POL01 - Politica di gestione degli incidenti di sicurezza

Luglio 2026

UNIVERSITAS STUDIORUM MUTINENSIS ET REGIENSIS
1175

UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

Sommario

0 Contesto

La continuità e l'efficienza dei servizi IT sono essenziali per il perseguimento delle missioni istituzionali e accademiche dell'Università. Garantire una risposta tempestiva ed efficace agli incidenti di sicurezza è fondamentale per evitare o limitare interruzioni che possano compromettere le attività di didattica, ricerca e gestione amministrativa.

Sulla base del Decreto Legislativo 4 settembre 2024, n. 138, che recepisce la **Direttiva Europea NIS2**, l'Agenzia per la Cybersicurezza Nazionale (**ACN**) ha inserito l'Università di Modena e Reggio Emilia (di seguito anche solo "Unimore" o "Ateneo")

nell'elenco dei soggetti NIS e classificato come soggetto importante per il settore della ricerca"

Questa designazione sottolinea il ruolo critico degli Atenei nella sicurezza informatica nazionale e nella resilienza delle infrastrutture strategiche, evidenziando la necessità di un approccio strutturato alla gestione degli incidenti.
Con la presente policy, l'Ateneo intende rafforzare la propria capacità di prevenire e gestire gli incidenti di sicurezza, tutelare il proprio patrimonio informativo e garantire la conformità alle normative vigenti.
Il documento disciplina il processo di gestione degli incidenti di sicurezza, definendo in modo chiaro le fasi operative, i ruoli e le responsabilità di tutte le parti coinvolte.

1 Scopo e Applicabilità

Il presente documento ha lo scopo definire tutte le attività organizzative messe in atto al fine di prevenire il verificarsi di possibili incidenti di sicurezza, e le modalità operative necessarie a consentire il superamento o il contenimento di incidenti di sicurezza, individuando Ruoli e Responsabilità degli attori coinvolti. Permette inoltre, attraverso l'analisi e la comprensione dei meccanismi di attacco e delle modalità utilizzate per la gestione dell'incidente, di migliorare continuamente la capacità di risposta agli incidenti.

In esso, viene altresì contemplata l'eventualità in cui un incidente di sicurezza comporti una violazione di dati personali, così come definita dall'art. 4, n. 12 del Regolamento (UE) n. 679/2016 (di seguito, "**Regolamento**" o "**GDPR**").
In tali circostanze, al fine di adempiere agli obblighi previsti dagli artt. 33 e 34 del GDPR, verrà fatto rinvio alla specifica procedura adottata dall'Ateneo per la gestione delle violazioni di dati personali ("**Data Breach Policy**"), garantendo così un trattamento conforme e appropriato degli eventi di data breach. Tutte le violazioni dei dati personali sono incidenti di sicurezza, ma non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali.

L'individuazione, la gestione e la tempestiva segnalazione di un incidente di sicurezza, inclusa la violazione di dati personali, costituiscono una concreta dimostrazione dell'efficacia delle misure adottate dall'Ente ai sensi dell'art. 32 del Regolamento (GDPR). A ciò si affiancano, in un'ottica di sicurezza complessiva, gli obblighi di notifica previsti dalla **Direttiva NIS2**, che impongono agli operatori di servizi importanti, come l'Ateneo, di segnalare prontamente gli incidenti significativi alle autorità competenti, come meglio sarà specificato nel seguito del presente documento.
Questa policy si applica a tutte le risorse e ai servizi informatici gestiti direttamente dall'Ateneo o affidati in outsourcing, garantendo un approccio integrato alla gestione della sicurezza e alla conformità normativa.

2 Termini e Acronimi

Termine/Acronimo	Definizione
GDPR	General Data Protection Regulation (Regolamento UE 2016/679 per la protezione dei dati personali)
NIS 2	Direttiva dell'Unione Europea che stabilisce misure volte a garantire un elevato livello comune di cybersicurezza nei settori essenziali e importanti, imponendo obblighi in materia di gestione del rischio, sicurezza dei sistemi informativi e comunicazione degli incidenti
D.LGS. 138/2024	Recepisce la Direttiva (UE) 2022/2555 – NIS 2 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione europea;
Disponibilità	Proprietà della sicurezza informatica secondo cui i sistemi, i dati e i servizi devono essere accessibili e utilizzabili quando richiesto dagli utenti autorizzati.
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.

Termine/Acronimo	Definizione
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
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.
Sistema informativo e di rete	Qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali.
Data Breach	Violazione della 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.

Tabella 1 – Termini e acronimi

3 Ruoli e Responsabilità

Nella seguente ***Tabella 2***., sono riportati i Ruoli con le rispettive responsabilità che intervengono durante le fasi del processo di gestione degli incidenti da parte di Unimore

Ruolo	Responsabilità
Computer Security Incident Response Team dell'Ateneo (CSIRT Unimore)	Gruppo responsabile della gestione tecnica dell'incidente, dall'analisi iniziale fino alla risoluzione. Parte integrante della Direzione Sistemi Informativi (Ufficio RTD) e presidio qualità (DIAQ), opera all'interno del **Gruppo Sicurezza ICT** dell'Ateneo. È coordinato dal Responsabile della rete di Ateneo. Collabora con il SOC per il monitoraggio, identifica, contiene e rimuove le minacce, e mantiene la tracciabilità delle operazioni e la documentazione degli eventi. Il CSIRT Unimore è composto dalle seguenti figure: • Responsabile della rete di Ateneo (coordinatore) • Responsabile dei sistemi di Ateneo • Responsabile delle attività di sicurezza connesse alla Data Protection • Responsabile della gestione delle identità Unimore • Responsabile dell'adeguamento alle Misure di Sicurezza
DPO	Viene coinvolto dal Responsabile Sicurezza ICT di Ateneo e dal Coordinatore del CSIRT quando l'incidente può comportare una violazione di dati personali. Valuta la qualificazione come Data Breach, supporta la notifica al Garante e la comunicazione agli interessati, garantendo la conformità al GDPR e alla normativa vigente.
RTD	Responsabile per la Transizione al digitale, è membro del CSIRT Unimore. L'RTD è il dirigente della DIAQ.

Ruolo	Responsabilità
Responsabile Sicurezza ICT di Ateneo	Ha il compito di attivare il CSIRT in caso di incidente e di coinvolgere il DPO se l'evento può riguardare dati personali. Coordina i rapporti con Titolare, Dirigenti, HR e Ufficio Legale, e valuta il coinvolgimento di strutture esterne, fornitori ICT o autorità competenti. È membro del CSIRT Unimore
Responsabile MMS	Responsabile dell'adeguamento alle Misure Minime di Sicurezza È membro del CSIRT Unimore
Responsabile CSIRT	Ha il compito di coordinare le attività del CSIRT Unimore collaborando con il Responsabile Sicurezza ICT di Ateneo e di curare la gestione complessiva dell'incidente, dalla notifica agli organi competenti alle fasi di chiusura e ripristino. Copre il ruolo di Referente CSIRT Italia all'interno di ACN
SOC	Struttura specializzata che svolge il monitoraggio continuo della rete e dei sistemi informativi dell'Ateneo, rilevando, analizzando e gestendo in tempo reale eventuali eventi di sicurezza. Opera in sinergia con la DIAQ Effettua la prima validazione tecnica degli alert, determina la severità dell'evento e, nei casi più critici, può attivare autonomamente misure di contenimento (es. isolamento di un host), previo accordo con l'Ateneo. Supporta il CSIRT Unimore nelle fasi di identificazione, contenimento e post-incidente, fornendo evidenze, log e analisi tecniche.
Referente di Sicurezza della Struttura	Individuato in ogni struttura dell'Ateneo, è il punto di contatto locale per la gestione degli incidenti di sicurezza. Opera in stretto coordinamento con la DIAQ e con il CSIRT Unimore

Ruolo	Responsabilità
Centro di Ricerca Interdipartimentale sulla Sicurezza e Prevenzione dei Rischi (CRIS Unimore)	Collabora con il CSIRT Unimore per attività di consulenza e di gestione degli incidenti informatici, per l'attività di VAPT, per la gestione dell'autenticazione MFA e per la formazione in materia di sicurezza informatica rivolta al personale;
COSC (Centro Operativo per la Sicurezza Cibernetica) dell'Emilia-Romagna	Collabora con il CSIRT Unimore attraverso un protocollo di intesa per la prevenzione e il contrasto dei crimini informatici sui sistemi informativi "critici" dell'Ateneo.
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 CybersSecurity) 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.

Tabella 2 – Ruoli e responsabilità

4 Generalità

In linea con quanto definito dal **NIST** (National Institute of Standards and Technology), è possibile individuare diverse fasi per identificare e gestire gli incidenti di sicurezza informatica, tra cui la preparazione agli incidenti, il rilevamento e l'analisi di un incidente di sicurezza, il contenimento, l'eradicazione e il recupero completo, nonché l'analisi e l'apprendimento post-incident,

Nei Paragrafi successivi, rispetto a quanto sopra riportato, verranno analizzate nel dettaglio le diverse fasi relative al processo di gestione degli incidenti di sicurezza.

Figura 1 - Fasi del processo di gestione degli incidenti di sicurezza

A seguire verrà riportato un workflow che sintetizza le attività principali svolte nell'ambito della Procedura di Gestione degli Incidenti di Sicurezza da parte di Unimore.

4.1 Preparazione

La fase di preparazione consente di definire tutte quelle azioni, organizzative ed operative, atte a mitigare i rischi connessi ad un ipotetico incidente di sicurezza.

Si riporta di seguito un elenco esemplificativo e non esaustivo delle azioni **organizzative che il CSIRT Unimore deve seguire,** azioni necessarie affinché la documentazione e le procedure interne risultino utili ed efficaci nel caso di un incidente:

- Mantenere e aggiornare le procedure ed i manuali operativi (playbook) da attuare in caso di incidente di sicurezza;
- Garantire che il processo di gestione degli incidenti di sicurezza (ed i relativi playbook) siano adeguatamente condivisi all'interno della Regione;
- Tenere aggiornato l'elenco del personale incaricato della gestione dell'incidente e modificarne i riferimenti in caso di qualsiasi cambiamento interno al team;
- Mantenere aggiornata la BIA (Business Impact Analysis), l'analisi dei rischi e l'inventario degli Asset;
- Esaminare periodicamente i report di gestione degli incidenti così da garantire che il gruppo preposto per la gestione e risoluzione degli incidenti sia sempre allineato sulla metodologia di mitigazione e risoluzione dell'incidente accorso;
- Condurre una regolare campagna di security awareness per tutti i dipendenti allo scopo di renderli consapevoli delle numerose minacce in ambito informatico ed istruirli a segnalare una possibile minaccia o un comportamento insolito rilevato;

- Condurre regolarmente campagne di phishing rivolte al personale, ai collaboratori e agli studenti, in modo da verificare se gli utenti sono in grado di rilevare un'e-mail malevola prima di cliccare su link o allegati pericolosi;
- Esaminare costantemente le documentazioni rilasciate pubblicamente relative alle più recenti minacce, attori malevoli e tecniche di attacco.

Di seguito sono riportate le **azioni operative**, cioè quelle azioni intraprese o avviate dall'Ateneo per consentire la mitigazione dei rischi legati all'incidente di sicurezza. Nel dettaglio:

- Mantenere attivo un **SOC Security Operation Center) che svolga attività** continuativa di **monitoraggio e analisi degli eventi di sicurezza** in tempo reale, individuando potenziali minacce tramite strumenti e tecniche avanzate
- Eseguire regolarmente il backup dei dati;
- Eseguire periodicamente test di ripristino dei dati;
- Eseguire **PT** (Penetration Test) sugli applicativi esposti su Internet per rilevare e risolvere eventuali vulnerabilità prima che possano essere sfruttate per possibili attacchi informatici;
- Eseguire **VA** (Vulnerability Assessment) prima della messa in produzione di nuovi sistemi o nuovi applicativi, al fine di verificare la presenza o meno di vulnerabilità e se necessario, sottoporle a PT mirati;
- Eseguire periodicamente attività di patching e hardening su tutti i sistemi;
- Aggiornare costantemente gli schemi di rete;
- Predisporre strumenti per la digital forensics;
- Configurare firewall (per la gestione del traffico ammesso o bloccato, intercettazione malware, ecc.);
- Attivare sistemi per il monitoraggio degli eventi di sicurezza su endpoint e server;
- Utilizzare l'MFA (Multi Factor Authentication) per gli accessi e in particolare per gli accessi in VPN;
- Accedere a immagini di installazioni pulite di sistemi operativi ed applicazioni per scopi di ripristino e recupero.

4.1.1 Raccolta delle Prove Legali

Qualora a seguito di un incidente di sicurezza, si renda necessario per l'Ateneo intraprendere un'azione legale (civile o penale) contro una persona fisica o giuridica oppure nel caso in cui ci siano le premesse affinchè l'Ateneo possa essere oggetto si azione legale (civile o penale), è fondamentale ricostruire con precisione e accuratezza la catena di custodia dei dispositivi coinvolti nell'incidente, documentando ogni fase del loro trattamento a partire dal momento della loro consegna.
La ricostruzione deve includere:

- Data e ora della consegna: specificare quando il dispositivo è stato affidato e da chi.

- Identificazione del dispositivo: includere dettagli quali il tipo di dispositivo, il numero di serie, e qualsiasi altro identificativo unico.
- Registrazione dei passaggi: indicare chiaramente chi ha avuto accesso al dispositivo in ogni momento, con le relative date e orari.
- Modalità di conservazione: documentare come il dispositivo è stato custodito per garantirne l'integrità (es. in un'area sicura, sigillato in una busta protettiva, ecc.).
- Interventi effettuati: elencare tutte le operazioni svolte sul dispositivo (es. analisi, copie forensi) specificando da chi e con quali strumenti.
- Consegna ad autorità competenti: qualora il dispositivo venga affidato a terze parti o alle autorità (es. forze dell'ordine, consulenti legali), annotare i dettagli del trasferimento e ottenere una ricevuta.

Questa documentazione deve essere accurata, firmata dalle parti coinvolte in ogni fase, e conservata in modo sicuro per garantire la piena tracciabilità del dispositivo, prevenendo contestazioni sull'integrità dei dati e sull'affidabilità delle prove.

Le evidenze oggettive vengono raccolte e conservate nel cosiddetto **Fascicolo delle evidenze** mantenuto dal CSIRT Unimore al fine di conformarsi ai requisiti di legge applicabili nelle sedi giurisdizionali competenti. Tutta la fase di raccolta delle evidenze viene fatta in modo che le evidenze siano utilizzabili in un processo giuridico. La documentazione dell'incidente comprensiva delle evidenze e delle valutazioni effettuate viene elaborata in maniera tale da non indicare, ove possibile, dati personali. Il tempo di conservazione di tale documentazione **è stabilito in 5 anni dalla chiusura dell'incidente**.

4.2 Identificazione, Segnalazione e Analisi

La fase di identificazione rappresenta il punto iniziale del processo di gestione degli incidenti di sicurezza informatica. In questo momento viene individuata una potenziale minaccia che può compromettere la riservatezza, l'integrità o la disponibilità delle informazioni o dei sistemi aziendali.
I possibili reali incidenti di sicurezza si possono classificare in diverse tipologie, dettagliate come segue (***Tabella 3***), sebbene non sia possibile redigere una lista esaustiva di tutti i possibili vettori di attacco:

Tipologia Incidente	Descrizione
Accesso non autorizzato	Accesso (sia logico che fisico) a reti, sistemi, applicazioni, dati di proprietà dell'Ente da parte di personale non autorizzato.
Denial of Service	Attacco informatico alla disponibilità di una rete o sistema. Qualora abbia successo, comporta la difficoltà all'accesso o la totale indisponibilità di determinati sistemi e/o servizi.

Tipologia Incidente	Descrizione
Codice malevolo	Un virus, worm, trojan, spyware, o qualsiasi altro codice malevolo che infetti un sistema.
Uso inappropriato	Violazione delle politiche di sicurezza e delle disposizioni su corretta gestione dei dati personali gestiti dall'Ente.
Data leakage	Diffusione di informazioni personali a seguito di data breach riuscito.
Alterazione delle informazioni	Modifica del contenuto di dati personali a seguito di una violazione riuscita.
Phishing	Truffa effettuata su Internet, che sfrutta tecniche di ingegneria sociale, attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso.
Furto/smarrimento totale o parziale di apparecchiature che contengono dati personali	Il furto o smarrimento di singoli dispositivi di memorizzazione (documenti analogici, hard disk, memorie di massa rimovibili ecc.) oppure dei computer o archivi che li ospitano. Una violazione dei dati personali sensibili contenuti configura una condizione di data breach che richiede, ai sensi del GDPR, l'attivazione delle specifiche procedure di notifica verso l'autorità Garante e gli utenti coinvolti.
Multiplo	Incidente di sicurezza che comprende due o più di quelli sopra elencati.
Malfunzionamento grave	Danneggiamento di un componente hardware o software, oppure degrado delle performance per cause esterne che possa arrecare impatti gravi alla disponibilità di servizio.

Tipologia Incidente	Descrizione
Disastro	Qualsiasi evento distruttivo, non provocato direttamente da azione di operatori informatici (es.: blackout, incendio, allagamento, terremoto) in grado di condizionare direttamente l'operatività dei sistemi informatici.

Tabella 3 - Tipologia Incidenti

Le segnalazioni di incidenti informatici devono essere indirizzate al **CSIRT Unimore** e possono provenire da diverse fonti:

- **Utenti interni dell'Ateneo:** possono rilevare anomalie quali alterazioni di siti web istituzionali, accessi non autorizzati ai dati o indisponibilità di risorse ICT. In tali casi, l'utente deve segnalare tempestivamente l'evento al **Referente di sicurezza** della propria struttura, che provvede a informare il **CSIRT Unimore**. Qualora ritenga l'incidente di particolare gravità, il Referente contatta inoltre il CSIRT Unimore **telefonicamente**, per garantire un intervento tempestivo.[1]
- **SOC (Security Operation Center):** svolge attività continuativa di **monitoraggio e analisi degli eventi di sicurezza** in tempo reale, individuando potenziali minacce tramite strumenti e tecniche avanzate. Quando rileva un evento anomalo:
  - **esegue una prima analisi tecnica**, valida l'alert e attribuisce un livello di severità;
  - in caso **di severity alta,** può applicare direttamente misure di contenimento immediate (es. isolamento rete, blocco processo), previo accordo operativo con l'Ateneo;
  - in caso di **severity bassa o media**, invia al CSIRT Unimore una segnalazione già contestualizzata.

  La comunicazione tra SOC e CSIRT Unimore avviene tramite i canali ufficiali:
  - e-mail;
  - sistema di ticketing gestito dal SOC;
  - notifiche push su piattaforme di uso comune; contatto telefonico per eventi critici
- **Enti o soggetti esterni:** possono segnalare incidenti informatici tramite i canali ufficiali dell'Ateneo (ad eesempio *csirt@unimore.it*, *abuse@unimore.it*, *urp@unimore.it*), via telefono o attraverso i recapiti pubblicati sul sito istituzionale www.unimore.it. Chi riceve la segnalazione deve rigirarla tempestivamente al CSIRT Unimore.
- **Rilevamento automatico:** attraverso strumenti e piattaforme di sicurezza (es. **SIEM – Security Information and Event Management**) che analizzano in modo continuativo eventi e log dei sistemi, generando segnalazioni automatiche al SOC o al CSIRT Unimore per la successiva valutazione e gestione.

Fonte Segnalazione	Owner Segnalazione	Modalità di Segnalazione	Canale Segnalazione

[1] Nella prassi potrebbe accadere che la segnalazione dell'incidente venga erroneamente trasmessa al DPO. In tal caso, il DPO dovrà coinvolgere il CSIRT d'Ateneo, nella persona del Responsabile Sicurezza, condividendo tutte le informazioni ricevute.

Segnalazione pervenuta da utenti interni dell'Ateneo	• Docenti; • Staff; • Studenti; • Soggetto esterno identificato nel sistema Identity di Ateneo	L'incidente deve essere segnalato al Referente di sicurezza di struttura che poi provvederà ad allertare il CSIRT Unimore.	I dati di contatto del referente di ciascuna struttura sono riportati nelle relative sedi organizzative.
	• Referente di sicurezza di struttura.	L'incidente rilevato direttamente dal Referente di Sicurezza di struttura, viene da questi comunicato direttamente al CSIRT Unimore via mail o telefono	• Comunicazione telefonica al numero: 059 2058903; • Comunicazione mediante mail al seguente indirizzo: csirt@unimore.it
Segnalazione pervenuta dall'esterno dell'Università	• Garr; • Gestori di un Servizio; • Partner	Via mail o telefono	• Comunicazione telefonica al numero: 059 2058903; • Comunicazione mediante mail al seguente indirizzo: csirt@unimore.it
SOC	SOC	Attraverso i canali concordati con il CSIRT Unimore	• Comunicazione telefonica al numero: 059 2058903; • Comunicazione mediante mail al seguente indirizzo: csirt@unimore.it

Tabella 4 – Fonti segnalazioni incidenti

Nel caso in cui l'evento sia stato rilevato dal SOC, la prima analisi tecnica è già stata svolta dallo stesso SOC, che trasmette al CSIRT Unimore un alert validato e classificato, riducendo i falsi positivi e accelerando l'avvio della fase di gestione da parte del CSIRT Unimore.
Se la fonte della segnalazione è un **utente interno dell'Ateneo** o un **soggetto esterno**, il **CSIRT Unimore** ne verifica la fondatezza e, in caso positivo, **apre formalmente l'incidente** secondo la procedura prevista:

- In primo luogo, Il **Responsabile Sicurezza ICT di Ateneo**, insieme agli altri componenti del CSIRT Unimore – e, se necessario, con il supporto del CRIS, del COSC e di eventuali appaltatori dei servizi di assistenza o manutenzione sistemistica – procede alla **valutazione della gravità** dell'incidente di sicurezza, servendosi, a sua discrezione, della **matrice qualitativa** rappresentata nella seguente tabella di gravità (***Tabella 5***), fermo restando il suo potere discrezionale nella classificazione finale.
- Durante questa fase, qualora emergano elementi che possano far sospettare un **data breach**, il Responsabile Sicurezza informa tempestivamente il DPO, seguendo le

istruzioni riportate al seguente paragrafo (*4.2.1 Data Breach coinvolgimento del DPO*), in modo da attivare immediatamente eventuali adempimenti normativi e procedurali.

- Il **CSIRT Unimore apre un ticket** sul sistema di gestione dedicato (denominato ***CSIRT MANAGER***), con lo scopo di **tracciare tutte le azioni intraprese** per il contenimento e la risoluzione dell'evento.
  Nel ticket devono essere registrate almeno le seguenti informazioni:
  - Nome e contatti del segnalante;
  - Ora della segnalazione;
  - Natura e descrizione dell'incidente;
  - Eventuali apparecchiature o persone coinvolte (e relativa posizione);
  - Modalità e arco temporale di rilevazione dell'incidente.

Qualora l'incidente sia stato rilevato dal SOC, quest'ultimo trasmette al CSIRT Unimore le informazioni tecniche da registrare nel ticket, compresi log, timeline e misure di contenimento eventualmente già applicate. Il CSIRT Unimore integra tali informazioni nella documentazione ufficiale.

Gravità incidente di sicurezza	Descrizione
Alta	Il grado di compromissione di servizi e/o sistemi è elevato. Si rilevano danni consistenti sugli asset. Il ripristino è di medio o lungo periodo. L'incidente presenta una tra le seguenti condizioni: • Danni a persone e rilevanti perdite di produttività • Compromissione di sistemi o di reti in grado di permettere accessi incontrollati a informazioni confidenziali • Siti web violati o utilizzati a fini di propagazione di materiale terroristico o pornografico • Frode o attività criminale che coinvolga servizi forniti dall'Ateneo • Impossibilità tecnica di fornire uno o più servizi critici a un elevato numero di utenti per un intervallo di tempo superiore ai 30 minuti nell'arco di una giornata • Impossibilità tecnica di fornire uno o più servizi di criticità media per un periodo di tempo superiore ai 30 giorni lavorativi • Significativa perdita economica, di immagine e/o reputazione nel confronto del pubblico o degli utenti

Media	L'incidente non presenta nessuna condizione che porti alla catalogazione "gravità alta". Il grado di compromissione di servizi e/o sistemi è di una certa rilevanza e possono essere rilevati danni sugli asset di una certa consistenza. Il ripristino ha tempi che non compromettono la continuità del servizio. L'incidente presenta una tra le seguenti condizioni: • Compromissione di server • Degrado di prestazioni relativo ai servizi offerti dall'ente con conseguente perdita di produttività da parte degli utilizzatori • Attacchi che provocano il funzionamento parziale o intermittente della rete • Impossibilità tecnica di fornire uno o più servizi critici ad un elevato numero di utenti per intervalli di tempo inferiori ai 30 minuti di tempo ripetuti su più giornate • Impossibilità tecnica di fornire uno o più servizi critici ad una piccola parte di utenti per un periodo di tempo superiore ai 30 minuti di tempo nell'arco di una o più giornate • Basso impatto in termini di perdita economica, di immagine e/o reputazione nei confronti degli utenti
Bassa	L'incidente non presenta nessuna condizione che porti alla catalogazione "gravità alta o media". Non vengono compromessi asset o servizi. L'incidente presenta le seguenti condizioni: • Interruzione dell'attività lavorativa di un numero ristretto di dipendenti e per un breve periodo di tempo. • Contaminazioni da virus in un medesimo sito ma comunque identificate dai sistemi anti-malware • Nessuna o limitata perdita di operatività o di business da parte di un ridotto numero di dipendenti.

Tabella 5 – Gravità incidenti

4.2.1 Data Breach (coinvolgimento del DPO)

Quando il Responsabile Sicurezza ICT di Unimore, di concerto con il CSIRT Unimore, accerta che l'incidente abbia coinvolto, o possa potenzialmente coinvolgere, **dati personali**, deve **contattare senza ingiustificato ritardo il Data Protection** Officer (DPO), in attuazione di quanto previsto dalla "Procedura di gestione della violazione dei dati personali", richiamato dall'art. 30 pubblicata in calce del Regolamento di Ateneo in materia di protezione dei dati personali (*https://www.unimore.it/sites/default/files/2024-07/RegolamentoPrivacy.pdf*).
Il contatto con il DPO deve avvenire **tramite posta elettronica** all'indirizzo **dpo@unimore.it**, seguendo le indicazioni riportate di seguito:

- **Oggetto della mail:** *"!! POTENZIALE DATA BREACH – COMUNICAZIONE CSIRT UNIMORE";*
- **Allegato:** compilare e allegare, anche in forma preliminare qualora non si disponga di tutte le informazioni, l'**Allegato A** alla "Procedura di gestione della violazione dei dati personali" (Modulo per la raccolta informazioni);
- **Corpo del messaggio:** indicare la **data** in cui il Responsabile Sicurezza ha avuto conferma del coinvolgimento di dati personali e fornire un **contatto telefonico diretto** per favorire un confronto tempestivo.

Tale comunicazione deve essere effettuata **senza ritardi ingiustificati**, al fine di consentire al DPO di valutare prontamente la qualificazione dell'evento come **Data Breach** e di attivare, se necessario, le procedure previste dalla **"Procedura di gestione della violazione dei dati personali".**

A fronte delle informazioni ricevute e degli eventuali successivi confronti intercorsi con il **Responsabile Sicurezza**, il **DPO** valuta se l'incidente di sicurezza debba essere qualificato come Data Breach.

- In caso di esito positivo, il **DPO** dà attuazione a quanto previsto dalla **Procedura di gestione della violazione dei dati personali.**
- In caso di esito negativo, il **DPO** comunica al **Responsabile Sicurezza** che l'incidente di sicurezza non deve essere qualificato come Data Breach.

Se il Responsabile Sicurezza ICT di Unimore è assente, la procedura sopra descritta deve essere garantita dal Coordinatore del CSIRT Unimore.

4.2.2 Notifica al Garante per la protezione dei dati personali

In ogni caso, ai sensi dell'articolo 33 del Regolamento (UE) 2016/679, la violazione dei dati personali, comporta, in capo al titolare del trattamento, l'obbligo di notificare al Garante per la protezione dei dati personali l'avvenuta violazione.
Tale notifica è effettuata per il tramite del Responsabile Sicurezza ICT di Ateneo e del **CSIRT Unimore** in coordinamento con **il DPO.**
La notifica deve essere trasmessa **senza ingiustificato ritardo** e, ove possibile, entro il termine di 72 ore dal momento in cui il Titolare è venuto a conoscenza della violazione, e deve includere almeno le seguenti informazioni:

- una descrizione della natura della violazione dei dati personali, comprensiva della tipologia di dati compromessi, delle categorie e del numero approssimativo di interessati e di record coinvolti;
- i dati di contatto del DPO (nome e recapiti) o di altro punto di contatto presso cui ottenere ulteriori informazioni;
- una descrizione delle probabili conseguenze della violazione dei dati personali e dei rischi per i diritti e le libertà degli interessati;
- una descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione e mitigarne i possibili effetti negativi;
- eventuali ulteriori informazioni ritenute utili ai fini della valutazione dell'incidente.

Qualora la notifica non possa essere effettuata entro il termine di 72 ore, la comunicazione all'Autorità di controllo deve essere corredata dei motivi del ritardo.

Si rammenta infine che le violazioni dei dati personali che comportano un rischio elevato per i diritti e le libertà delle persone fisiche devono essere comunicate agli interessati senza ingiustificato ritardo, ai sensi dell'articolo 34 del Regolamento (UE) 2016/679.

La comunicazione agli interessati deve avvenire secondo quanto previsto dalla Data Breach Policy dell'Ateneo.

4.2.3 Notifica al CSIRT ITALIA

In conformità con il D.Lgs. 138/2024, attraverso la figura del **Coordinatore del CSIRT Unimore**, 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 pre-notifica 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 trasmissione dell'ultima notifica 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 CSIRT Italia ha predisposto una specifica piattaforma per la segnalazione di incidenti di sicurezza raggiungibile al seguente link: https://www.csirt.gov.it/segnalazione.

Il CSIRT Unimore si conforma alle linee guida di CSIRT Italia, facendo riferimento ai seguenti documenti:

- ***Allegato B,*** per il dettaglio delle informazioni e delle tempistiche da condividere con il CSIRT Italia
- ***Allegato C***, per la notifica ai destinatari dei servizi degli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi e
- ***Allegato G***, per le istruzioni operative per la notifica degli incidenti sulla piattaforma messa a disposizione dal CSIRT Italia.

4.3 Attivazione della procedura e monitoraggio delle attività

L'attivazione della procedura di gestione dell'incidente è di competenza del **CSIRT Unimore** che opera in modalità differenziata in funzione della gravità attribuita all'evento.

In presenza di un incidente di gravità "**Alta**"

- **il Coordinatore del CSIRT Unimore e il Responsabile Sicurezza ICT** compilano il **Report incidente di sicurezza** (***Allegato E***), nelle parti disponibili al momento dell'attivazione. Il rapporto viene poi condiviso con il DPO in caso di coinvolgimento di dati personali.
- Qualora l'evento sia stato rilevato dal **SOC**, il SOC stesso fornisce il contributo iniziale al Rapporto, indicando le modalità di rilevazione, la prima analisi tecnica, il livello di gravità attribuito, i sistemi coinvolti e le eventuali misure di contenimento già adottate. Il CSIRT Unimore verifica e completa le informazioni, garantendo la continuità della gestione tecnica. Il Rapporto viene completato al termine dell'incidente e conservato per almeno **cinque anni** in formato elettronico, in una collocazione soggetta a backup periodico e ad accesso controllato. Qualora l'incidente comporti un impatto significativo sulla continuità operativa dei servizi dell'Ateneo, il CSIRT attiva le strutture competenti e coordina le azioni con il Piano di continuità operativa.

In presenza di incidenti di gravità "**Media" o "Bassa"**

- la gestione può essere condotta direttamente dal **CSIRT Unimore**, fermo restando il coinvolgimento del **DPO** nei casi di violazione di dati personali
- Qualora l'evento sia rilevato dal SOC, quest'ultimo trasmette al CSIRT una segnalazione validata e contestualizzata; in tali casi, la redazione del **Report incidente di sicurezza** non è obbligatoria, salvo specifiche esigenze, restando comunque necessario garantire la tracciabilità delle informazioni e delle attività svolte attraverso il sistema di ticketing.

In ogni caso, le attività di gestione degli incidenti contribuiscono alla base informativa dell'Ateneo in materia di sicurezza e supportano le successive fasi di contenimento, rimozione, ripristino e miglioramento continuo del sistema di protezione.

5 Azioni di Contenimento

Le operazioni di contenimento hanno due importanti finalità:

- evitare che il danno si propaghi o, almeno, limitarne la diffusione;
- acquisire e preservare eventuali evidenze digitali utili a fini di analisi o di indagine, prima che possano essere compromesse.

A tal fine è necessario:

- identificare i sistemi coinvolti o potenzialmente compromessi;
- raccogliere e mettere in sicurezza le evidenze digitali in modo valido dal punto di vista forense;
- documentare in modo dettagliato tutte le operazioni eseguite, al fine di garantirne la tracciabilità e l'utilizzabilità in sede tecnica o legale.

Le attività di contenimento devono essere eseguite da personale qualificato, ovvero da tecnici dell'Ateneo o da personale incaricato e opportunamente formato, sotto la supervisione e responsabilità del **CSIRT Unimore.**

Quando l'incidente è rilevato dal **SOC**, quest'ultimo supporta il CSIRT Unimore fornendo analisi, log, evidenze tecniche e, ove previsto, applicando direttamente azioni di contenimento automatiche o manuali.

Il SOC procede secondo le seguenti logiche operative:

- **Severity alta**: può isolare host, bloccare traffico o disattivare credenziali compromesse, previo accordo con l'Ateneo;
- **Severity media o bassa**: non esegue azioni dirette, ma notifica l'evento al CSIRT Unimore e ai tecnici competenti.

Tutti gli alert gestiti dal SOC vengono validati e contestualizzati prima dell'inoltro al CSIRT Unimore, riducendo i falsi positivi e migliorando la tempestività della risposta

Tutte le operazioni eseguite devono essere riportate nel **Rapporto di Incidente di Sicurezza**, specificando:

- data e ora delle azioni eseguite sui sistemi, applicazioni o dati;
- generalità delle risorse che hanno materialmente eseguito le operazioni;
- risultati conseguiti.

Il **Coordinatore del CSIRT Unimore** comunica al **Responsabile Sicurezza ICT** quanto eseguito al termine di questa fase, raccordandosi, ove **necessario, con l'Ufficio Legale dell'Ateneo** per la trasmissione della documentazione utile alle eventuali azioni di competenza.
Se l'incidente di sicurezza è stato qualificato come **Data Breach**, le attività di contenimento e ripristino dovranno essere condivise anche con il **DPO**, al fine di consentire la compilazione del Registro dei Data Breach e l'eventuale notifica all'Autorità o agli interessati (sul punto *cfr.* 4.2.1 e 4.2.2, della presente politica).

6 Rimozione e Ripristino

Le operazioni di rimozione e ripristino hanno l'obiettivo di eliminare in modo definitivo la causa dell'incidente, ristabilendo un livello adeguato di sicurezza dei sistemi coinvolti e garantendo il ritorno alla piena operatività in condizioni controllate.

Se l'incidente è stato inizialmente rilevato dal **SOC**, quest'ultimo fornisce al **CSIRT Unimore** la prima analisi tecnica e le eventuali azioni di rimozione o mitigazione attivate in autonomia per evitare aggravamenti.

Dopo la fase di contenimento, **il CSIRT Unimore**, con il supporto del SOC, valuta le misure tecniche necessarie per neutralizzare le vulnerabilità sfruttate, rimuovere eventuali elementi malevoli e ripristinare la funzionalità dei sistemi.

Le attività possono comprendere, a titolo esemplificativo:

- aggiornamento o reinstallazione del sistema operativo o di componenti software compromessi;
- eliminazione di servizi, applicazioni o configurazioni non sicure (hardening del sistema);
- disinfezione o, ove più efficace, ricostruzione completa dei sistemi colpiti;
- verifica e aggiornamento delle policy di sicurezza e delle regole di detection.

Durante questa fase, il **SOC** continua a monitorare gli asset coinvolti per assicurare che le anomalie non si ripresentino e che le misure correttive siano efficaci. In caso di nuovi indicatori di compromissione, viene avviata una nuova segnalazione verso il CSIRT Unimore, che valuta se proseguire con ulteriori azioni di bonifica o rafforzamento delle difese.
Le operazioni di rimozione e ripristino possono comportare impatti tecnici ed economici rilevanti (acquisto di hardware o licenze, interventi esterni, test di sicurezza).
Il **Coordinatore del CSIRT Unimore**, in coordinamento con il **Responsabile Sicurezza ICT** e gli uffici competenti, redige un report tecnico-economico che dettaglia tempi, costi e risorse necessarie, così da consentire l'attuazione delle azioni approvate in modo formalizzato.

Al termine delle attività, il **CSIRT Unimore** verifica che:

- i sistemi siano stati correttamente ripristinati;
- le vulnerabilità originarie siano state eliminate o mitigate;
- siano state implementate le misure preventive per evitare il ripetersi dell'incidente;
- il SOC non rilevi ulteriori eventi anomali correlati.

Solo dopo queste verifiche l'incidente può considerarsi chiuso, e viene predisposto il Rapporto di chiusura dell'incidente con la documentazione delle attività svolte, delle evidenze raccolte e delle misure di prevenzione adottate.

6.1 Attività post-incidente

La fase post-incidente coinvolge tutte le risorse impiegate nella gestione e risoluzione dell'evento, con l'obiettivo di analizzare le cause, valutare l'efficacia delle azioni intraprese e individuare misure correttive o preventive per evitare il ripetersi di incidenti simili.

1. **Riattivazione dei sistemi**

Il **Responsabile Sicurezza ICT**, in collaborazione con il **Coordinatore del CSIRT Unimore**, il **SOC** e i referenti tecnici competenti, definisce il piano di riattivazione dei servizi impattati, autorizzando il ritorno in produzione dei sistemi coinvolti solo dopo aver verificato il ripristino della sicurezza operativa.
Il SOC opera in raccordo con il CSIRT Unimore per effettuare un monitoraggio rafforzato degli asset ripristinati, così da confermare l'assenza di indicatori di compromissione e la stabilità delle misure correttive.

2. **Documentazione e archiviazione**

Tutti gli incidenti devono essere documentati nel **Registro degli incidenti** gestito dal CSIRT Unimore tramite la piattaforma **CSIRT MANAGER (https://csirtmanager.unimore.it)** corredato da eventuale documentazione integrativa ed evidenze tecniche.

I **Data Breach** sono archiviati separatamente, anche se non notificati all'Autorità Garante e/o agli interessati, così come previsto dalla Data Breach Policy.

Il **Responsabile Sicurezza ICT** redige e firma digitalmente il **Report finale sull'incidente**, che viene conservato in modo riservato e sicuro per almeno cinque anni.

3. **Analisi post-incidente**

A incidente concluso, il **Responsabile Sicurezza ICT** convoca una **riunione di revisione post-incidente** con i membri del **CSIRT Unimore**, ed eventualmente del **SOC** e degli altri gruppi tecnici coinvolti, per esaminare:

- le cause tecniche e procedurali dell'incidente;
- l'efficacia delle misure adottate di contenimento, rimozione e ripristino;
- le criticità operative o organizzative riscontrate.

Il SOC contribuisce alla revisione post-incidente fornendo log, timeline, analisi comportamentali e informazioni sugli alert generati, supportando l'identificazione delle cause radice e delle eventuali lacune di detection.

4. **Azioni migliorative**

Durante la revisione vengono individuate e pianificate eventuali azioni di miglioramento, tra cui:

- aggiornamento di policy, procedure o strumenti di sicurezza;
- revisione delle regole di monitoraggio e detection gestite dal SOC;
- attività di formazione e sensibilizzazione del personale;
- rafforzamento delle misure di mitigazione del rischio.

Un **verbale della riunione post-incidente** viene redatto da parte del **CSIRT Unimore** condiviso con le strutture coinvolte, al fine di integrare le lezioni apprese nei processi di sicurezza dell'Ateneo

Eventuali aggiornamenti alle regole di detection e monitoraggio (es. SIEM, EDR, log enrichment) sono valutati e implementati congiuntamente da SOC e CSIRT Unimore.

7 Matrice RACI

Di seguito sono rappresentati i ruoli e le responsabilità per ogni fase del processo di gestione degli incidenti di sicurezza, secondo il Modello R.A.C.I.:

- **Responsible**, soggetto che esegue materialmente l'attività;
- **Accountable**, soggetto responsabile dell'attività;
- **Consulted**, soggetto che è consultato durante lo svolgimento dell'attività e supporta il Responsible;
- **Informed**, soggetto che deve essere informato dell'avvio e della conclusione dell'attività.

Fase	Attività	Coordinatore CSIRT Unimore	Resp. Sicurezza ICT Unimore	SOC	RFS	Utenti Interni	Fornitori e Utenti esterni	DPO
Preparazione	Preparazione	A	R	C	I	I	I	I
Identificazione, segnalazione e analisi	Segnalazione Utenti o Soggetti Esterni	A	I	I	R	I	I	I
	Rilevamento SOC	A	I	R	I	I	I	I
	Prima analisi tecnica (segnalazioni non SOC)	R	C	I	C	I	C	I
	Prima analisi tecnica (segnalazioni SOC)	C	I	R	I	I	I	I
	Classificazione gravità	R	A	C	I	I	I	C

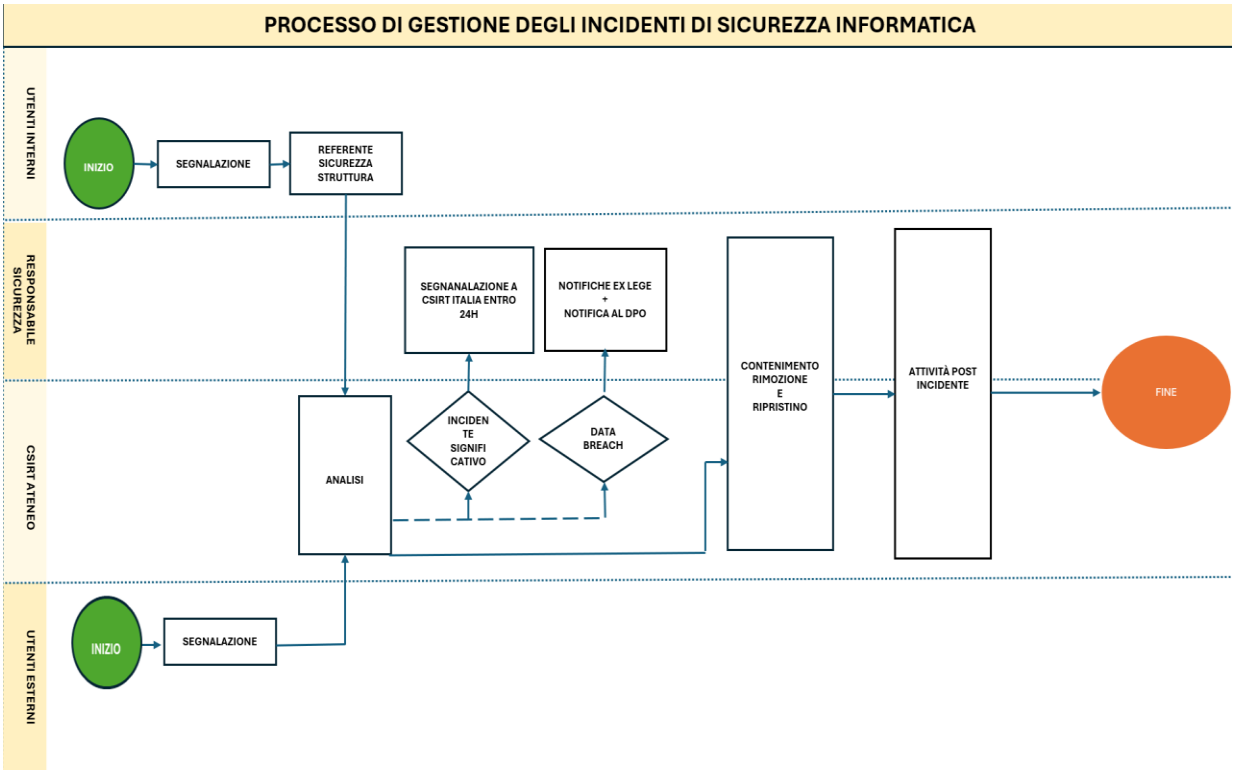
	dell'incidente							
	Apertura del ticket	R	A	C	C	C	C	I
Contenimento eradicazione e ripristino	Contenimento, eradicazione e ripristino	R	A	C/R*	C	C	C	I
Attività post-incidente	Riunione di analisi post-incidente	R	A	C	C	I	I	C

*Le attività del SOC descritte nella presente matrice assumono rilevanza diretta e operativa solo nei casi in cui l'incidente sia stato rilevato dal SOC stesso. Negli altri scenari il SOC opera in supporto al CSIRT Unimore, fornendo analisi tecniche, log, evidenze, alert validati, contributo alla classificazione e monitoraggio degli asset coinvolti

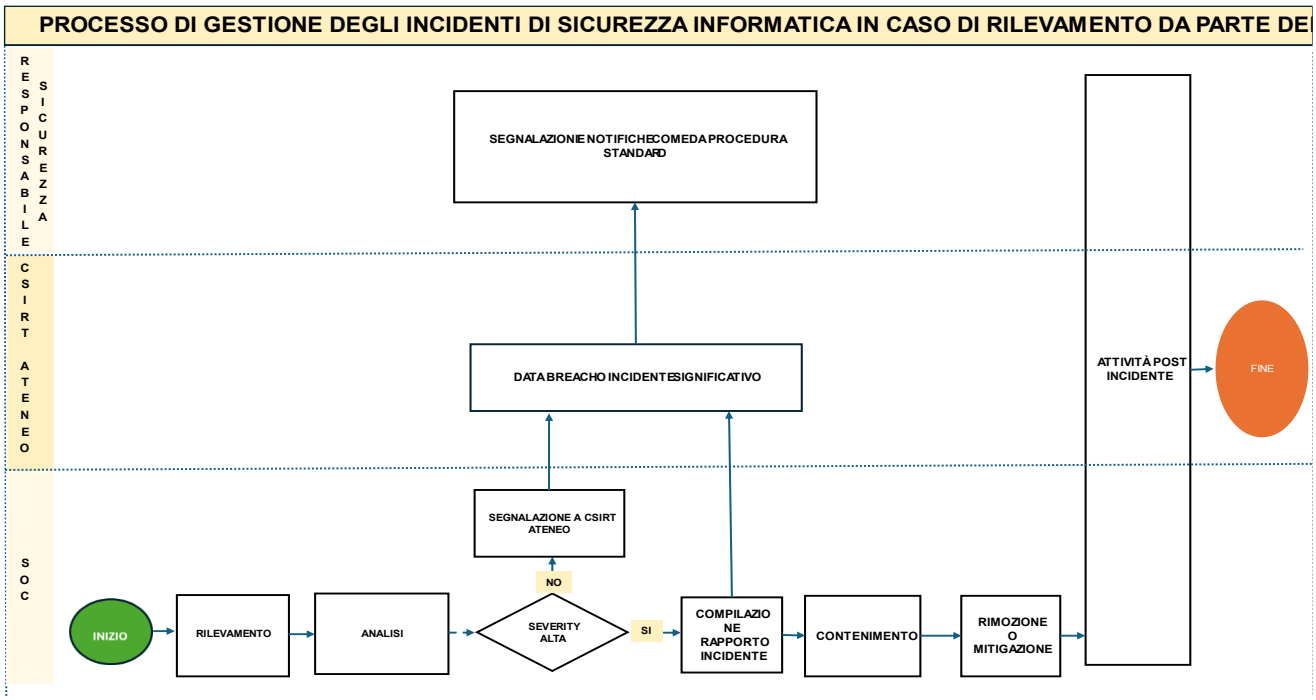
8 Workflow Incidente

I workflow seguenti rappresentano due scenari distinti di gestione degli incidenti di sicurezza. Il primo descrive il flusso operativo standard, attivato quando l'incidente viene segnalato da utenti interni o soggetti esterni o sistemi, mentre il secondo riguarda il caso in cui l'evento venga rilevato direttamente dal SOC, che avvia una prima analisi tecnica e, ove necessario, le prime azioni di contenimento prima del coordinamento con il CSIRT Unimore.

Flusso operativo standard



Evento rilevato direttamente dal SOC



9 Allegati

- ***Allegato A "Modulo per la raccolta informazioni"; richiesto dalla "Procedura di gestione della violazione dei dati personali***

Allegato A "Modulo per la raccolta informa

- ***Allegato B "Linee guida segnalazioni CSIRT"; - a cura di CSIRT ITALIA***

Allegato B_Linee guida segnalazioni CS

- ***Allegato C "Comunicazione ai destinatari dei servizi impattati" - a cura di CSIRT ITALIA***

Allegato C_Comunicazione ai c

- ***Allegato G "Istruzioni operative per la notifica degli incidenti sulla piattaforma" - a cura di CSIRT ITALIA***

Allegato G_Istruzioni Operative alla notifica

- ***Allegato E "Report incidente di Sicurezza" – da compilare obbligatoriamente in caso di incidente di gravità Alta***

MOD01_Report Incidente di Sicurezza

9.1 Riferimenti ad altre politiche di Ateneo

- Testo completo del Regolamento Privacy di Ateneo "REGOLAMENTO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI IN ATTUAZIONE DEL REGOLAMENTO UE 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO E DEL DECRETO LEGISLATIVO 30 GIUGNO 2016, N. 196 CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI" in vigore dal 07/05/2019 con particolare riferimento all'art.27 dove si menziona il **Gruppo Sicurezza ICT** (all'interno del quale opera il CSIRT Unimore) e all'art. 30 che menziona le procedure di Data Breach.
  https://www.unimore.it/sites/default/files/2024-07/RegolamentoPrivacy.pdf
- "Procedura di gestione della violazione dati (Data Breach)" aggiornata al 21/06/2024
  https://www.unimore.it/sites/default/files/2024-07/RegolamentoPrivacy.pdf