UNIVERSITÀ DEGLI STUDI DI TRIESTE

PROCEDURA PER LA GESTIONE DEGLI INCIDENTI INFORMATICI

CONSIGLIO DEGLI STUDENTI	
SENATO ACCADEMICO	
CONSIGLIO AMMINISTRAZIONE	26.01.2026
DECRETO RETTORALE	172/2026 dd 25/02/2026
UFFICIO COMPETENTE	Unità di staff Gestione dell'innovazione e dei Progetti ICT

Data ultimo aggiornamento: 26 febbraio 2026	*a cura dell'Ufficio Affari Generali e Trasparenza Amministrativa*

1.Scopo

La presente procedura definisce le modalità di gestione e monitoraggio degli incidenti informatici (di seguito "incidenti") all'interno dell'Università degli Studi di Trieste (di seguito "Ateneo"), con particolare attenzione agli eventi che possono compromettere l'operatività, la disponibilità dei sistemi informativi e la sicurezza dei dati.

Il presente documento ha l'obiettivo di assicurare che la gestione di incidenti avvenga in maniera tempestiva, strutturata e documentata, riducendo al minimo gli impatti sui servizi digitali e sull'operatività dell'Ateneo.

Un'adeguata gestione di tali eventi consente di limitare le interruzioni dei servizi digitali, salvaguardare la riservatezza, l'integrità e la disponibilità delle informazioni trattate e garantire la trasparenza verso gli utenti e gli stakeholder istituzionali.

Il presente documento costituisce parte integrante del Sistema di Gestione della Sicurezza delle Informazioni adottato dall'Ateneo e assicura il rispetto delle disposizioni normative e degli standard di riferimento in materia. È redatto in conformità al D.Lgs. 138/2024 di attuazione della Direttiva NIS2, nonché agli standard internazionali quali la norma ISO/IEC 27001 e il NIST Cybersecurity Framework.

2.Campo di applicazione

La presente procedura è valida per tutte le sedi dell'Ateneo e si applica a tutti i soggetti che accedono o utilizzano i sistemi informatici, le reti e le piattaforme digitali in uso presso l'Ateneo.

3.Responsabilità

Di seguito vengono elencati e descritti i ruoli e le responsabilità dei soggetti coinvolti nella gestione degli incidenti.

TERMINE	**RESPONSABILITÀ**

ACN (Agenzia per la Cybersicurezza Nazionale)	L'ACN è responsabile del coordinamento nazionale degli incidenti di sicurezza informatica in Italia. Fornisce supporto alle organizzazioni nella gestione degli incidenti e si occupa della notifica degli incidenti di sicurezza a livello nazionale.
CSIRT Italia	Il CSIRT Italia è l'unità operativa nazionale che supporta la gestione degli incidenti informatici significativi. Il CSIRT fornisce supporto tecnico e facilita la condivisione di informazioni tra le organizzazioni per rispondere agli attacchi informatici e mitigare i rischi.
ENISA	L'ENISA (European Union Agency for Network and Information Security) fornisce supporto e linee guida per la gestione della sicurezza informatica a livello europeo. È un punto di riferimento per le pratiche di gestione della sicurezza e la protezione delle reti e dei sistemi informativi.
SOC Manager	Responsabile della gestione del processo di gestione di un incidente informatico. In particolare, è responsabile delle seguenti attività: indirizzamento, coordinamento e monitoraggio delle attività complessive di gestione e risoluzione degli incidenti IT; coordinamento della stesura della documentazione necessaria a riepilogare le attività di identificazione, prioritizzazione, gestione e mitigazione degli incidenti occorsi.
Organi di Amministrazione e Direzione	Gli organi di amministrazione e direzione sono responsabili per la supervisione generale del processo di gestione degli incidenti. Approvano le politiche aziendali in materia di sicurezza informatica e garantiscono che i processi di gestione siano attuati in conformità con le normative di sicurezza informatica e le politiche interne
Referente CSIRT	Persona fisica incaricata di interfacciarsi con il CSIRT Italia e di notificare tempestivamente gli incidenti significativi ai sensi del D. Lgs. 138/2024.
Soggetto che ha riscontrato l'anomalia	Ha il compito di rilevare un evento anomalo e segnalarlo tempestivamente al SOC. La sua responsabilità principale è garantire che l'informazione arrivi subito ai canali corretti.
Settore Cybersicurezza, infrastrutture telematiche e in cloud (funge da Security Operations Center – SOC-)	Responsabile della gestione operativa degli incidenti, compresa l'analisi tecnica e la risoluzione delle problematiche informatiche. È coinvolto nell'attuazione delle misure di contenimento e nella collaborazione con SOC manager per una pronta risposta.
Amministratori di Sistema (AdS)	Implementano le azioni di contenimento e rimedio.
Direzione Area dei Servizi ICT	Definisce la procedura, supervisiona il processo e decide con RSGSI e SOC le eventuali azioni correttive.

(ASICT)	
Responsabile del Sistema di Gestione della Sicurezza delle Informazione (RSGSI)	Verifica periodicamente che la procedura sia seguita, coadiuva il SOC manager e la Direzione in tutto il processo, raccoglie le evidenze e aggiorna il SGSI.

4.Definizioni

Di seguito vengono riportate le definizioni e la terminologia di termini e abbreviazioni utilizzati all'interno del documento:

TERMINE	DEFINIZIONE
Disponibilità	Proprietà della sicurezza informatica secondo cui i sistemi, i dati e i servizi devono essere accessibili e utilizzabili quando richiesto dagli utenti autorizzati.
Evento di sicurezza	Qualsiasi cambiamento significativo che possa indicare un possibile incidente di sicurezza, come un comportamento anomalo o sospetto nei sistemi.
Gestione degli incidenti	Azioni e procedure volte a prevenire, rilevare, analizzare e contenere un incidente o a rispondervi e recuperare da esso.
Incidente	Evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi.
Incidente significativo	Un incidente è considerato significativo se: a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato; b) ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.
Integrità	Proprietà della sicurezza informatica secondo cui le informazioni devono essere accurate, complete e non alterate in modo non autorizzato.
Minaccia informatica	Qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo su sistemi informativi e di rete, sugli utenti di tali sistemi e altre persone.

Patch di sicurezza	Aggiornamento software rilasciato dal fornitore o dall'ufficio IT con l'obiettivo di correggere vulnerabilità note al fine di migliorare la sicurezza dei sistemi e delle applicazioni.
Quasi-incidente	Evento che avrebbe potuto configurare un incidente senza che quest'ultimo si sia tuttavia verificato, ivi incluso il caso in cui l'incidente sia stato efficacemente evitato.
Riservatezza	Proprietà della sicurezza informatica che garantisce che le informazioni siano accessibili solo a soggetti autorizzati.
Rischio	Combinazione dell'entità dell'impatto di un incidente, in termini di danno o di perturbazione, e della probabilità che quest'ultimo si verifichi.
Rischio informatico	Possibilità di danno derivante dall'uso non autorizzato o dall'interferenza con i sistemi informatici, che può compromettere la riservatezza, l'integrità o la disponibilità dei dati.
Sicurezza dei sistemi informativi e di rete	Capacità dei sistemi informativi e di rete di resistere, con un determinato livello di affidabilità, agli eventi che potrebbero compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informativi e di rete o accessibili attraverso di essi.
Sicurezza informatica	Insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche.
Data Breach	Un incidente che coinvolge dati personali. È una violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.
Azioni di contenimento/ rimedio	È un'azione immediata conseguente a un evento/incidente/data breach o ad una non conformità per rimediare a quanto successo nel più breve tempo possibile. Normalmente è effettuata da chi ha la responsabilità del sistema o del servizio impattato.
Azione correttiva	È una misura che viene adottata per eliminare le cause di una non conformità rilevata o di un near miss/incidente/data breach al fine di prevenirne la ripetizione.

5.Procedura

Il processo di gestione degli incidenti viene attivato nel momento in cui un evento inerente alla sicurezza delle informazioni viene qualificato come incidente. Tale processo è finalizzato a garantire l'individuazione tempestiva degli incidenti, la loro corretta classificazione, la riduzione dei tempi di analisi e risoluzione, la rapida attivazione delle eventuali misure di continuità

operativa, nonché una comunicazione efficace e conforme verso i soggetti interni ed esterni coinvolti nel processo di gestione degli incidenti che si articola nelle seguenti macro-fasi: prevenzione e misure proattive, identificazione, valutazione e classificazione, gestione, chiusura, post-incident, lessons learned e monitoraggio.

5.1 Prevenzione e misure proattive

In questa fase sono definite le azioni preventive e le misure proattive volte a ridurre il rischio di incidenti.
L'Ateneo adotta un approccio proattivo alla sicurezza informatica, orientato alla prevenzione degli incidenti e alla riduzione dell'esposizione al rischio, in conformità a quanto previsto dal D.Lgs. 138/2024.
A tal fine, vengono implementate misure tecniche e organizzative che includono, in particolare:

- la valutazione periodica del rischio informatico in relazione ai processi critici dell'Ateneo;
- il monitoraggio continuo della rete e dei sistemi informativi, finalizzato all'individuazione tempestiva di vulnerabilità, anomalie o comportamenti sospetti;
- la definizione e l'applicazione di policy e procedure per la gestione degli accessi;
- la formazione e la sensibilizzazione di tutto il personale sui temi della sicurezza informatica e sui comportamenti corretti da adottare nell'utilizzo delle risorse digitali;
- la gestione delle vulnerabilità mediante l'applicazione tempestiva di aggiornamenti e patch di sicurezza, al fine di proteggere i dati e le risorse critiche.

Rientrano inoltre in questo ambito le attività di manutenzione dei server e dei sistemi operativi. Tali misure fanno parte di un sistema di gestione della sicurezza delle informazioni, soggetto a verifiche e aggiornamenti periodici, anche sulla base delle analisi post-incidente e dell'evoluzione delle minacce.

5.2 Identificazione

L'attività di identificazione e segnalazione di un evento di sicurezza informatica si articola in due momenti distinti e complementari:

- **rilevazione**, intesa come individuazione di un evento anomalo o potenzialmente critico;
- **segnalazione**, intesa come comunicazione formale dell'evento all'interno dell'Organizzazione, al fine di avviare il processo di gestione dell'incidente.

Fase di rilevazione
La rilevazione consiste nel riconoscimento di un possibile evento di sicurezza informatica e può avvenire attraverso:

- l'individuazione di anomalie riscontrate durante il normale svolgimento delle attività, quando emergono comportamenti inattesi o non conformi alla consueta operatività dei sistemi;
- l'identificazione di eventi di sicurezza tramite le attività di monitoraggio continuo svolte dall'Area dei Servizi ICT, trasmissione di bollettini di sicurezza da parte enti (s. ACN, GARR-CERT, Polizia Postale) o fornitori IT (rif. PRO007-Procedura per la Threat Intelligence).

Fase di segnalazione
Una volta rilevato un evento sospetto o un incidente, si procede alla fase di segnalazione, che consiste nella trasmissione formale delle informazioni necessarie all'avvio del processo di gestione degli incidenti.

Il soggetto che ha individuato l'evento ha l'obbligo di segnalarlo tempestivamente, inviando una comunicazione all'indirizzo e-mail **sicurezzainformatica@units.it**.

5.3 Valutazione e classificazione

In questa fase vengono svolte le attività di analisi e categorizzazione degli incidenti (rif. MOD07 - Segnalazione evento, incidente, data breach) in base alla loro gravità e all'impatto potenziale o effettivo, al fine di determinare le azioni di risposta più appropriate.
L'attività di valutazione e classificazione degli incidenti, che segue immediatamente la fase di identificazione, ha lo scopo di stabilire se un evento rientri tra quelli qualificabili come significativi ai sensi del Decreto Legislativo 138/2024, di recepimento della Direttiva (UE) 2022/2555 (NIS 2). Ai sensi dell'articolo 2, comma 1, lettera t) del D.Lgs. 138/2024, per incidente si intende "un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati, nonché dei servizi forniti dai sistemi informativi e di rete o accessibili tramite essi".
Considerata la molteplicità delle modalità con cui un incidente può manifestarsi, è innanzitutto necessario distinguere tra le seguenti categorie:
Eventi o anomalie sui sistemi: rientrano in questa categoria gli eventi che causano un'interruzione o un degrado temporaneo dei servizi dell'Ateneo senza essere riconducibili a minacce informatiche. Si tratta di eventi di natura tecnica, operativa o accidentale che, pur non derivando da azioni intenzionali, possono incidere sulla disponibilità dei sistemi e sulla continuità dei servizi. Esempi tipici includono guasti hardware su server, apparati di rete o sistemi di archiviazione, interruzioni dell'alimentazione elettrica, malfunzionamenti degli impianti di condizionamento delle sale server, errori di configurazione dovuti a interventi umani o perdita e corruzione di dati causate da difetti tecnici. Sebbene non abbiano origine cibernetica, tali eventi devono essere gestiti secondo le procedure operative interne, in quanto potenzialmente impattanti sui servizi istituzionali; ***Incidenti cyber:*** gli incidenti cyber comprendono tutti gli eventi che comportano, o tentano di comportare, una violazione della riservatezza, dell'integrità o della disponibilità di dati e sistemi informativi dell'Ateneo. Essi possono derivare, direttamente o indirettamente, da azioni malevole o accidentali, quali malware, accessi non autorizzati, campagne di phishing o attacchi mirati; ***Quasi-incidenti:*** i quasi-incidenti sono eventi che avrebbero potuto configurare un incidente vero e proprio, ma che sono stati evitati o neutralizzati efficacemente. Ne sono esempi un'e-mail di phishing bloccata dai sistemi antispam, il rilevamento e la bonifica tempestiva di un malware su una postazione isolata o tentativi di accesso non autorizzato respinti dai meccanismi di autenticazione. ***Data Breach:*** è un incidente che coinvolge dati personali. È una violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali. Per tale tipologia di incidente si rimanda al documento dedicato: Procedura per la gestione dei Data Breach.

Tutti gli eventi sopradescritti devono essere segnalati all'indirizzo **sicurezzainformatica@units.it**. Anche qualora un evento appaia di scarsa rilevanza, deve essere sempre segnalato; pur non avendo generalmente una priorità elevata, tali segnalazioni devono essere monitorate e gestite secondo le procedure interne, in quanto possono costituire indicatori di minacce più ampie o di vulnerabilità sistemiche.
Le segnalazioni verificate dal SOC sono comunicate al RSGSI per le eventuali valutazioni e azioni sul Sistema di Gestione della Sicurezza delle Informazioni (SGSI) all'indirizzo **ict.sgsi@units.it**. Ai sensi del D.Lgs. 138/2024, e come richiamato nel capitolo "Definizioni", un incidente è considerato **significativo** quando ha causato o è in grado di causare una grave perturbazione operativa dei servizi, perdite finanziarie per il soggetto interessato, oppure

ripercussioni rilevanti su altre persone fisiche o giuridiche, determinando perdite materiali o immateriali di significativa entità.
A integrazione del quadro normativo, l'Agenzia per la Cybersicurezza Nazionale ha emanato la Determinazione n. 379907/2025, che fornisce ulteriori chiarimenti e indicazioni operative per individuare gli eventi qualificabili come incidenti significativi. In particolare, un incidente è considerato significativo quando l'Ateneo acquisisce evidenza oggettiva di eventi che comportano la perdita di riservatezza o di integrità dei dati, oppure la violazione dei livelli di servizio attesi.
Nello specifico, si configura un incidente significativo quando:

- l'Ateneo ha evidenza della perdita verso l'esterno della riservatezza di dati digitali di sua proprietà o sui quali esercita, anche parzialmente, il controllo.
  Esempio: diffusione non autorizzata di elenchi contenenti dati personali di studenti o personale tramite e-mail o repository pubblicamente accessibili.
- l'Ateneo ha evidenza della perdita di integrità di dati di sua proprietà o sotto il suo controllo, con impatti verso l'esterno.
  Esempio: alterazione di documenti ufficiali pubblicati sul portale istituzionale o manipolazione dei risultati d'esame nel sistema informativo didattico.
- l'Ateneo ha evidenza della violazione dei livelli di servizio attesi dei propri servizi o delle proprie attività, sulla base dei livelli di servizio (SL) definiti.
  Esempio: indisponibilità prolungata del portale studenti o della piattaforma e-learning a seguito di un attacco DDoS o della compromissione di un sistema.

Gli incidenti classificati come significativi devono essere gestiti con la massima tempestività, ricevere priorità elevata ed essere oggetto di un'analisi approfondita volta a valutare l'impatto effettivo o potenziale sulla sicurezza dei dati, sulla disponibilità dei servizi critici e sul rispetto degli obblighi normativi.

Tali incidenti devono essere comunicati dal SOC al RSGSI e al Direttore dell'Area dei Servizi ICT, nonché notificati al CSIRT Italia entro i termini previsti dal D.Lgs. 138/2024, secondo quanto indicato successivamente.

5.4 Gestione

Questa fase riguarda la definizione e l'attuazione delle misure necessarie per il contenimento dell'incidente e il ripristino dei sistemi e dei servizi coinvolti. In tale ambito rientrano anche le comunicazioni e le notifiche, interne ed esterne, previste dalla normativa vigente. L'attività di gestione dell'incidente è articolata in tre fasi operative e prevede il coinvolgimento del Security Operations Center (SOC) e degli amministratori di sistema, sotto il coordinamento del SOC Manager.

Fase di contenimento

La fase di contenimento ha l'obiettivo di limitare l'impatto dell'incidente, isolando il problema e impedendone la propagazione ad altri sistemi dell'infrastruttura informatica dell'Ateneo. Il SOC Manager, con il supporto del SOC e degli Amministratori di Sistema (AdS), definisce la strategia di risposta più adeguata, stabilendo le contromisure necessarie, le responsabilità per la loro attuazione e le modalità di verifica.
Nella scelta delle misure si valutano i potenziali danni, l'impatto sui servizi, le risorse e i tempi richiesti, l'effetto atteso e l'eventuale necessità di raccogliere e preservare le evidenze dell'incidente. Le azioni devono garantire, per quanto possibile, la continuità dei servizi. Il SOC Manager coordina le priorità e le risorse coinvolte, inclusi eventuali fornitori esterni.

Fase di ripristino

Completata la fase di contenimento, si procede al ripristino dei sistemi e delle applicazioni coinvolte, con l'obiettivo di riportarli ai livelli di servizio e sicurezza precedenti all'incidente. Gli Amministratori di Sistema (AdS) definiscono e attuano le attività necessarie, che possono comprendere: il recupero dei dati compromessi; il ripristino completo del servizio; l'implementazione di procedure temporanee alternative per garantire la continuità operativa; il ripristino parziale o con prestazioni limitate, in attesa del ripristino definitivo.

Ove opportuno, possono essere effettuati ripristini parziali o temporanei anche durante la gestione dell'incidente, al fine di ridurre l'interruzione delle attività istituzionali.

Durante questa fase, l'AdS o una figura da esso incaricata analizza il servizio oggetto di attacco e, se possibile, ne crea una copia virtuale per consentire le analisi della fase successiva.

Fase di raccolta e analisi

Il SOC Manager, con il supporto del SOC e degli amministratori di sistema coinvolti, raccoglie i dati pertinenti all'incidente per comprenderne cause, modalità di accadimento e azioni di rimedio adottate. L'analisi delle evidenze consente di delimitare i sistemi coinvolti, ricostruire le diverse fasi dell'incidente — a partire dall'evento originario — e valutare l'efficacia delle misure di contenimento e di ripristino adottate, nonché individuare eventuali azioni correttive per evitare il ripetersi dell'evento. Tutte le evidenze devono essere documentate e trasmesse al RSGSI all'indirizzo **ict.sgsi@units.it.**

Su richiesta del CSIRT Italia, l'Ateneo è tenuto a condividere una **relazione intermedia** sull'incidente, al fine di mantenere aggiornato il CSIRT in merito allo stato di avanzamento delle attività di gestione e mitigazione.

Tale adempimento è previsto dall'articolo 25, comma 5, lettera c) del D.Lgs. 138/2024, e ha l'obiettivo di garantire un flusso informativo continuo tra l'Ateneo e le autorità competenti, assicurando il coordinamento e la coerenza delle azioni intraprese in materia di sicurezza informatica (si rimanda ai capitoli successivi sugli obblighi e sulle tempistiche di segnalazione).

5.5 Chiusura

In questa fase si procede alla chiusura formale dell'incidente: una volta completate le operazioni di contenimento e, se necessario, di ripristino, l'incidente di sicurezza può essere considerato chiuso. Il SOC Manager redige il rapporto finale e registra la chiusura dell'incidente (rif. MOD019-Incident Report) e invia le evidenze al RSGSI che le conserva in apposito repository documentale e aggiorna il registro degli incidenti (rif. MOD023- Registro eventi, incidenti, data breach). La chiusura dell'incidente viene comunicata a tutti i soggetti interessati.

5.6 Post-incident, lessons learned e monitoraggio

Dopo la chiusura dell'incidente, si avvia una fase di analisi conclusiva per trasformare l'esperienza in un'opportunità di miglioramento. L'obiettivo è prevenire eventi analoghi e ridurre i tempi di reazione in futuro.

Il RSGSI convoca una riunione con le parti interessate per: esaminare l'incidente, le cause, le modalità di ripristino e gli eventuali errori. Se necessario si procede a: aggiornare la procedura di disaster recovery; valutare rischi su servizi analoghi e proporre misure preventive; predisporre un documento condiviso con raccomandazioni operative e tecniche. Le informazioni raccolte si

traducono quindi in interventi concreti: aggiornamento delle policy, rafforzamento delle misure di sicurezza e formazione del personale e degli utenti.

La Direzione, in collaborazione con il RSGSI e il SOC Manager, verifica se sia necessario adottare azioni correttive. A supporto di tale fase, il SOC manager e il RSGSI possono compilare il questionario Lessons Learned (rif. MOD020- Questionario Lessons Learned), che raccoglie evidenze e suggerisce aree di miglioramento.

6.Notifiche e segnalazioni

Nel rispetto di quanto previsto dall'art. 25 comma 1 del D. Lgs. 138/2024, nel caso in cui un incidente di sicurezza coinvolga dati personali o sia classificabile come significativo, in accordo al sopracitato Decreto, è necessario procedere tempestivamente con la segnalazione alle autorità competenti, in conformità con le normative vigenti. La segnalazione deve essere effettuata dal personale preposto e seguendo procedure definite per garantire la conformità legale e la gestione efficiente della crisi. A seconda della natura dell'incidente, le segnalazioni devono essere indirizzate a:

- **CSIRT Italia:** la segnalazione al CSIRT Italia è richiesta per incidenti che minacciano la sicurezza informatica di sistemi, reti o servizi critici a livello nazionale o per le infrastrutture di pubblica utilità rientranti negli Enti essenziali dal D.Lgs. 138/2024.
- **Garante per la protezione dei dati personali**: la notifica al garante della privacy è obbligatoria in caso di violazione dei dati personali che possa comportare rischi per i diritti e le libertà degli interessati.

Inoltre, al fine di garantire la piena conformità a quanto previsto dal D.Lgs. 138/2024, è necessario che gli Organi di Amministrazione e Direzione dell'Ateneo siano tempestivamente informati dell'incidente e delle azioni intraprese per la sua gestione.

Tale aggiornamento consente di assicurare un adeguato livello di supervisione, responsabilità e tracciabilità decisionale, nonché di predisporre tempestivamente eventuali comunicazioni istituzionali o adempimenti verso altri soggetti regolatori.

6.1 Notifica al CSIRT ITALIA

In conformità con il D.Lgs. 138/2024, attraverso la figura del Referente CSIRT, l'Ateneo deve segnalare tempestivamente al CSIRT Italia qualsiasi incidente informatico che possa avere un impatto significativo sulla sicurezza delle reti e dei sistemi informatici.

Secondo quanto previsto dal D.Lgs. 138/2024, l'Ateneo è tenuto a trasmettere al CSIRT Italia le seguenti notifiche riguardanti un incidente:

- **Pre-notifica** (early warning): deve essere inviata senza ingiustificato ritardo, e comunque entro **24 ore dal momento in cui si è venuti a conoscenza dell'incidente**. La pre-notifica deve, ove possibile, includere un'indicazione preliminare sul fatto che l'incidente possa essere il risultato di atti illegittimi o malevoli, e se potrebbe avere un impatto transfrontaliero;

- **Notifica dell'incidente** (incident notification): deve essere trasmessa **senza ingiustificato ritardo**, e comunque entro **72 ore dal momento in cui si è venuti a conoscenza dell'incidente.** Questa notifica deve aggiornare, ove possibile, le informazioni fornite nella prenotifica e includere una valutazione iniziale dell'incidente, con una stima della sua gravità e impatto. Inoltre, dove disponibili, devono essere forniti anche gli indicatori di compromissione relativi all'incidente.
- **Relazione finale:** deve essere trasmessa entro un mese dalla chiusura dell'incidente e deve includere un'analisi dettagliata dell'incidente ivi inclusi la sua gravità e il suo impatto, il tipo di minaccia o la causa originale che ha probabilmente innescato l'incidente, le misure di attenuazione adottate e in corso e ove noto, l'impatto transfrontaliero dell'incidente.

Inoltre, **su richiesta del CSIRT Italia**, l'Ateneo deve condividere una relazione intermedia sui pertinenti aggiornamenti della situazione.

Queste comunicazioni permettono al CSIRT Italia di monitorare e coordinare una risposta adeguata agli incidenti che possono influenzare la sicurezza delle reti e dei sistemi informatici a livello nazionale e internazionale.
Il CSRIT Italia ha predisposto una specifica piattaforma per la segnalazione di incidenti di sicurezza raggiungibile al seguente link: https://www.csirt.gov.it/segnalazione.

Successivamente, l'Ateneo provvede a informare i destinatari dei servizi in merito agli incidenti significativi che possono avere un impatto negativo sull'erogazione degli stessi (rif. PRO016 – Comunicazione ai destinatari dei servizi interessati da un incidente significativo).

6.2 Notifica di un incidente con potenziale Data Breach

Un "Data Breach" è una violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.

Il titolare del trattamento (soggetto pubblico, impresa, associazione, partito, professionista, ecc.), senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, deve notificare la violazione al Garante, a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche.
Il responsabile del trattamento che viene a conoscenza di una eventuale violazione è tenuto a informare tempestivamente il titolare in modo che possa attivarsi.

Le notifiche al Garante effettuate oltre il termine delle 72 ore devono essere accompagnate dai motivi del ritardo. Inoltre, se la violazione comporta un rischio elevato per i diritti delle persone, deve essere comunicata a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto.

In particolare, devono essere notificate unicamente le violazioni di dati personali che possono avere effetti avversi significativi sugli individui, causando danni fisici, materiali o immateriali. Ciò può includere, ad esempio:

- la perdita del controllo sui propri dati personali;

- la limitazione di alcuni diritti, la discriminazione;
- il furto d'identità o il rischio di frode;
- la perdita di riservatezza dei dati personali protetti dal segreto professionale;
- una perdita finanziaria, un danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale.

La notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile tramite il seguente indirizzo: https://servizi.gpdp.it/databreach/s/.

Per i dettagli relativi a tale tipologia di incidente, si rimanda alla consultazione del documento dedicato: Procedura per la gestione dei Data Breach.

7.Predisposizione delle relazioni

In conformità con quanto previsto dal D.Lgs. 138/2024, l'Ateneo deve predisporre specifiche relazioni documentali relative agli incidenti informatici classificati come significativi. Tali relazioni, che devono essere condivise al CSIRT Italia tramite l'apposito Referente, hanno lo scopo di garantire la tracciabilità, la trasparenza e l'adempimento degli obblighi normativi, e includono:

- una descrizione dettagliata dell'incidente, delle cause accertate o presunte, e della sua evoluzione temporale;
- una valutazione dell'impatto sui sistemi informativi, sui dati trattati e sui servizi critici aziendali;
- le misure tecniche e organizzative adottate per la gestione dell'incidente e per prevenirne il ripetersi;
- l'elenco delle segnalazioni eventualmente effettuate al CSIRT Italia, all'Agenzia per la Cybersicurezza Nazionale (ACN) e, ove previsto, al Garante per la Protezione dei Dati Personali;
- ogni ulteriore informazione richiesta dalle autorità competenti ai fini della conformità normativa e della cooperazione istituzionale.

La redazione delle relazioni è curata dal SOC manager con il supporto di SOC, Ads, RSGSI. Le tempistiche e le modalità di predisposizione sono definite nel presente documento e nelle procedure interne correlate.

Inoltre, in conformità con quanto previsto dall'articolo 37, comma 3, lettere g) e h) del decreto legislativo n. 137/2024, l'Ateneo è tenuto a garantire una comunicazione tempestiva e appropriata, ove ritenuto opportuno e tecnicamente possibile, previa consultazione con il CSIRT Italia o su intimazione dell'Agenzia per la cybersicurezza nazionale, finalizzata a informare i destinatari dei servizi in merito a eventuali incidenti significativi che possano compromettere la continuità o la sicurezza della fornitura, nonché a fornire indicazioni sulle misure di mitigazione da adottare in risposta a minacce informatiche rilevanti.

8.Riesame e controllo

La presente procedura è soggetta a riesame e aggiornamento periodico almeno ogni due anni, oppure ogniqualvolta si verifichino:

- incidenti di sicurezza informatica rilevanti;

- modifiche significative al contesto regolamentare di riferimento, incluse le normative in materia di sicurezza informatica (come il D.Lgs. 138/2024);
- cambiamenti organizzativi o tecnologici interni rilevanti;
- variazioni significative nel livello di esposizione al rischio.