- **ISMS Manager / RSGSI / Responsabile Sicurezza delle Informazioni**

È incaricato di coordinare, implementare e mantenere il Sistema di Gestione per la Sicurezza delle Informazioni in conformità ai requisiti della norma ISO/IEC 27001, alle politiche aziendali e alla normativa applicabile.

In particolare, il Responsabile del SGSI:

- assicura lo sviluppo, l'aggiornamento e l'attuazione delle politiche, delle procedure e dei controlli in materia di sicurezza delle informazioni;
- coordina il processo di valutazione e trattamento dei rischi per la sicurezza delle informazioni, monitorandone l'evoluzione nel tempo;
- verifica l'efficacia delle misure di sicurezza adottate e ne propone il miglioramento continuo;
- supporta la gestione degli incidenti di sicurezza delle informazioni, incluse le attività di analisi, risposta e reporting;
- fornisce supporto al Comitato di Alta Direzione e agli organi competenti nello svolgimento delle attività di riesame del Sistema di Gestione della Sicurezza delle Informazioni (SGSI), contribuendo a facilitare i processi decisionali, evidenziando eventuali aree di miglioramento e supportando l'individuazione di azioni correttive e di sviluppo del sistema, in coerenza con gli obiettivi strategici e con i requisiti normativi applicabili;
- collabora con le funzioni aziendali interessate al fine di garantire la corretta integrazione dei requisiti di sicurezza delle informazioni nei processi aziendali;
- supporta le attività di audit interni ed esterni relative al SGSI e contribuisce alla preparazione dei riesami di direzione.

5.3. Funzioni operative nell'ambito della Sicurezza delle Informazioni

Al fine di assicurare una gestione efficace della sicurezza delle informazioni e della continuità operativa, il Politecnico di Bari ha individuato specifiche funzioni nell'ambito del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), alle quali sono assegnate le principali responsabilità e attività in materia.

Le funzioni descritte di seguito definiscono ambiti di responsabilità del SGSI, concepiti in modo flessibile e non necessariamente coincidenti con strutture organizzative o ruoli formalmente istituiti. La declinazione operativa dei compiti e delle responsabilità è formalizzata all'interno del Modello Organizzativo [NOME DOCUMENTO], anche mediante l'adozione di una Matrice RACI, al fine di garantire chiarezza nei ruoli e nelle responsabilità. La relativa struttura organizzativa e le sue eventuali modifiche sono soggette ad approvazione da parte della Direzione Generale. Tale impostazione consente una maggiore adattabilità al contesto organizzativo e alle esigenze operative.

Le attività sono svolte da personale incaricato all'interno del Politecnico di Bari, individuato in base a competenze e responsabilità, con la possibilità di presidiare anche più ambiti funzionali in un'ottica di integrazione ed efficienza.

- **Funzione Governo della Sicurezza e della Continuità Operativa**

Assicura le attività di governo e di coordinamento delle attività connesse alla gestione della continuità operativa e della sicurezza delle informazioni del Politecnico di Bari, indirizzando le attività svolte dalle competenti strutture.

- **Funzione Sicurezza delle Informazioni**

Provvede alla definizione delle Linee Guida e delle policy del Politecnico di Bari in materia di sicurezza delle informazioni e sicurezza informatica, operando in coordinamento con le altre funzioni aziendali interessate, al fine di garantire un approccio omogeneo e coerente alla gestione della sicurezza.

La Funzione supporta le strutture competenti nell'individuazione e nella definizione degli interventi di sicurezza delle informazioni necessari a contenere il profilo di rischio entro i livelli definiti e accettati dal Politecnico di Bari. In tale ambito, contribuisce alla diffusione delle migliori pratiche e al rafforzamento dei presidi di sicurezza.

La Funzione definisce, i criteri per il censimento e la classificazione delle informazioni e degli asset ICT e fornisce supporto nella definizione degli scenari di rischio, delle librerie delle minacce e dei relativi controlli di sicurezza.

Collabora inoltre con la Funzione Risorse Umane alla definizione dei piani formativi in relazione ai fabbisogni in materia di sicurezza delle informazioni, includendo programmi periodici di formazione e sensibilizzazione finalizzati ad accrescere la consapevolezza del personale.

La Funzione riferisce, almeno con frequenza annuale, al Comitato Sicurezza, Protezione dei Dati Personali e Continuità Operativa (CSCO) in merito allo stato delle attività svolte e all'evoluzione del livello di sicurezza delle informazioni.

- **Funzione ICT**

Concorre, di concerto con la Funzione Sicurezza delle Informazioni, alla definizione della presente Politica e dei suoi successivi aggiornamenti, assicurandone la coerenza con il sistema complessivo di gestione dei rischi del Politecnico di Bari.

La Funzione è responsabile dell'identificazione e della valutazione dei rischi ICT e di sicurezza, inclusi quelli connessi a modifiche di sistemi e servizi ICT nonché a progetti ICT rilevanti, assicurando un presidio continuo dell'evoluzione del profilo di rischio.

Sulla base degli esiti delle analisi e delle verifiche condotte, propone alle funzioni competenti gli interventi di sicurezza delle informazioni necessari a mantenere il rischio entro i livelli definiti e accettati, monitorando l'avanzamento e l'efficace attuazione delle attività conseguenti.

La Funzione contribuisce alla definizione dei criteri per il censimento e la classificazione degli asset ICT, acquisendone e valutandone i risultati e fornendo, per quanto di competenza, supporto specialistico alle strutture tecniche coinvolte. Definisce inoltre, di concerto con la Funzione Sicurezza delle Informazioni, i criteri per il censimento e la classificazione delle informazioni.

- **Area Chief Information Officer**

Ha la responsabilità di indirizzare, coordinare e governare la definizione delle strategie, delle politiche e delle linee guida in materia di Information and Communication Technology (ICT), assicurando un presidio efficace e coerente del Sistema ICT del Politecnico di Bari.

Nello svolgimento delle proprie responsabilità, l'Area CIO si avvale, per gli ambiti di competenza, del contributo della Funzione ICT, garantendo l'integrazione dei requisiti di sicurezza delle informazioni e di gestione del rischio nelle scelte strategiche e operative in ambito ICT.

- **Funzione Incident Management**

Ha la responsabilità di seguire, supportare e monitorare l'intero processo di gestione degli incidenti, inclusi gli incidenti di sicurezza delle informazioni.

La Funzione assicura il coordinamento delle attività di rilevazione, analisi, risposta e risoluzione degli incidenti, nonché il monitoraggio delle azioni correttive e preventive, contribuendo alla riduzione dell'impatto degli eventi e al miglioramento continuo dei presidi di sicurezza.

- **Funzione ICT Compliance**

Garantisce, per quanto di competenza, il monitoraggio continuo dell'adeguatezza e dell'efficacia delle misure di sicurezza adottate dal Politecnico di Bari.

La Funzione monitora inoltre l'evoluzione del quadro normativo e regolamentare applicabile, effettuando le opportune analisi dei requisiti in ambito sicurezza delle informazioni e valutandone l'impatto sui processi, sui sistemi e sulle attività del Politecnico di Bari, supportando le strutture competenti nell'adeguamento ai requisiti applicabili.

- **Funzione Data Protection Officer**

Verifica periodicamente, per gli ambiti di propria competenza, l'adeguatezza delle misure di sicurezza adottate a protezione dei dati personali.

La Funzione svolge il ruolo di punto di contatto per le questioni connesse al trattamento dei dati personali e collabora con la Funzione ICT al fine di identificare e valutare i rischi per i diritti e le libertà degli interessati, contribuendo all'individuazione delle misure di mitigazione più idonee.

- **Funzione Audit ICT**

Verifica l'adeguatezza, l'affidabilità e la sicurezza del Sistema Informativo del Politecnico di Bari, valutando l'efficacia dei controlli e dei presidi adottati in ambito ICT e sicurezza delle informazioni.

Le attività di audit contribuiscono a fornire alla Direzione e agli organi di governo una valutazione indipendente sul livello di controllo del Sistema Informativo e sul grado di conformità alle politiche, alle procedure interne e ai requisiti normativi applicabili.

- **Funzione Risorse Umane**

Contribuisce alla tutela della sicurezza delle informazioni attraverso la gestione dei profili professionali, delle competenze e dei percorsi formativi del personale.

Nell'ambito dei processi di selezione e inserimento delle risorse, la Funzione verifica l'idoneità dei candidati rispetto al ruolo da ricoprire e, ove necessario, le competenze tecniche in materia di sicurezza delle informazioni, in coerenza con i requisiti previsti per le posizioni che comportano l'accesso a informazioni e asset critici.

Collabora con le funzioni competenti nell'individuazione delle esigenze di sviluppo delle competenze.

- **Funzione Formazione**

Definisce e pianifica, almeno con cadenza annuale e in coordinamento con la Funzione Sicurezza delle Informazioni, i programmi di formazione e le iniziative di sensibilizzazione in materia di sicurezza delle informazioni, assicurandone la coerenza con gli obblighi normativi, i requisiti interni e i rischi identificati.

Garantisce l'erogazione dei programmi formativi e delle attività di sensibilizzazione, monitorandone lo stato di attuazione e l'efficacia.

Contribuisce alla diffusione della cultura della sicurezza all'interno dell'organizzazione, promuovendo la consapevolezza del personale rispetto ai rischi e alle responsabilità connesse alla gestione delle informazioni.

- **Funzione Gestione degli Accessi Fisici**

È responsabile dell'esecuzione delle attività operative specialistiche in materia di controllo degli accessi fisici.

La Funzione presidia la gestione del rischio di sicurezza fisica e/o operativo associato agli ambienti, alle infrastrutture e agli asset aziendali, definendo e attuando l'impianto di misure e controlli volto a prevenire e mitigare le minacce rilevanti, in coerenza con le politiche e le linee guida di sicurezza adottate dal Politecnico di Bari.

Nello svolgimento delle proprie attività, la Funzione assicura il rispetto dei requisiti di sicurezza applicabili e collabora con le altre funzioni competenti al fine di garantire un adeguato livello di protezione degli ambienti e degli asset critici.

5.4. Direttori di Dipartimento

Assicurano, per quanto di competenza, l'attuazione della presente Politica nell'ambito delle strutture organizzative di riferimento, promuovendo comportamenti coerenti con i principi di sicurezza delle informazioni e garantendo il rispetto delle disposizioni applicabili.

5.5. Responsabili di area a Perimetro SGSI

I Responsabili delle funzioni di Didattica e Ricerca sono richiamati nel presente documento esclusivamente in quanto afferenti a processi e attività ricompresi nel perimetro del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI).

Il loro coinvolgimento è pertanto da intendersi limitato agli ambiti di competenza, in coerenza con il modello organizzativo adottato dall'Ateneo.

5.5.1. Responsabile della Funzione Didattica

Collabora, per quanto di competenza, all'attuazione dei requisiti di sicurezza delle informazioni applicabili nell'ambito delle attività didattiche, operando in coerenza con le disposizioni del SGSI e fornendo supporto informativo e operativo ove richiesto.

Fornisce, nell'ambito delle attività di propria competenza, le informazioni necessarie a garantire che l'accesso alle informazioni e ai sistemi informativi sia coerente con le esigenze operative e con i principi di

necessità di conoscere e minimo privilegio, e contribuisce alla gestione degli incidenti di sicurezza delle informazioni, segnalando eventuali eventi o anomalie rilevanti.

5.5.2. Responsabile della Funzione di Ricerca

Collabora, per quanto di competenza, all'attuazione dei requisiti di sicurezza delle informazioni applicabili nell'ambito delle attività di ricerca, operando in coerenza con le disposizioni del SGSI e fornendo supporto informativo e operativo ove richiesto, con particolare attenzione alla protezione dei dati di ricerca e delle informazioni sensibili trattate nell'ambito dei progetti.

Fornisce, nell'ambito delle attività di propria competenza, le informazioni necessarie a garantire che l'accesso alle informazioni e ai sistemi informativi sia coerente con le esigenze operative e con i principi di necessità di conoscere e minimo privilegio, e contribuisce alla gestione degli incidenti di sicurezza delle informazioni, segnalando eventuali eventi o anomalie rilevanti.

5.6. Utenti

Gli Utenti comprendono tutti i soggetti che, a qualsiasi titolo, accedono o trattano informazioni e risorse ICT del Politecnico di Bari, inclusi, a titolo esemplificativo e non esaustivo, docenti, ricercatori, studenti, dottorandi, borsisti, personale tecnico-amministrativo e bibliotecario, nonché soggetti esterni quali ospiti, partner di ricerca, aziende ed enti istituzionali.

Gli sono responsabili di un utilizzo corretto e sicuro delle informazioni e delle risorse ICT, in conformità ai ruoli, alle autorizzazioni assegnate e alle politiche e procedure in vigore.

Gli Utenti contribuiscono alla salvaguardia della riservatezza, dell'integrità e della disponibilità delle informazioni e rispettano le misure di sicurezza e le disposizioni operative adottate dall'Ateneo.

Essi sono inoltre tenuti a segnalare tempestivamente alle strutture competenti eventuali incidenti, anomalie o situazioni che possano compromettere la sicurezza delle informazioni.

Il Politecnico di Bari promuove la consapevolezza degli Utenti in materia di sicurezza delle informazioni attraverso attività di informazione e formazione, al fine di favorire comportamenti responsabili e ridurre i rischi connessi all'utilizzo delle informazioni e delle risorse ICT.

6. Disposizioni in materia di Sicurezza delle Informazioni

Il Politecnico di Bari promuove le proprie attività ponendo al centro del proprio agire la persona e la comunità accademica e istituzionale, comprendente studenti, personali, collaboratori e altri soggetti interessati; il suo impegno costante è diretto a garantire servizi e attività istituzionali, amministrative e gestionali capaci di produrre valore pubblico, sociale e culturale per la collettività.

In tale contesto, il Politecnico di Bari reputa essenziale adottare, nello svolgimento delle proprie attività, i principi espressi dalla presente Politica al fine di perseguire l'obiettivo di assicurare la protezione delle informazioni e dei dati personali in linea con gli obiettivi istituzionali, con l'approccio alla gestione dei rischi e in conformità anche ai requisiti legali, normativi e contrattuali applicabili, tenendo altresì conto delle esigenze delle terze parti interessate.

Il Politecnico di Bari intende proteggere le informazioni e i dati personali definendo un sistema di governo della sicurezza delle informazioni costituito da politiche, processi e misure organizzative, tecnologiche e fisiche da mettere in atto. La realizzazione di tale sistema di governo tiene conto della natura pubblica dell'Ateneo, della complessità e del profilo di rischio dei processi e dei servizi svolti, dell'evoluzione del contesto interno ed esterno e delle esigenze delle parti interessate. Tali requisiti sono identificati e aggiornati anche in funzione dei risultati dell'analisi dei rischi ICT e di sicurezza che, effettuata almeno annualmente e,

comunque, in occasione di cambiamenti di contesto organizzativi e/o tecnologici, consente di acquisire consapevolezza sul livello di esposizione al rischio del sistema informativo dell'Ateno, a partire da:

- valutazione iniziale del rischio potenziale, effettuata sulla base dell'impatto che può derivare dalla mancata applicazione di misure di sicurezza alle informazioni e ai sistemi informativi e della probabilità di effettivo sfruttamento delle vulnerabilità esistenti;
- valutazione del livello di adeguatezza del sistema dei controlli di sicurezza;
- valutazione del rischio residuo, inteso come la componente di rischio non adeguatamente mitigata dalle misure di sicurezza adottate;
- analisi del rischio residuo e identificazione di ulteriori azioni di mitigazione, necessarie qualora il livello di rischio residuo ecceda la soglia di accettabilità del rischio definita dal Politecnico

I risultati della valutazione dei rischi ICT e di sicurezza, ai quali sono esposti i processi, servizi e asset di supporto, supportano la fase di determinazione delle azioni e delle misure di sicurezza da intraprendere al fine di contenere o ridurre il rischio residuo entro la soglia di accettabilità stabilita dall'Ateneo.

Devono essere quindi definite e attuate misure di sicurezza preventive per mitigare i rischi ICT e di sicurezza, al fine di proteggere il patrimonio informativo in accordo con la sua classificazione.

Tali misure devono comprendere attività e processi inerenti all'ambito organizzativo, tecnologico e fisico.

Le misure di sicurezza devono essere adeguatamente documentate, e aggiornate sulla base di quanto appreso e formalizzato durante la loro implementazione e delle attività di monitoraggio e riesame del SGSI.

6.1. Principi

Per orientare le diverse iniziative di protezione e, più in generale, i comportamenti di tutto il personale, a diverso titolo coinvolto nella gestione delle informazioni dell'Ateneo e dei dati personali, il Politecnico di Bari ritiene opportuno adottare i seguenti principi:

- i servizi, i processi e le attività dell'Ateneo, nonché le relative informazioni trattate, devono essere formalmente censiti e classificati secondo la loro criticità sulla base dei criteri di riservatezza, integrità e disponibilità;
- sulla base del censimento di cui al punto precedente, deve essere effettuata, periodicamente e comunque in presenza di situazioni che possono influire sul complessivo livello di rischio, un'attività di identificazione e valutazione dei rischi connessi alla sicurezza delle informazioni trattate (analisi dei rischi), che includa gli scenari di rischi informatici e di rischi cyber;
- in base ai risultati della valutazione dei rischi, devono essere identificate le corrette opzioni di trattamento e, eventualmente, adottati opportuni controlli. Tali controlli devono garantire adeguati livelli di protezione nei confronti delle minacce considerate rilevanti (eventi naturali, frodi, errori, etc.) per la specifica informazione e per ogni possibile contesto in cui l'informazione viene trattata. In ogni caso il livello di protezione identificato deve risultare conforme alle disposizioni normative esterne applicabili, nonché ai regolamenti e alle politiche interni dell'Ateneo;
- i presidi progettati ed attivati devono risultare allineati allo stato delle tecnologie e delle best practices di riferimento per il settore, tenuto conto del bilanciamento tra il costo della protezione, il rischio connesso e il livello di accettabilità del rischio definito e approvato dall'Ateneo;
- le responsabilità di gestione delle informazioni devono essere formalmente assegnate e includere, tra le altre, l'analisi della rilevanza/criticità di ciascuna informazione e la conseguente definizione dei criteri di protezione, qualità, ritenzione, concessione delle autorizzazioni di uso. Le strutture dell'Ateneo responsabili dei processi che trattano le informazioni hanno il compito di fornire indicazioni che le strutture tecniche adottano per progettare, implementare e gestire i necessari presidi organizzativi, applicativi e di sistema al fine di proteggere le informazioni;

- tutto il personale deve operare in modo da salvaguardare la riservatezza, l'integrità e la disponibilità delle informazioni gestite, nonché ridurre i rischi a cui le stesse sono esposte. Devono essere individuati i fabbisogni formativi e informativi in modo da realizzare programmi di formazione e sensibilizzazione adeguati ai diversi destinatari e coerenti con gli obiettivi formativi definiti dall'Ateneo;
- deve essere garantita la conformità alle disposizioni normative (nazionali, europee e internazionali), in materia di sicurezza delle informazioni, di protezione dei dati personali e di cybersecurity, nonché il rispetto degli impegni di sicurezza delle informazioni stabiliti nei contratti e negli accordi con le terze parti;
- deve essere perseguito il miglioramento continuo della sicurezza delle informazioni, al fine di assicurare l'allineamento agli standard internazionali e alle migliori pratiche di riferimento.

La conformità alle misure di sicurezza contenute nella presente Politica è da considerarsi obbligatoria, con un livello di dettaglio proporzionato alle informazioni trattate, alle risorse ICT e ai processi che ne supportano il trattamento nonché alla natura, allo scopo, alla complessità e alla rischiosità dei servizi e delle attività dell'Ateneo.

I principi di sicurezza esposti nella presente Politica devono essere garantiti, sulla base di specifici accordi contrattuali o di esternalizzazione, anche in caso di affidamento a terzi di attività, risorse ICT o servizi che comportino il trattamento di informazioni dell'Ateneo

6.2. Obiettivi

Gli obiettivi sono orientati a garantire un adeguato livello di protezione delle informazioni trattate, assicurandone riservatezza, integrità e disponibilità, nonché a promuovere il miglioramento continuo delle misure organizzative e tecniche adottate. In tale quadro, l'organizzazione si impegna a tradurre gli obiettivi generali in traguardi misurabili, periodicamente riesaminati dalla Direzione, affinché la sicurezza delle informazioni supporti in modo efficace i processi di business e la tutela degli stakeholder.

In particolare, gli obiettivi target del Politecnico di Bari sono:

- garantire un'immagine di affidabilità e trasparenza istituzionale in termini di protezione del patrimonio informativo trattato e di misure di sicurezza adottate;
- garantire le risorse necessarie (umane, economiche e infrastrutturali) per il raggiungimento degli obiettivi di sicurezza delle informazioni;
- definire i ruoli e le responsabilità per lo sviluppo e il mantenimento della sicurezza delle informazioni;
- aumentare, nel proprio personale, e nei fornitori esterni, il livello di consapevolezza e la cultura sulla sicurezza delle informazioni, anche al fine di prevenire e ridurre al minimo l'impatto degli incidenti volontari o accidentali;
- assicurare la protezione delle informazioni dell'Ateneo e dei dati personali in coerenza con gli obiettivi istituzionali e con l'approccio alla gestione dei rischi, tutelando i diritti e le libertà delle persone fisiche;
- contenere il rischio di sicurezza delle informazioni, attraverso la definizione e l'implementazione di un framework integrato per la gestione dei rischi ICT e di sicurezza delle informazioni;
- disporre di processi e controlli adeguati a garantire che tutti i rischi ICT e di sicurezza siano identificati, analizzati, misurati, monitorati, gestiti e opportunamente segnalati;
- garantire che la Politica in materia di sicurezza delle informazioni sia integrata in tutti i processi dell'Ateneo e che le procedure ed i controlli siano definiti coerentemente con essa e attuati in modo efficace;
- garantire la definizione e l'attuazione di adeguate misure di controllo degli accessi logici ai sistemi e alle informazioni;

- garantire che l'accesso alle sedi e ai singoli locali dell'Ateneo sia consentito esclusivamente a personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti;
- garantire l'individuazione dei requisiti di sicurezza delle informazioni da prevedere per contrastare rischi specifici con impatto sulla riservatezza, integrità e disponibilità dei dati, sin dalle fasi di progettazione e sviluppo di nuovi servizi, sistemi o soluzioni;
- garantire che le anomalie e gli incidenti con impatto sul sistema informativo e sui livelli di sicurezza delle informazioni siano tempestivamente riconosciuti e correttamente gestiti attraverso adeguati processi di rilevazione, comunicazione e intervento, al fine di minimizzarne gli effetti;
- garantire la continuità operativa, prevenendo e minimizzando eventuali interruzioni delle attività dell'Ateneo anche in condizioni critiche o di emergenza;
- garantire il perseguimento degli obiettivi espressi nella presente Politica e l'efficace attuazione delle disposizioni previste per la protezione delle informazioni e delle risorse ICT che le trattano anche in caso di ricorso a fornitori esterni;
- monitorare l'esposizione alle minacce per la sicurezza delle informazioni anche in ottica di prevenzione delle anomalie e degli incidenti di sicurezza.

7. Governo e organizzazione della sicurezza delle informazioni

Il Politecnico di Bari definisce un modello di governo e di organizzazione della sicurezza delle informazioni finalizzato a garantire il coordinamento, il controllo e l'efficace attuazione delle misure di sicurezza, in coerenza con gli obiettivi istituzionali dell'Ateneo e con i principi stabiliti dalla presente Politica.

Il governo della sicurezza delle informazioni si fonda su una chiara attribuzione dei ruoli, responsabilità e autorità, nonché su un adeguato coinvolgimento degli organi di governo, delle strutture organizzative e delle funzioni competenti, al fine di assicurare un approccio sistematico e integrato alla gestione della sicurezza delle informazioni.

Le attività di governo e coordinamento della sicurezza delle informazioni sono assicurate dalla Funzione Governo della Sicurezza e della Continuità Operativa.

7.1. Organizzazione della sicurezza delle informazioni

I ruoli e le responsabilità relativi alla sicurezza delle informazioni sono definiti in conformità alla normativa vigente e agli standard di riferimento in materia di sicurezza delle informazioni, al fine di garantire il corretto recepimento della presenta Politica, nonché l'attuazione e il monitoraggio delle misure di sicurezza in essa previste.

Le strutture e le funzioni dell'Ateno sono responsabili dell'applicazione delle misure di sicurezza nell'ambito dei rispettivi processi e attività, mentre il coordinamento complessivo della sicurezza delle informazioni è assicurato dalla Funzione Sicurezza delle Informazioni, che supporta la Direzione nel governo del SGSI e nel monitoraggio della sua efficacia.

7.2. Sicurezza delle risorse umane

Il personale del Politecnico di Bari (dipendenti e collaboratori esterni) deve comprendere ed essere consapevole delle proprie responsabilità in materia di sicurezza delle informazioni e deve, altresì, risultare idoneo a ricoprire i ruoli per i quali viene preso in considerazione e che gli sono affidati.

Con riferimento al personale dipendente, la struttura competente in materia di Risorse Umane dell'Ateneo ha il compito di curare, nell'ambito delle procedure di reclutamento e selezione previste dalla normativa vigente,

la verifica delle caratteristiche di idoneità dei candidati all'impiego. Tali verifiche devono essere effettuate in proporzione alle esigenze dell'Ateneo, al livello di classificazione delle informazioni di cui è previsto il trattamento nel corso dell'impiego e ai rischi connessi al ruolo previsto.

Gli accordi contrattuali con il personale dipendente e con i collaborati esterni devono applicare le misure di sicurezza delle informazioni in conformità con le politiche e le procedure stabilite dall'Ateneo.

Il Politecnico di Bari prevede l'applicazione di misure e sanzioni nei confronti di chi commette violazioni delle regole previste nell'ambito della normativa interna in materia di sicurezza delle informazioni, in coerenza con quanto previsto dal sistema disciplinare e dai regolamenti vigenti.

In caso di cessazione del rapporto di lavoro o di collaborazione, la struttura competente in materia di risorse umane dell'Ateneo ha il compito di informare tempestivamente le strutture responsabili della sicurezza delle informazioni e della gestione degli accessi fisici e logici, affinché procedano alla tempestiva revoca delle autorizzazioni agli accessi e, ove applicabile, garantiscano la restituzione degli asset assegnati.

Analoga comunicazione dovrà essere effettuata dalla struttura competente in materia di risorse umane anche in occasione di modifiche del rapporto in essere che comportino variazioni rilevanti ai fini degli accessi logici o fisici quali, a titolo esemplificativo e non esaustivo, il cambiamento di incarico o di ruolo, la variazione di appartenenza a strutture organizzative o il cambiamento della sede di lavoro.

7.3. Formazione, informazione e consapevolezza

Il Politecnico di Bari riconosce la formazione, l'informazione e la consapevolezza del personale e dei soggetti esterni come elementi fondamentali per garantire l'efficace attuazione della sicurezza delle informazioni. Il personale dipendente e i fornitori esterni che, a qualsiasi titolo, partecipano alla gestione delle informazioni e dei sistemi informativi dell'Ateneo devono essere adeguatamente formati sulle politiche, sui principi e sulle disposizioni organizzative applicabili, al fine di adempiere correttamente ai compiti e alle responsabilità assegnate.

Le attività di formazione e sensibilizzazione sono finalizzate a ridurre il rischio di errori operativi, abusi, frodi, utilizzi impropri, perdite o compromissioni delle informazioni e a favorire la conoscenza delle modalità di gestione dei rischi relativi alla sicurezza delle informazioni.

La funzione competente in materia di formazione, in coordinamento con la funzione di sicurezza delle informazioni, definisce e attua un programma di formazione e sensibilizzazione in materia di sicurezza delle informazioni, rivolto al personale dell'Ateneo e, ove applicabile, ai fornitori esterni.

La funzione risorse umane supporta tali attività in coerenza con i processi di gestione e sviluppo delle competenze del personale.

Tale programma è pianificato con periodicità almeno annuale ed è finalizzato a promuovere e diffondere una cultura della sicurezza delle informazioni all'interno dell'organizzazione.

Il programma di formazione e sensibilizzazione deve prevedere, in coerenza con i ruoli e le responsabilità assegnati:

- Una formazione mirata, adeguata ai diversi profili professionali e gli ambiti di attività, finalizzata a rendere il personale consapevole dei rischi per la sicurezza delle informazioni e delle corrette modalità di gestione delle stesse in relazione alle mansioni svolte;
- Una pianificazione strutturata delle iniziative formative, definita in modo sistematico e coerente con le esigenze organizzative dell'Ateneo, al fine di garantire la continuità e l'efficacia delle attività di formazione e sensibilizzazione;

- Un aggiornamento periodico dei contenuti, volto ad assicurare l'allineamento delle conoscenze e delle competenze del personale all'evoluzione del contesto organizzativo, tecnologico e normativo, nonché ai cambiamenti dei rischi per la sicurezza delle informazioni.

8. Gestione della sicurezza delle informazioni

Le strutture del Politecnico di Bari che gestiscono direttamente, totalmente o in parte, il sistema informativo dell'Ateneo (ad esempio: gestione delle infrastrutture IT, gestione delle reti, sviluppo e manutenzioni di applicazioni e sistemi informativi) devono garantire, per mezzo delle proprie strutture e funzioni competenti, che l'operatività si svolga conformemente alle misure di sicurezza previste nei paragrafi successivi della presente Politica, avvalendosi, qualora necessario, del supporto della funzione competente in materia di sicurezza delle informazioni per gli ambiti oggetto della Politica stessa.

Con riferimento ai servizi informatici erogati internamente dall'Ateneo, le attività operative necessarie a garantire la gestione della sicurezza delle informazioni sono svolte dalle strutture competenti del Politecnico di Bari; tali funzioni, ciascuno per gli ambiti di propria competenza, hanno il compito di implementare e mantenere efficaci nel tempo le misure di sicurezza volte a garantire il rispetto e il mantenimento di quanto previsto nella presente Politica, secondo quanto dettagliato nei paragrafi successivi. Ciò anche al fine di garantire il soddisfacimento dei requisiti richiesti ai fini dell'ottenimento e/o del mantenimento delle certificazioni in materia di gestione della sicurezza delle informazioni.

Con riferimento ai servizi informatici erogati da terzi, le attività operative necessarie per assicurare la gestione della sicurezza delle informazioni devono essere garantite dai fornitori o soggetti esternalizzati, in conformità alle disposizioni contrattuali, ai requisiti di sicurezza definiti dal Politecnico di Bari e alle misure previste dalla presente Politica.

8.1. Procedure operative di sicurezza

La sostenibilità della presente Politica deve essere garantita da procedure operative e/o norme di processo specifiche, che declinano gli ulteriori requisiti di sicurezza delle informazioni al fine di rispondere ad esigenze particolari e di disciplinare ambiti e tematiche specifiche.

La funzione competente in materia di sicurezza delle informazioni del Politecnico di Bari, in coordinamento con le altre strutture interessate, ha il compito di definire un insieme di procedure operative specifiche inerenti alla sicurezza delle informazioni, finalizzati al raggiungimento degli obiettivi di controllo della sicurezza delle informazioni, sulla base dei risultati del processo di analisi e valutazione dei rischi.

8.2. Gestione delle risorse ICT

Le risorse ICT devono essere identificate e devono essere definite le adeguate responsabilità di gestione in modo da agevolare l'implementazione degli adeguati livelli di protezione.

Le strutture ICT competenti del Politecnico di Bari hanno il compito di registrare gli asset informatici presenti nell'Ateneo, nonché le interrelazioni tra gli stessi e con i processi istituzionali, amministrativi e gestionali che supportano, garantendo il presidio puntuale dell'intero ciclo di vita dell'hardware e del software nell'ambito di un complessivo processo di asset management.

- identificare e manutenere un inventario delle risorse ICT (sistemi, apparati di rete, database, etc.) comprensivo delle principali configurazioni delle interdipendenze tra gli asset;
- assegnare formalmente la responsabilità di gestione degli asset;

- classificare e rendere identificabili ("etichettare") opportunamente gli asset secondo quanto previsto nella Politica di Ateneo in materia di Classificazione delle Informazioni;
- assicurare l'adozione delle modalità di gestione delle informazioni all'interno dei sistemi informatici in conformità alla Politica di Ateneo in materia di Classificazione delle Informazioni;
- attuare processi di monitoraggio del ciclo di vita delle risorse ICT, verificando che le stesse siano supportate dai fornitori e/o dagli sviluppatori esterni o interni e che le patch e gli aggiornamenti pertinenti siano applicati secondo processi documentati; devono inoltre essere previste misure di mitigazione dei rischi derivanti dall'utilizzo di risorse ICT non aggiornate o non più supportate, al fine di garantire il soddisfacimento dei requisiti dell'Ateneo e di gestione dei rischi;
- assicurare un corretto trattamento quando gli asset in fase di dismissione o distruzione.

8.3. Gestione Identità e accessi logici

L'accesso alle informazioni deve avvenire in modo da prevenire trattamenti non autorizzati delle stesse o la loro visione da parte di soggetti privi dei necessari diritti.

L'accesso alle informazioni e alle risorse ICT è disciplinato nel rispetto dei principi di riservatezza, necessità di conoscere e minimo privilegio, al fine di ridurre il rischio di accessi non autorizzati impropri delle informazioni.

La Funzione competente in materia di Sicurezza Informatica del Politecnico di Bari, in coordinamento con le strutture ICT competenti, ha il compito di garantire l'attuazione delle procedure di sicurezza logica in coerenza con quanto previsto dalla presente Politica.

La funzione competente in materia di sicurezza delle informazioni, in coordinamento con le strutture ICT, ha altresì il compito di progettare, realizzare e manutenere le soluzioni adottate per garantire la sicurezza degli accessi logici alle informazioni dell'Ateneo, ai dati personali e alle risorse ICT.

Nell'ambito della gestione degli accessi logici, devono essere osservati i seguenti principi:

- l'accesso logico alle risorse ICT è ristretto ai soggetti formalmente autorizzazione ed è limitato a quanto strettamente necessario in base alle effettive esigenze operative. I diritti di accesso logico devono essere concessi, revocati o modificati tempestivamente secondo procedure di approvazione predefinite che coinvolgano il responsabile funzionale dell'applicazione, per quanto riguarda le applicazioni software, o le strutture ICT competenti per i sistemi ICT. I diritti di accesso devono, inoltre, essere sottoposti a revisioni periodiche, al fine di garantire una corretta gestione delle utenze assegnate ed essere tempestivamente revocati in caso di cessazione del rapporto di lavoro. L'accesso alle informazioni, a dati personali ed alle risorse ICT deve avvenire per mezzo di applicazioni informatiche;
- deve essere garantita l'applicazione dei principi di "segregazione dei compiti" e di "minimo privilegio", con particolare attenzione alla separazione degli ambienti IT (in particolare di sviluppo, collaudo e produzione);
- gli accessi ai sistemi con utenze dotate di abilitazioni privilegiate (es. utenza da amministratore di sistema) devono essere strettamente limitati e monitorati, attraverso misure quali il controllo degli accessi logici, la registrazione e la revisione delle attività, tecnologie di autenticazione forte e il monitoraggio delle anomalie. L'assegnazione dei diritti di accesso privilegiato deve essere controllata attraverso un processo formale di autorizzazione al fine di garantire la sicurezza delle comunicazioni e ridurre i rischi connessi. L'accesso da remoto attraverso l'utilizzo di utenze privilegiate a sistemi critici è concesso esclusivamente sulla base delle esigenze operative e tramite l'utilizzo di soluzioni di autenticazione forte. Con particolare riferimento alle utenze privilegiate, i registri degli accessi devono essere protetti per impedire modifiche o cancellazioni non autorizzate;
- l'accesso logico alle risorse ICT deve avvenire previa identificazione e autenticazione dell'utente;

- l'uso di account utente generici e condivisi deve essere limitato il più possibile. Gli utenti devono comunque poter essere identificati per le azioni effettuate sulle risorse ICT;
- le modalità di autenticazione devono essere commisurate alla confidenzialità delle informazioni trattate all'interno delle risorse ICT, prevedendo, ove prescritto o valutato necessario, anche l'utilizzo di tecniche di autenticazione a più fattori;
- devono essere stabiliti criteri e regole per garantire la conservazione e il monitoraggio delle registrazioni degli accessi logici.

8.4. Misure di sicurezza fisica e ambientale

L'accesso alle sedi ed ai singoli locali del Politecnico di Bari deve essere consentito esclusivamente al personale autorizzato, al fine di prevenire la perdita, il danneggiamento, la compromissione di asset o l'interruzione delle attività istituzionali, amministrative e gestionali.

Le strutture competenti per la gestione degli accessi fisici dell'Ateneo identificano, attuano e documentano le misure di sicurezza fisica necessaria a disciplinare l'accesso alle sedi e si singoli locali, garantendo adeguati livelli di tutela delle informazioni contro i rischi di sottrazione, alterazione o distruzione, in particolare nelle aree operative ad accesso controllato o ristretto.

I criteri di assegnazione degli accessi fisici devono essere sottoposti a verifiche periodiche per garantire che i diritti di accesso non necessari vengano prontamente revocati.

Deve essere garantita la gestione della sicurezza delle aree e dei locali tramite:

- l'individuazione delle aree e la classificazione dei locali in base alla criticità delle informazioni presenti sia in forma digitale sia cartacea;
- la definizione degli adeguati livelli di protezione sia fisica che ambientale;
- l'implementazione dei meccanismi di protezione individuati.

Deve essere garantita la sicurezza delle apparecchiature tramite:

- la definizione di un'adeguata collocazione e protezione fisica delle apparecchiature per l'elaborazione delle informazioni;
- la messa a disposizione delle risorse necessarie al loro funzionamento;
- la predisposizione di un adeguato livello di manutenzione.

8.5. Sicurezza delle reti

La riservatezza e l'integrità dei dati in transito, su reti private, pubbliche o su wireless, devono essere salvaguardate tramite controlli speciali, definiti in funzione del livello di rischio e della classificazione delle informazioni, al fine di prevenire accessi non autorizzati o alterazioni dei dati.

La/e Funzione/i competente/i dell'Ateneo hanno il compito di realizzare le misure di sicurezza necessarie a garantire adeguati meccanismi di protezione delle informazioni sull'architettura hardware e software di rete e il monitoraggio delle infrastrutture di rete, della rete interna dell'Ateneo, delle reti dei Data center, delle reti WAN, della rete wireless e delle connessioni con utenti autorizzati, fornitori e altri soggetti esterni.

La/e Funzione/i competente/i dell'Ateneo, di concerto con la Funzione competente in materia di Sicurezza delle informazioni, hanno il compito di gestire gli apparati di sicurezza in ambito di protezione di rete (es. Firewall, Web Application Firewall, Intrusion Detection System, etc.).

Al fine di mantenere la sicurezza delle informazioni in transito nelle reti, devono essere considerate le seguenti linee guida:

- le reti devono essere presidiate e controllate adeguatamente e costantemente contro i tentativi di intrusione, intercettazione e attacco, al fine di proteggere le informazioni nei sistemi e nelle applicazioni;
- nelle reti devono essere garantiti meccanismi di segregazione di gruppi di servizi, di utenti e di sistemi informativi a seconda del livello di rischio inerente ai relativi asset e in base alla classificazione dei dati in transito;
- l'accesso a diversi domini di rete deve essere controllato a livello perimetrale attraverso un gateway (per esempio firewall, router), a seconda del livello di classificazione11 delle informazioni in transito, al fine di garantire che la sicurezza del dominio di rete di destinazione sia adeguata al livello di criticità dell'informazione in transito;
- deve essere assicurata la riservatezza del traffico di rete, in linea con il livello di classificazione delle informazioni in transito, attraverso l'adozione di tecnologie crittografiche deve essere effettuata un'adeguata raccolta di log degli apparati di rete/sicurezza e un monitoraggio che permettano la registrazione e l'individuazione delle azioni che potrebbero avere impatti sulla sicurezza delle informazioni.

8.6. Sviluppo, acquisizione e manutenzione delle risorse ICT

La sicurezza delle informazioni deve essere considerata in tutte le fasi del ciclo di vita dei sistemi informativi, ivi compreso lo sviluppo degli stessi, al fine di contribuire ad evitare l'introduzione di vulnerabilità che possono essere sfruttate da una minaccia, interna o esterna all'organizzazione.

La funzione competente in materia di sicurezza delle informazioni dell'Ateneo, in coordinamento con le strutture ICT competenti, ha il compito di definire le misure operative di sicurezza relative all'acquisizione o sviluppo sicuro di sistemi (Security By Design, SSDLC), in modo da garantire il presidio dei rischi connessi al ciclo di vita dello sviluppo e/o acquisizione del software.

La/e Funzione/i ICT competenti dell'Ateneo, in collaborazione con la funzione competente in materia di sicurezza delle informazioni, assicura/no che, nei processi di sviluppo e acquisizione software, sia verificata la rispondenza ai principi di sicurezza delle informazioni fin dalla fase di progettazione, secondo i principi di Security by default e Security by design.

Nell'ambito dell'acquisizione, dello sviluppo e della manutenzione delle risorse ICT devono essere considerate almeno le seguenti linee guida:

- la definizione dei requisiti funzionali e non funzionali, ivi compresi i requisiti di sicurezza delle informazioni;
- la definizione di misure indirizzate ad attenuare il rischio di alterazioni non intenzionali o manipolazioni intenzionali dei sistemi ICT durante lo sviluppo e nell'implementazione in ambiente di produzione;
- la definizione di una metodologia per verificare e approvare i sistemi ICT, i servizi ICT e le misure di sicurezza delle informazioni prima e durante il loro utilizzo al fine di individuare e risolvere potenziali debolezze, violazioni e incidenti di sicurezza;
- la definizione di misure per garantire l'integrità e la riservatezza dei dati di produzione in ambienti non produttivi (ad esempio l'accesso ai dati di produzione ai soli utenti autorizzati);
- la definizione di misure per proteggere l'integrità dei codici sorgente dei sistemi ICT sviluppati internamente;
- la definizione di un processo formale per l'esecuzione delle attività di test nel caso di acquisizione da terzi dei sistemi ICT, in coerenza con le procedure e le politiche dell'Ateneo in materia di sviluppo sicuro del software;
- la garanzia che i dati di test siano selezionati con attenzione, protetti e mantenuti sotto controllo;

- la garanzia che i contratti con i fornitori riportino i requisiti di sicurezza identificati nell'ambito dei modelli contrattuali e delle disposizioni vigenti dell'Ateneo.

8.7. Gestione dei progetti e dei cambiamenti ICT

I cambiamenti alle risorse ICT all'interno del ciclo di vita devono essere monitorati attraverso l'utilizzo di procedure formali di controllo dei cambiamenti al fine di minimizzare l'impatto degli stessi sui servizi IT.

Nell'ambito della gestione dei progetti ICT, la funzione competente in materia di sicurezza delle informazioni dell'Ateneo, coordinandosi con le strutture ICT competenti, ha il compito di definire e verificare i requisiti di sicurezza nelle iniziative di cambiamento di natura evolutiva e progettuale.

Il processo di gestione dei progetti ICT deve considerare al minimo i seguenti elementi:

- gli obiettivi del progetto, inclusi gli obiettivi per la sicurezza delle informazioni;
- i ruoli e le responsabilità del progetto;
- una valutazione dei rischi del progetto, inclusi i rischi ICT e di sicurezza al fine di identificare i controlli di sicurezza necessari;
- il piano, i tempi e le fasi del progetto;
- le milestone fondamentali;
- i requisiti di gestione dei cambiamenti.

Nell'ambito dei cambiamenti ICT, la/e struttura/e ICT competente/i dell'Ateneo ha/hanno il compito di presidiare il processo di Change management e di gestire la pianificazione dei rilasci applicativi e degli interventi sui sistemi, al fine di garantire che tutte le modifiche alle risorse ICT siano registrate, testate, valutate, approvate, implementate e verificate in modo controllato.

Tale processo deve prendere in considerazione almeno i seguenti elementi:

- l'identificazione, la registrazione e l'approvazione dei cambiamenti significativi;
- la pianificazione dei cambiamenti e di tutte le fasi del processo;
- la valutazione degli impatti potenziali, inclusi quelli relativi alla sicurezza delle informazioni, di tali cambiamenti;
- la definizione di una procedura di approvazione formale dei cambiamenti proposti;
- la focalizzazione sui principi di privacy by design e privacy by default;
- la verifica che i requisiti per la sicurezza delle informazioni siano rispettati;
- l'esecuzione di test in ambiente di collaudo, effettuati da personale qualificato, e di test lato utente da parte delle funzioni richiedenti le modifiche, prima che la modifica sia rilasciata in ambiente di esercizio;
- la comunicazione delle specifiche dei cambiamenti a tutto il personale coinvolto;
- l'aggiornamento della documentazione relativa alle risorse ICT per ogni cambiamento effettuato;
- l'aggiornamento dell'inventario degli asset ICT laddove vengano introdotte nuove risorse ICT (hardware o software) o ne vengano modificate di esistenti oppure vengano modificate le relative configurazioni;
- la definizione di procedure di *rollback*, comprensive delle responsabilità operative e decisionali, per il ripristino controllato dello stato precedente in caso di esito negativo dei cambiamenti;
- la definizione di procedure di *fall-back*, comprensive delle responsabilità operative e decisionali, per garantire la continuità operativa attraverso l'attivazione di soluzioni alternative in caso di malfunzionamenti o eventi imprevisti;
- la predisposizione di un processo per i cambiamenti "in emergenza" che permetta l'attuazione rapida e controllata dei cambiamenti necessari a risolvere, ad esempio, un incidente.

8.8. Gestione e sicurezza delle attività operative ICT

Devono essere implementate misure di sicurezza delle attività operative ICT per prevenire il verificarsi di problemi di sicurezza nelle risorse ICT e nei servizi ICT e per assicurare che i requisiti di sicurezza siano inclusi in tutte le fasi del ciclo di vita (progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione delle risorse ICT e dei servizi informatici).

Le misure adottate sono orientate a garantire nel tempo l'integrità e la disponibilità delle informazioni e dei servizi ICT e sono soggette a monitoraggio e riesame periodico, al fine di assicurarne la continua adeguatezza ed efficacia.

La/e strutture ICT competenti dell'Ateneo, di concerto con la funzione competente in materia di sicurezza delle informazioni, hanno il compito di garantire l'adozione delle misure di sicurezza durante le attività operative. Tali misure devono prevedere almeno:

- l'identificazione delle specifiche funzionali delle risorse ICT con la relativa configurazione, sulla base dell'inventario degli asset ICT individuato (sistemi, apparati di rete, database, etc.);
- l'attuazione di un piano di manutenzione correttiva ed evolutiva delle risorse ICT al fine di prevenirne l'obsolescenza;
- l'individuazione delle potenziali vulnerabilità, che dovrebbero essere valutate e corrette garantendo che il software e il firmware siano aggiornati mediante la distribuzione di patch di sicurezza critiche o la realizzazione di controlli compensativi;
- la configurazione della sicurezza di base (*hardening*);
- l'implementazione di meccanismi per la protezione delle risorse ICT al fine di assicurare che questi soddisfino gli standard e i requisiti di sicurezza definiti, prima che questi ottengano l'accesso alla rete dell'Ateneo;
- l'implementazione di meccanismi per verificare l'integrità di software, firmware e dati;
- l'implementazione di tecniche di cifratura per i dati memorizzati e in transito in base alla classificazione dei dati utilizzando algoritmi e lunghezze di chiavi che nel tempo assicurano l'adeguato livello di protezione ai dati interessati. Qualora per qualsiasi motivo, interno o esterno, la chiave di cifratura o gli algoritmi vengono compromessi o vi sia un fondato sospetto della loro compromissione, le informazioni memorizzate devono essere ricodificate e, se necessario, deve essere implementato un algoritmo diverso per sostituire quello considerato violato;
- l'attuazione di processi di monitoraggio delle prestazioni e della capacità delle risorse ICT per prevenire, individuare e rispondere in modo tempestivo a problemi di prestazioni dei sistemi ICT e di riduzione delle loro capacità o ad eventuali incidenti di sicurezza;
- la definizione e attuazione di procedure di backup e ripristino dei dati e delle risorse ICT, comprendenti:
    - l'ambito e la frequenza dei backup, definiti in funzione delle esigenze di ripristino e della criticità dei dati e delle risorse;
    - le modalità di pianificazione e attuazione di verifiche periodiche;
    - i criteri di conservazione sicura dei backup in sedi fisicamente separate dal sito primario, in modo da ridurre l'esposizione agli stessi rischi;
- la registrazione, la conservazione e il relativo monitoraggio dei log degli eventi, delle attività degli utenti, delle eccezioni, dei malfunzionamenti e degli eventi relativi alla sicurezza delle informazioni;
- l'implementazione ed impiego di software per la prevenzione, l'individuazione e la rimozione del malware;
- l'adozione di procedure di dismissione controllata delle risorse ICT (per esempio cancellazione sicura dei dischi).

8.9. Gestione degli incidenti di sicurezza delle informazioni

Le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza dell'Ateneo devono essere tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione, al fine di minimizzarne l'impatto sui processi istituzionali, amministrativi e gestionali.

La gestione degli incidenti è finalizzata a contenere gli impatti sulla riservatezza, integrità e disponibilità delle informazioni; tutti i soggetti coinvolti sono tenuti a collaborare attivamente secondo i ruoli e le responsabilità assegnate.

La funzione competente in materia di sicurezza delle informazioni dell'Ateneo ha il compito di garantire, tramite modalità strutturate definite dall'Ateneo, le attività di monitoraggio degli eventi nell'ambito della sicurezza informatica e la relativa classificazione, considerando altresì nuove minacce e vulnerabilità che possono emergere anche a seguito di attività di "information sharing".

Il processo di monitoraggio degli eventi e di gestione degli incidenti di sicurezza delle informazioni deve considerare almeno i seguenti elementi:

- I processi, i ruoli, le responsabilità e le strutture organizzative appropriate per garantire il coerente e integrato monitoraggio, le modalità di gestione, la segnalazione, le eventuali escalation e il follow-up degli incidenti;
- un'unica metodologia per la classificazione degli incidenti in linea con le disposizioni di vigilanza, gli standard e le best practices di sistema, con particolare attenzione agli incidenti con impatti sulla sicurezza delle informazioni, sui diritti e le libertà fondamentali dell'interessato (violazione dei dati personali ovvero "*data breach*");
- criteri e soglie appropriati per la classificazione di un evento come incidente, inclusi la classificazione come "grave incidente di sicurezza informatica";
- processi efficaci e tempestivi di comunicazione degli incidenti alle Autorità, laddove richiesto dalla normativa esterna vigente;
- opportune procedure di risposta agli incidenti.

8.10. Gestione della Continuità Operativa

I servizi, i processi e i sistemi devono essere implementati e gestiti assicurando una solida gestione della continuità operativa allo scopo di massimizzare la capacità di prestare servizi su base continuativa e di limitare le perdite in caso di gravi interruzioni dell'operatività.

La funzione competente dell'Ateneo in materia di continuità operativa, nell'ambito del modello di gestione della continuità operativa del Politecnico di Bari, elabora e mantiene la metodologia di Business Impact Analysis.

La gestione della continuità operativa, esercitata dai ruoli definiti nell'ambito dell'Organizzazione dell'Ateneo, deve prevedere almeno i seguenti elementi:

- l'identificazione e la valutazione, in termini di probabilità di accadimento e possibili conseguenze, di tutti gli eventi che possono determinare un'interruzione della continuità operativa, anche mediante analisi interne e/o esterne;
- l'attribuzione delle priorità alle azioni da effettuare per garantire la continuità operativa ricorrendo ad un approccio basato sul rischio, sulla base delle valutazioni delle funzioni, dei processi, delle risorse ICT, delle operazioni e delle interdipendenze individuati e classificati come critici;

- la predisposizione di un piano di Continuità Operativa che permetta all'organizzazione di affrontare, in modo organizzato ed efficiente, le conseguenze di un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e modalità idonei a ridurre l'impatto sull'operatività;
- la redazione, la validazione e la divulgazione di tutte le procedure operative ed organizzative necessarie per assicurare l'implementazione del piano di continuità;
- un processo di comunicazione tempestivo e appropriato nei confronti di tutte le parti interessate rilevanti, interne ed esterne, compresi i fornitori di servizi;
- l'esecuzione periodica di test per le componenti significative del piano di Continuità Operativa;
- il mantenimento e l'aggiornamento dei piani e delle procedure di cui ai punti precedenti, al fine di garantire l'efficacia del sistema nel tempo a fronte di eventuali cambiamenti organizzativi, operativi o tecnologici.

Le attività di revisione ed eventuale aggiornamento del piano di Continuità Operativa e dei relativi allegati, devono essere effettuate con frequenza almeno annuale. I piani devono essere aggiornati sulla base dei risultati delle verifiche, delle informazioni sulle minacce correnti, della condivisione delle informazioni, dei mutevoli obiettivi di ripristino e delle analisi degli scenari operativamente e tecnicamente plausibili non ancora verificatisi, nonché, se del caso, a seguito di modifiche alle risorse ICT ed ai processi.

8.11. Gestione della sicurezza delle informazioni nelle relazioni con i fornitori

Le misure di mitigazione dei rischi ICT e di sicurezza devono essere garantite anche quando si ricorre all'affidamento a terzi di attività, risorse o servizi ICT che implicano il trattamento di informazioni dell'Ateneo, al fine di minimizzare il rischio che il ricorso a una terza parte per la fornitura di sistemi ICT o servizi connessi, incida negativamente sulle prestazioni e sulla gestione del rischio.

In ogni caso, il Politecnico di Bari, che affida a terzi attività, risorse o servizi ICT comportanti il trattamento di informazioni, mantiene la piena responsabilità di quanto compiuto dal fornitore di servizi verso il quale ha eseguito l'affidamento, e deve adottare misure adeguate a garantire il rispetto di quanto previsto dalla presente Politica e dalla normativa in materia di esternalizzazioni delle funzioni dell'Ateneo o di approvvigionamento di beni e servizi.

I contratti con i fornitori (fornitori di outsourcing o terze parti incaricate) devono almeno includere:

- obiettivi e misure adeguati e proporzionati in materia di sicurezza delle informazioni, compresi i requisiti minimi di sicurezza informatica, le specifiche del ciclo di vita dei dati, gli eventuali requisiti in materia di crittografia dei dati, le misure di sicurezza della rete, i processi di monitoraggio della sicurezza e l'ubicazione dei data center, procedure di back up e di ripristino;
- obblighi per i fornitori di osservare la presente Politica di Sicurezza delle Informazioni dell'Ateneo;
- obblighi per i fornitori, una volta concluso il rapporto contrattuale e trascorso un periodo di tempo concordato, di eliminare qualsiasi copia o stralcio di dati riservati di proprietà della Società che esegue l'affidamento e presente su proprie risorse ICT, sistemi o supporti, in modo tale da escludere qualunque accesso successivo;
- diritti di audit da parte del Politecnico di Bari nei confronti dei fornitori, previa notifica, con accesso ai locali, alle risorse ICT e al personale coinvolto nell'erogazione dei servizi o nel trattamento delle informazioni;
- requisiti di continuità operativa (es. requisiti normativi e standard previsti, Piano di Continuità Operativa, tempo di ripartenza del processo/servizio, tempo massimo di perdita di dati e informazioni);
- procedure operative e di gestione degli incidenti di sicurezza, ivi compresi i processi di escalation e reportistica;
- processi di monitoraggio e reportistica dei livelli di conformità dei fornitori rispetto agli obiettivi di sicurezza delle informazioni, alle misure adottate o da adottare e agli obiettivi dell'Ateneo.

8.12. Gestione della sicurezza delle informazioni nei rapporti con soggetti esterni

Il Politecnico di Bari garantisce che, nell'ambito delle relazioni con soggetti esterni, inclusi quelli con cui intrattiene rapporti di fornitura (es. clienti), nonché con i destinatari dei propri servizi istituzionali, siano adottate misure adeguate a garantire la riservatezza, l'integrità e la disponibilità delle informazioni trattate, in conformità alla normativa applicabile e alle disposizioni interne.

In tale ambito, il Politecnico assicura che le informazioni scambiate con suddetti soggetti siano trattate in modo sicuro, prevenendo accessi non autorizzati, divulgazioni indebite, alterazioni o perdite, e che siano definite modalità di gestione coerenti con la classificazione delle informazioni e con i rischi identificati.

Nell'ambito delle relazioni con i clienti, sono definiti e adottati, ove applicabile, criteri e misure per:

- la regolamentazione delle modalità di accesso e utilizzo delle informazioni e dei servizi ICT messi a disposizione;
- la protezione dei dati personali e delle informazioni riservate, nel rispetto della normativa vigente;
- la gestione sicura dei canali di comunicazione e di scambio delle informazioni;
- la definizione delle responsabilità e degli obblighi delle parti in materia di sicurezza delle informazioni;
- la gestione degli incidenti di sicurezza che coinvolgono i clienti, inclusi i processi di segnalazione e risposta;
- la limitazione dell'accesso alle informazioni ai soli soggetti autorizzati, secondo il principio di necessità di conoscere e minimo privilegio;
- la promozione della consapevolezza dei clienti, ove opportuno, in merito alle corrette modalità di utilizzo dei servizi e delle informazioni.

Qualora soggetti esterni, legittimati a formulare richieste in materia di sicurezza delle informazioni, presentino specifiche esigenze o condizioni nell'ambito dei rapporti contrattuali, il Politecnico di Bari assicura che tali richieste siano valutate in coerenza con la presente Politica e con il complessivo assetto normativo e organizzativo dell'Ateneo.

A tal fine, la Politica per la Sicurezza delle Informazioni costituisce il riferimento primario per la gestione dei rapporti con soggetti esterni; eventuali richieste ulteriori o difformi rispetto a quanto in essa previsto sono sottoposte alla valutazione del Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni (RSGSI).

Il RSGSI a seguito di valutazione, cura l'istruttoria delle richieste e le sottopone alla valutazione e approvazione del Comitato di Alta Direzione. L'adozione di eventuali misure aggiuntive o la definizione di specifici impegni contrattuali è subordinata alle determinazioni assunte dal Comitato.

Il Comitato può, inoltre, ove ritenuto necessario, avvalersi del supporto del Responsabile della Protezione dei Dati (DPO) per quanto di sua competenza.

9. Monitoraggio, audit e miglioramento continuo

Il Politecnico di Bari assicura il monitoraggio continuo dell'efficacia delle misure di sicurezza delle informazioni adottate, al fine di individuare tempestivamente potenziali minacce, anomalie o debolezze e di garantire il mantenimento di un adeguato livello di protezione delle informazioni.

Le attività di monitoraggio, audit e riesame sono finalizzate a supportare il miglioramento continuo del SGSI e tengono conto dell'evoluzione del contesto organizzativo, tecnologico e normativo, nonché dei fattori interni ed esterni che possono influire sui processi dell'Ateneo e sulle risorse informative.

9.1. Monitoraggio e misurazione

Il Politecnico di Bari definisce indirizzi per il monitoraggio e la misurazione delle misure di sicurezza delle informazioni, al fine di valutarne nel tempo l'efficacia e l'adeguatezza rispetto ai rischi individuati.

Il monitoraggio comprende attività finalizzate a rilevare eventi di sicurezza, vulnerabilità, violazioni o situazioni che possano compromettere la riservatezza, l'integrità o la disponibilità delle informazioni e delle risorse ICT, nonché verifiche volte ad accertare la conformità alle disposizioni normative, agli standard di riferimento e alle regole interne applicabili.

Le misure di sicurezza sono oggetto di verifiche periodiche, anche a seguito di modifiche rilevanti ai sistemi, alle infrastrutture, ai processi o in conseguenza di incidenti di sicurezza significativi, al fine di assicurarne la continua efficacia. I risultati delle attività di monitoraggio e verifica sono analizzati e valutati e costituiscono un elemento di input per l'adozione di eventuali azioni correttive e di miglioramento.

Il Politecnico di Bari definisce indicatori e criteri di misurazione adeguati a supportare una valutazione oggettiva delle prestazioni e dell'efficacia delle misure di sicurezza delle informazioni, in coerenza con gli obiettivi del SGSI.

9.2. Audit interni

Il Politecnico di Bari assicura l'esecuzione di audit interni periodici sul SGSI, al fine di verificare la conformità ai requisiti normativi e agli standard di riferimento, nonché l'efficace attuazione della presente Politica e delle disposizioni interne applicabili.

Gli audit interni sono pianificati e condotti secondo criteri che tengono conto dell'importanza dei processi, dei risultati delle precedenti verifiche e del livello di rischio associato alle attività e ai sistemi oggetto di audit. I risultati degli audit costituiscono un elemento di input per il miglioramento del SGSI.

9.3. Riesame della Direzione

La Direzione effettua, con periodicità definita, il riesame del SGSI al fine di valutarne la continua adeguatezza, efficacia e coerenza con gli obiettivi istituzionali dell'Ateneo.

Il riesame della Direzione tiene conto, tra l'altro, dei risultati delle attività di monitoraggio e misurazione, degli audit interni, degli incidenti di sicurezza, dello stato delle azioni correttive e di miglioramento, nonché delle variazioni del contesto interno ed esterno e dei requisiti applicabili. Gli esiti del riesame supportano le decisioni strategiche in materia di sicurezza delle informazioni e l'allocazione delle risorse necessarie.

9.4. Gestione delle non conformità e azioni correttive

Il Politecnico di Bari assicura la gestione delle non conformità rilevate nell'ambito del SGSI, adottando azioni correttive adeguate al fine di eliminarne le cause e prevenire il loro ripetersi.

Le non conformità, gli esiti delle attività di monitoraggio e audit e le segnalazioni di incidenti di sicurezza costituiscono elementi fondamentali per il miglioramento continuo della sicurezza delle informazioni. Il

Politecnico promuove un approccio sistematico al miglioramento, volto ad accrescere nel tempo l'efficacia delle misure di sicurezza e la maturità complessiva del SGSI.

10. Documentazione di supporto

Il Politecnico di Bari assicura che l'attuazione della presente Politica sia supportata da un insieme strutturato e coerente di documenti, procedure e registrazioni che costituiscono il SGSI.

La documentazione di riferimento e i documenti di supporto definiscono, in modo dettagliato, le modalità operative, i controlli e le responsabilità necessari per garantire l'effettiva applicazione dei principi e degli indirizzi stabiliti dalla presente Politica, in coerenza con il campo di applicazione del SGSI.

Tale elenco è da intendersi a titolo esemplificativo e non esaustivo e può essere aggiornato nel tempo in funzione dell'evoluzione del SGSI, senza che ciò comporti la necessità di modificare la presente Politica.

La documentazione di riferimento e i documenti di supporto sono gestiti, mantenuti e aggiornati secondo modalità definite, al fine di garantirne l'adeguatezza, la coerenza e l'allineamento con l'evoluzione del contesto organizzativo, tecnologico e normativo.

11. Modalità di diffusione, recepimento e aggiornamento della Politica

La presente Politica per la Sicurezza delle Informazioni è approvata dal Consiglio di Amministrazione del Politecnico di Bari ed è resa disponibile alle parti interessate secondo modalità idonee a garantirne la conoscenza e l'accessibilità.

La Politica è diffusa all'interno dell'Ateneo e comunicata ai soggetti esterni rilevanti, inclusi fornitori, partner e clienti, ove applicabile, al fine di assicurare la consapevolezza dei principi e degli indirizzi in materia di sicurezza delle informazioni e di favorirne il corretto recepimento in relazione ai ruoli e alle responsabilità assegnati.

Il recepimento della presente Politica è garantito attraverso l'integrazione dei suoi contenuti nei processi organizzativi e nelle attività del SGSI, nonché mediante iniziative di informazione e sensibilizzazione rivolte al personale e ai soggetti coinvolti.

La Politica è oggetto di riesame periodico ed è aggiornata ogniqualvolta si rendano necessari adeguamenti in relazione a modifiche significative del contesto organizzativo, normativo o tecnologico, ovvero a seguito di esiti di audit, riesami della Direzione o incidenti rilevanti di sicurezza delle informazioni. Le versioni aggiornate della Politica sono approvate secondo le modalità previste e comunicate tempestivamente alle parti interessate.