Gestione degli incidenti di sicurezza

Università degli Studi di Modena e reggio Emilia

21.06.2024

Sommario

POL01 - GESTIONE DEGLI INCIDENTI DI SICUREZZA 1
0 SCOPO E APPLICABILITÀ 3
1 RESPONSABILITÀ 4
2 GENERALITÀ 6
2.1 DATA BREACH AI SENSI DEL GDPR 6
3 PROCEDURA DI GESTIONE DEGLI INCIDENTI DI SICUREZZA 7
3.1 PREPARAZIONE 8
3.2 IDENTIFICAZIONE E ANALISI DELL'INCIDENTE 8
3.3 VALUTAZIONE D'IMPATTO DELL'INCIDENTE 10
3.4 VALUTAZIONE DEI RISCHI DERIVANTI DAL VERIFICARSI DEL DATA BREACH 13
3.5 COMUNICAZIONE DEGLI INCIDENTI 14
3.6 LA NOTIFICA DELLA VIOLAZIONE AL GARANTE 14
3.7 LA NOTIFICA DELLA VIOLAZIONE AGLI INTERESSATI 14
3.8 ATTIVAZIONE DELLA PROCEDURA E MONITORAGGIO DELLE ATTIVITÀ 14
3.9 CONTENIMENTO, RIMOZIONE E RIPRISTINO 15
3.9.1 Contenimento a breve termine *16*
3.9.2 Contenimento a lungo termine *17*
3.9.3 Rimozione *18*
3.9.4 Ripristino *19*
3.10 ATTIVITÀ POST-INCIDENTE 19
4 ALLEGATI 22
4.1 RAPPORTO INCIDENTE DI SICUREZZA 22
Premessa *22*
Descrizione dettagliata dell'incidente – compilare il modulo allegato *22*
Note *22*
4.2 RIFERIMENTI AD ALTRE POLITICHE DI ATENEO 22

Indice tabelle

Tabella 1 - Tipologia Incidenti 12
Tabella 2 - Tassonomia Incidenti 14

0 Scopo e Applicabilità

Il presente documento rappresenta il riferimento dell'Università di Modena e Reggio Emilia (di seguito Unimore) per la regolamentazione della gestione degli incidenti di sicurezza informatica che possano occorrere ai servizi e ai dati gestiti.

La corretta gestione degli incidenti di sicurezza permette di evitare o minimizzare la compromissione dei dati dell'Ente in caso di incidente; 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.

Il presente documento considera anche il caso in cui l'incidente di sicurezza comporti una violazione di dati personali, così come definita dall'art. 4, n. 12 del Regolamento (EU) n. 679/2016 (di seguito **Regolamento** o **GDPR**).

In tali casi, anche per adempiere agli obblighi previsti dagli artt. 33 e 34 del GDPR, il presente documento richiama l'applicazione della specifica procedura ("*Procedura di gestione della violazione dei dati personali "**Data Breach Policy***") redatta dall'Ateneo al fine di una corretta gestione delle violazioni di dati personali (c.d. "**Data Breach**")

Si rappresenta che l'art. 32 del suddetto Regolamento dispone che debbano essere approntate misure tecniche e organizzative per garantire un livello adeguato di sicurezza dei dati personali. Individuare, indirizzare e segnalare tempestivamente un incidente di sicurezza, come una violazione di dati, è espressione dell'adeguatezza delle misure implementate dall'Ente.

Tutte le violazioni dei dati personali sono incidenti di sicurezza, ma non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali.

Il presente documento è applicabile alle risorse ed ai servizi di tipo informatico gestiti in modo diretto oppure esternalizzato da parte dell'Ateneo.

1 Responsabilità

La criticità del processo di gestione degli incidenti di sicurezza informatica e del Data breach deve essere opportunamente affrontata da una unità organizzativa competente, in possesso di adeguata formazione e in grado di prendere rapidamente le decisioni imposte dalla delicatezza del compito assegnato.

L'Ateneo ha istituito con il Regolamento 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 un **Gruppo Sicurezza ICT (**di seguito **Gruppo)** con le seguenti competenze:

- rappresentare il punto di riferimento univoco a cui il personale dell'Ente deve rivolgersi per segnalare un potenziale incidente oppure un comportamento sospetto;
- gestire tutte le attività inerenti all'analisi e alla gestione di un incidente di sicurezza, ivi comprese quelle relative alla sua notifica e documentazione;
- garantire la disponibilità delle liste di contatti (es.: personale dipendente, collaboratori, fornitori), necessarie per la gestione di un incidente di sicurezza;
- garantire che il processo di gestione degli incidenti sia sempre adeguato alle esigenze aziendali, provvedendo che il medesimo sia sempre aggiornato.

I riferimenti del Gruppo (nominativi, indirizzo e-mail, numeri di telefono ecc.) sono mantenuti **dal Responsabile per la transizione al digitale** di Ateneo e includono

- Responsabile per la transizione al digitale (di seguito **RTD**);
- Il Responsabile dell'Ufficio Reti, Fonia, Sistemi e Cybersecurity (di seguito **Responsabile sicurezza**) della Direzione Sistemi Informativi (Ufficio RTD) e Assicurazione Qualità (di seguito **DIAQ**) che è la figura che ha in carico la gestione degli incidenti;
- Il Data Protection Officer (di seguito **DPO**);
- Il responsabile del Centro di ricerca sulla Sicurezza e Prevenzione dei rischi (di seguito **CRIS**);
- Il Responsabile dell'adeguamento alle Misure Minime di Sicurezza (di seguito **Responsabile MMS**).

All'interno del **Gruppo** opera il **Computer Security Incident Response Team** (di seguito **CSIRT**) che si configura come il nucleo operativo del Gruppo.
È costituito da

- Il **Responsabile sicurezza;**
- Gli Access Port Manager (di seguito **APM**) della rete Unimore;
- I tecnici del Settore Rete della DIAQ**;**
- I tecnici del Settore Sistemi della DIAQ**;**
- Il **Responsabile MMS.**

Nel corso del processo di gestione di un incidente di sicurezza informatico e, eventualmente, di un Data breach, il **Gruppo** potrà essere coadiuvato di volta in volta

dal Direttore/Dirigente della struttura i cui dati sono stati oggetto di Data breach e da tutti coloro che il Gruppo stesso riterrà necessario coinvolgere, a seconda della tipologia di incidente e della tipologia di dati coinvolti.

Nelle attività di gestione di un incidente di sicurezza deve essere coinvolto il **DPO** dell'Ateneo, il quale esercita le proprie funzioni di monitoraggio della conformità in caso di Data breach, fornendo il proprio parere in ordine alla necessità di effettuare la notifica e, quindi, sulle valutazioni precedentemente descritte.

Il **Responsabile Sicurezza** ha il compito di attivare il **CSIRT** in caso di incidenti di sicurezza. Tutte le volte in cui l'incidente di sicurezza presenta anche solo potenzialmente profili rilevanti in tema di protezione dei dati personali, il Responsabile Sicurezza coinvolge tempestivamente il **DPO** al fine qualificare o meno l'incidente di sicurezza come Data Breach (in merito alle specifiche modalità di coinvolgimento del **DPO** si veda, in particolare, il successivo Paragrafo 3.2 "Identificazione e analisi dell'incidente").

Il **Responsabile Sicurezza** deve inoltre coinvolgere, a seconda della gravità dell'incidente, il Titolare o i Dirigenti competenti per gli aspetti di comunicazione interna ed esterna e nel caso, durante la gestione dell'incidente, emergano responsabilità da parte di personale interno dell'Ateneo deve coinvolgere la Direzione Risorse Umane ed eventualmente l'Ufficio Legale dell'Ateneo.

Nel caso in cui le attività di analisi dell'incidente di sicurezza evidenzino particolari difficoltà oppure impatti che si estendono al di fuori del perimetro dell'Ateneo, il **Responsabile Sicurezza** deve valutare l'opportunità o la necessità, di coinvolgere le strutture di riferimento regionali e nazionali (ad esempio Lepida ScpA considerando il proprio ruolo nell'ambito della sicurezza della Community Network, CERT-PA, …). Inoltre, il **Responsabile Sicurezza** deve prevedere il coinvolgimento dei propri fornitori di servizi ICT per il supporto all'analisi e per l'ottenimento di informazioni utili oltre alle autorità di pubblica sicurezza nel caso in cui l'incidente possa presentare risvolti dal punto di vista penale.

In ogni struttura dell'Ateneo è individuato un **Referente di sicurezza della struttura** che opera in stretto contatto con la DIAQ**.**

Di seguito sono descritti i comportamenti, le attività e i regolamenti che l'Ateneo ha attivato per cercare di prevenire gli incidenti di sicurezza, riducendo il livello di rischio e l'esposizione a possibili attacchi informatici.
Tali contromisure, di natura sia tecnologica che organizzativa, sono adottate dall'Ateneo per mettere in sicurezza i sistemi ICT.

2 Generalità

Ai sensi del presente documento, per **incidente di sicurezza** deve intendersi "**la violazione, la minaccia imminente di violazione di una politica di sicurezza informatica, di politiche di utilizzo accettabili o di prassi standard di sicurezza, correlate a una violazione di dati o informazioni**".
Esempi di incidenti sono:

- un utente malintenzionato esegue operazioni al fine di inviare un numero elevato di richieste di connessione ad un server web, provocando l'arresto anomalo del servizio;
- gli utenti sono indotti ad aprire un file allegato alla mail che in realtà è un malware l'esecuzione del quale comporta l'infezione del dispositivo stabilendo connessioni con un host esterno;
- un utente malintenzionato ottiene dati sensibili e minaccia l'organizzazione di diffonderli se non viene pagato un riscatto.

2.1 DATA BREACH ai sensi del GDPR

Il Regolamento, all'art. 4, n. 12, definisce la violazione dei dati personali come "l**a 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 trattat**i".

Le violazioni declinate dalla norma sono sintetizzabili come:

- Violazione della riservatezza che si verifica in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali;
- Violazione dell'integrità che si verifica in caso di alterazione non autorizzata o accidentale dei dati personali;
- Violazione della disponibilità che si verifica in caso di perdita o distruzione di dati personali accidentale o illecita o di impossibilità di accesso ai dati personali da parte dei soggetti autorizzati.

Una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione di queste.

Gli effetti di una violazione possono causare danni fisici, materiali o immateriali, cioè la perdita del controllo sui propri dati personali, la limitazione dei propri diritti, la discriminazione, il furto d'identità o la frode, la perdita finanziaria, l'inversione non autorizzata di pseudonimizzazione, il danno alla reputazione e la perdita di riservatezza dei dati personali protetti dal segreto professionale. Può anche includere qualsiasi altro significativo svantaggio economico o sociale per gli individui che ne siano oggetto.
Se, a seguito del coinvolgimento del **DPO** (secondo le modalità descritte nel successivo paragrafo 3.2), l'incidente di sicurezza viene qualificato come Data Breach, è necessario rispettare le fasi e gli adempimenti previsti nella relativa policy (**Data Breach Policy**) a cui si rimanda.

3 Procedura di gestione degli INCIDENTI DI SICUREZZA

Viene di seguito definita la procedura per la gestione degli incidenti di sicurezza.

L'Ateneo ne garantisce il necessario aggiornamento. Tale procedura ha i seguenti obiettivi:

- preparare il personale;
- identificare un incidente in corso;
- minimizzare i danni relativi all'incidente e impedirne la propagazione;
- garantire la tempestiva attivazione, ove necessario, della "Procedura di gestione della violazione dei dati personali" allegata al "Regolamento privacy di Ateneo";
- gestire correttamente il processo di ripristino dei sistemi e delle applicazioni;
- acquisire nel modo appropriato le eventuali evidenze digitali di reato;
- riconoscere gli errori commessi, assumerne le responsabilità e formulare proposte volte a migliorare la procedura stessa.

La decisione su quali soluzioni adottare in caso di incidente di sicurezza è demandata al **CSIRT** con l'eventuale supporto delle figure ritenute necessarie (**DPO, Ufficio Legale, Referenti di sicurezza delle strutture coinvolte**) tenendo conto della complessità e della variabilità dell'argomento trattato.

Per facilitare la gestione degli incidenti di sicurezza il **CSIRT** mantiene un manuale operativo che riporta le varie fasi di intervento, in particolare il flusso delle comunicazioni fra i vari attori.

Tale misura ha anche lo scopo di facilitare la produzione del report relativo all'incidente e di tenere aggiornate le statistiche sugli incidenti di sicurezza.
Oltre ai requisiti di riservatezza ed integrità, vengono considerate anche le esigenze di disponibilità dei dati e dell'infrastruttura ICT preposta all'erogazione dei servizi informatici. Nel caso si verifichi un incidente di sicurezza che possa pregiudicare per un periodo sufficientemente lungo la disponibilità delle informazioni occorre fare riferimento a disposizioni contenute in un **Piano di continuità operativa dell'Ateneo** adottato con una chiara definizione delle strutture e delle responsabilità della gestione delle emergenze che dovranno operare in stretto coordinamento con il **Gruppo** e il **CSIRT**.

Qualora, a seguito di un incidente relativo alla sicurezza, risulti 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 affinché L'Ateneo possa essere oggetto di azione legale (civile o penale), le evidenze oggettive vengono raccolte e conservate nel cosiddetto **Fascicolo dell'incidente** 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 raccolta delle

evidenze può avvenire anche qualora si voglia semplicemente procedere con indagini più approfondite, non necessariamente legate ad un proseguo forense.

La documentazione relativa agli incidenti di sicurezza, 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**, nel caso in cui siano presenti dati personali, che, alla scadenza, devono essere cancellati e senza limiti di tempo, nel caso non siano presenti dati personali.

Tutti i dipendenti e collaboratori dell'Ateneo che accedono alle risorse dell'Ente sono tenuti a osservare i principi contenuti nel presente documento e a segnalare in modo tempestivo la presenza di condizioni che possano indurre a valutare delle anomalie riconducibili ad attacchi informatici oppure a comportamenti scorretti.

Eventuali **amministratori di sistema** che, a causa del loro comportamento, gravemente negligente, o in palese contrasto con le politiche di sicurezza dell'Ateneo, fossero causa diretta o indiretta di un incidente di sicurezza, potranno essere soggetti a un accertamento di eventuali responsabilità rispetto alla violazione delle politiche di sicurezza informatica dell'Ateneo.

3.1 Preparazione

Si tratta di attività necessarie per consentire un'adeguata gestione degli incidenti informatici di sicurezza che devono essere eseguite rigorosamente. Si tratta ad esempio di:

- definizione della struttura tecnica di supporto nella gestione degli incidenti e dei necessari interventi di formazione per le risorse potenzialmente coinvolte nella gestione degli incidenti;
- predisposizione degli strumenti hardware e software necessari;
- definire e distribuire le apposite procedure relative alle modalità di comunicazione verso l'esterno dell'accaduto.

3.2 Identificazione e analisi dell'incidente

Si tratta di attività che mirano a valutare se un evento riscontrato sia effettivamente riconducibile ad un incidente di sicurezza oppure si tratti di un cosiddetto falso positivo. Le operazioni di identificazione (*Detection and Analysis*) devono permettere di verificare, per ogni caso di evento anomalo o sintomo di un incidente, se si è in presenza di un incidente reale di sicurezza.
La segnalazione di incidente di sicurezza può arrivare direttamente da parte di un utente, il quale può per esempio rilevare situazioni di alterazione di un sito web dell'Ateneo, di accesso non autorizzato a dati, di indisponibilità di una risorsa ICT per un tempo prolungato etc.

Le segnalazioni degli utenti devono pervenire al **CSIRT**.

La segnalazione può pervenire in modo automatico da strumenti appositi o da un processo di analisi continuativa degli eventi di sicurezza registrati da vari dispositivi e gestiti, eventualmente, in modo centralizzato attraverso una piattaforma SIEM (*Security Information and Event Management*), opportunamente configurata. Nel caso in cui venga rilevato un riscontro positivo durante l'analisi di tali eventi viene aperto un incidente di sicurezza che segue la procedura di gestione.

Nel caso di segnalazioni pervenute dal personale, dai collaboratori o da parte di soggetti terzi, l'Ateneo avvia senza indugio un'indagine volta a verificare che si sia verificato effettivamente l'incidente segnalato.

Quando il **Responsabile Sicurezza** viene informato dal **CSIRT** in merito ad una segnalazione pervenuta tramite i canali sopra menzionati, dovrà procedere come segue.

I. Innanzitutto, il **Responsabile Sicurezza** dovrà attivarsi immediatamente per verificare, tramite il **CSIRT**, la fonte della segnalazione o altra modalità ritenuta opportuna, se l'incidente abbia coinvolto anche solo potenzialmente dati personali.
II. Ricevuta la conferma che l'incidente di sicurezza presenta profili potenzialmente rilevanti in tema di protezione dei dati personali, il **Responsabile Sicurezza** provvederà a coinvolgere il **DPO**.
III. Il **DPO** dovrà essere contattato con una comunicazione a mezzo mail all'indirizzo dpo@unimore.it. In particolare, il **Responsabile Sicurezza** avrà cura di:
    - utilizzare la seguente dicitura come oggetto della mail "!! POTENZIALE DATA BREACH – COMUNICAZIONE GRUPPO SICUREZZA ICT";
    - compilare e allegare (anche in termini approssimativi, in mancanza di una conoscenza specifica degli elementi) l'**Allegato A alla "Procedura di gestione della violazione dei dati personali" (Modulo per la raccolta informazioni)**[1]**.** Inoltre, è fondamentale indicare, anche nel corpo della mail, la data in cui il **Responsabile Sicurezza** ha avuto conferma del coinvolgimento dei dati personali;
    - mettere a disposizione un contatto telefonico affinché possa intervenire un confronto per le vie brevi nel minor tempo possibile.

Il coinvolgimento del **DPO** deve essere tempestivo. Infatti, il **Responsabile Sicurezza** deve necessariamente considerare che, laddove l'incidente di sicurezza comporti un Data Breach, deve essere rispettato quanto previsto dagli articoli 33 e 34 del Regolamento:

- se sussistono le condizioni, la violazione di dati personali deve essere notificata all'autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui il Titolare viene a conoscenza della violazione di dati personali.

[1] https://www.unimore.it/sites/default/files/2023-10/RegolamentoPrivacy.pdf

Si ritiene che le 72 ore decorrano dal momento in cui il **Responsabile Sicurezza** viene a conoscenza del fatto che l'incidente di sicurezza abbia coinvolto dati personali;

- qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è necessario corredare la notifica stessa con i motivi del ritardo;
- quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare deve comunicare la violazione all'interessato senza ingiustificato ritardo.

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 **Data Breach Policy.**
- 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** è assente, la procedura sopra descritta deve essere garantita dal Responsabile **CSIRT**.

3.3 Valutazione d'impatto dell'incidente

I possibili reali incidenti di sicurezza si possono classificare in diverse tipologie, dettagliate come segue:

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
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
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.

Tipologia Incidente	Descrizione
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
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
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

Tabella 1 - Tipologia Incidenti

È di fondamentale importanza effettuare una prima valutazione sull'impatto dell'incidente ai fini di indirizzare in modo efficace le risorse necessarie alla sua gestione. Tale attività consiste in una prima classificazione della sua portata in base ad alcuni parametri di seguito elencati:

- il livello di criticità della risorsa coinvolta, determinato in base alle valutazioni inerenti alla Business Impact Analysis. (in caso di coinvolgimento di più risorse verrà assunto come tale quello a maggiore criticità)
- il numero di risorse informatiche coinvolte, inteso come numero di server/applicazioni;
- il numero di utenti o postazioni di lavoro potenzialmente impattati dalla indisponibilità del servizio informatico;
- l'eventuale coinvolgimento di risorse ICT/utenti esterni all'organizzazione;
- l'esposizione su Internet del servizio
- il tipo di danno arrecato (economico, immagine, mancato adempimento normativo ecc.);
- gli enti o le organizzazioni coinvolte nell'incidente;
- l'eventualità di coinvolgere le forze dell'ordine a causa di possibili risvolti di natura penale.

In questa fase il **Responsabile Sicurezza insieme agli altri componenti del CSIRT**, anche coinvolgendo eventuali appaltatori dei servizi di assistenza e manutenzione sistemistica, deve valutare anche la gravità dell'incidente di sicurezza. Per fare ciò può inizialmente avvalersi della seguente matrice contraddistinta da una valutazione di tipo qualitativo, ma la classificazione della gravità dell'incidente è comunque a sua totale discrezione.

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 2 - Tassonomia Incidenti

Poiché per alcuni incidenti può risultare difficile assegnare un livello di gravità definitivo prima che l'analisi sia completa, occorre che la valutazione sia effettuata sulla base delle evidenze note sino a quel momento, assumendo che la gravità potrebbe molto probabilmente aumentare nel caso in cui non si effettui alcuna operazione di contenimento.

3.4 Valutazione dei rischi derivanti dal verificarsi del DATA BREACH

In caso di Data Breach l'Ateneo, in concerto con il **DPO**, deve valutare i rischi per i diritti e le libertà delle persone fisiche secondo quanto previsto nella **Data Breach Policy**.

3.5 Comunicazione degli incidenti

Tutti i potenziali incidenti dovranno essere comunicati via mail come primo punto di contatto al **Referente di Sicurezza della struttura di appartenenza** il quale avviserà prontamente il **CSIRT**, punto unico di contatto presso la DIAQ, all'indirizzo csirt@unimore.it.

Il **Responsabile Sicurezza**, coinvolge il **DPO** secondo le modalità definite nel precedente Paragrafo 3.2 quando l'incidente di sicurezza presenta profili potenzialmente rilevanti in tema di protezione dei dati personali.

Se l'incidente di sicurezza viene qualificato, in concerto con il **DPO**, come Data Breach, il **DPO** stesso darà parallela attuazione alla **Data Breach Policy**.

3.6 La notifica della violazione al Garante

Nei casi in cui l'incidente consista o comporti una violazione di dati personali, L'Ateneo deve notificare l'incidente al Garante per la protezione dei dati personali se, sulla scorta della valutazione approfondita, strutturata e documentata di cui al paragrafo precedente, si assuma come probabile che la violazione dei dati personali presenti effettivamente un rischio per i diritti e le libertà delle persone fisiche.

La notifica al Garante dovrà avvenire secondo quanto previsto dalla **Data Breach Policy**.

3.7 La notifica della violazione agli Interessati

Le violazioni di dati che comportano un rischio elevato per i diritti e le libertà delle persone fisiche devono essere comunicate agli interessati senza ingiustificato ritardo.

La comunicazione agli interessati dovrà avvenire secondo quanto previsto dalla **Data Breach Policy.**

3.8 Attivazione della procedura e monitoraggio delle attività

L'attivazione della procedura di gestione incidenti è a carico del **CSIRT**, il quale, a seconda della gravità attribuita in fase di identificazione dell'incidente, utilizzerà diverse modalità di attivazione e tracking.

Incidente di gravità "Alta"

Il **CSIRT** coinvolge immediatamente il **Referente sicurezza** mediante l'invio dell'apposito ***Rapporto incidente di sicurezza (Allegato 4.1.)*****,** compilando soltanto le parti che in questa fase è possibile conoscere. Il **Referente sicurezza** condivide il rapporto con il **Gruppo**. Il **DPO** viene coinvolto se sussistono le condizioni descritte nel precedente Paragrafo 3.2.

Lo scopo principale di questa prima fase è di attivare la gestione dell'incidente. Il ***Rapporto incidente di sicurezza*** sarà poi completato in tutte le sue parti in fase di chiusura dell'incidente.
Il Rapporto deve essere conservato per almeno **cinque anni**, in formato elettronico, in una collocazione soggetta a backup periodico e ad accesso opportunamente limitato.
È altresì fondamentale che tutte le operazioni eseguite per la gestione di un eventuale incidente siano opportunamente tracciate (es. strumento informatico di ticketing o altro), permettendo in tal modo di poter identificare tutte le risorse coinvolte nelle operazioni tecniche di gestione e poterle eventualmente indicare in ambito giudiziale come testimoni.
Le indagini svolte e le operazioni di gestione formano quindi una base dati che andrà ad incrementare la conoscenza dell'Ateneo in merito agli incidenti di sicurezza informatica.
Nel caso in cui l'incidente di sicurezza abbia un impatto sulla continuità operativa per un tempo di disservizio non accettabile per l'Ateneo, è necessario attivare il **Gruppo** e fare riferimento al **Piano di continuità operativa**.

Incidente di gravità "Media" o "Bassa"

In caso di incidente di gravità media o bassa, l'incidente può essere completamente gestito dal **CSIRT** fermo restando il coinvolgimento del **Gruppo** e, nel caso di un Data Breach, del **DPO** (nelle modalità descritte nel Paragrafo 3.2). In tale caso non è necessaria (anche se è consigliabile) la stesura del ***Rapporto incidente di sicurezza***, ma è comunque necessario tracciare opportunamente le operazioni permettendo in tal modo di poter identificare tutte le risorse coinvolte nelle operazioni tecniche di gestione e di poterle eventualmente indicare in ambito giudiziale come testimoni.
Anche in questo caso le indagini svolte e le operazioni di gestione formano una base dati che andrà a incrementare la conoscenza dell'Ateneo in merito agli incidenti di sicurezza informatica.

Se l'incidente di sicurezza è stato qualificato come Data Breach, la descrizione delle operazioni di gestione e il ***Rapporto incidente di sicurezza*** verranno condivisi anche con il **DPO** ove necessario al fine della compilazione del Registro dei Data Breach ovvero al fine del perfezionamento della notifica al Garante o della comunicazione agli interessati.

3.9 Contenimento, rimozione e ripristino

Le operazioni di contenimento hanno due importati fini:

- evitare che il danno si propaghi, o almeno limitarne la diffusione;

- acquisire le eventuali evidenze digitali di reato prima che queste possano essere compromesse.

A tal fine è necessario:

- identificare tutti i sistemi che possono essere stati compromessi o sui cui sia possibile raccogliere eventuali evidenze digitali di reato;
- effettuare delle copie delle eventuali evidenze digitali di reato in modo valido dal punto di vista forense;
- documentare in modo dettagliato tutte le operazioni eseguite, onde evitare, in un eventuale ambito giudiziale, possibili contestazioni sulla correttezza delle operazioni eseguite.

Le attività di contenimento dovranno essere eseguite da personale qualificato, ovvero da sistemisti appositamente addestrati per eseguire le operazioni necessarie, dipendenti dell'Ateneo o incaricati dal medesimo.

Tutte le operazioni eseguite saranno comunque sotto la responsabilità del **CSIRT** il quale dovrà riportare nel ***Rapporto incidente di Sicurezza***:

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

Il **CSIRT** dovrà comunicare al **Responsabile Sicurezza** quanto eseguito al termine di questa fase, raccordandosi poi con l'**Ufficio Legale dell'Ateneo** per la trasmissione di copia della documentazione utile ai fini della proposizione delle azioni legali di competenza.

Se l'incidente di sicurezza è stato qualificato come Data Breach, le operazioni di contenimento, rimozione e rispristino verranno condivise anche con il **DPO** ove necessario al fine della compilazione del Registro dei Data Breach ovvero al fine del perfezionamento della notifica al Garante o della comunicazione agli interessati.

Le operazioni di contenimento possono essere di due tipologie: **a breve termine e a lungo termine**.

3.9.1 Contenimento a breve termine

Le operazioni di contenimento a breve termine mirano a mettere in sicurezza gli eventuali sistemi interessati da un incidente, senza alterarne la configurazione o inquinare eventuali evidenze digitali di reato.

Come esempi, non esaustivi, di azioni di contenimento a breve termine si possono indicare:

- creazione di regole firewall atte a bloccare l'accesso ai sistemi coinvolti;
- disabilitazione di account utente sui sistemi centralizzati di autenticazione;

- cambio di configurazione sui sistemi DNS;
- disconnessione dalla rete dei sistemi coinvolti mediante riconfigurazione di apparati di rete.

Dopo aver messo in sicurezza i sistemi coinvolti nell'incidente, mediante l'operazione di contenimento a breve termine, è possibile procedere all'acquisizione di eventuali evidenze digitali (es. mediante copia dei dischi) oppure procedere con l'esecuzione di normali backup atti a mettere in sicurezza i dati per poterli riutilizzare nella eventuale ricostruzione del sistema colpito dall'incidente.

È necessario procedere all'acquisizione delle evidenze digitali di reato in ogni caso in cui si preveda un prosieguo in ambito legale come per esempio:

- accessi abusivi a sistemi o informazioni;
- attività illecite commesse da dipendenti o comunque da utenti dei servizi dell'Ateneo mediante il sistema informativo gestito dell'Ateneo stesso;
- interruzione di pubblici servizi critici;
- violazioni della privacy di dipendenti, utenti e cittadini;
- utilizzo illegale dei sistemi per perpetrare truffe o diffondere materiale illecito.

Quando invece l'incidente è causato da malfunzionamenti o errori umani è possibile procedere eseguendo una normale operazione di backup relativa a dati o configurazioni eventualmente presenti sul dispositivo coinvolto nell'incidente. Questa operazione potrà quindi essere eseguita utilizzando i sistemi e i programmi utilizzati per effettuare le comuni operazioni di backup e hanno lo scopo di mettere in sicurezza le informazioni necessarie per un'eventuale reinstallazione del dispositivo.

3.9.2 Contenimento a lungo termine

Il contenimento a lungo termine comporta l'esecuzione di operazioni tecniche direttamente sui sistemi coinvolti nell'incidente; per questo motivo questa azione deve essere eseguita solo dopo aver messo in sicurezza le evidenze digitali di reato e i dati presenti sul sistema impattato.

Tali operazioni mirano a rendere i sistemi coinvolti più sicuri e permettono di lasciarli in attività sino al momento in cui sia possibile procedere a operazioni più complesse di rimozione delle cause. A titolo esemplificativo e non esaustivo, si possono indicare quali operazioni di contenimento a lungo termine:

- installazione di patch o aggiornamenti di sistema e/o applicativi;
- cancellazione di file o dati;
- arresto di servizi o processi malevoli;
- cambio di configurazione di programmi.

Al termine di queste operazioni i sistemi coinvolti nell'incidente non possono ancora dichiararsi sicuri, ma è possibile utilizzarli temporaneamente sino a quando non sia

possibile procedere con le operazioni di rimozione definitiva di quanto ha scatenato l'incidente.

Durante questa fase, possono emergere diverse necessità, come per esempio:

- allocare risorse economiche per la fase di acquisizione delle prove di reato e le successive fasi di gestione;
- isolare e/o arrestare eventuali servizi o sistemi critici di produzione coinvolti;
- valutare eventuali conseguenze legali;
- relazionarsi con le strutture dell'Ateneo per comunicare eventuali disservizi.

In tali casi il **CSIRT** può operare le corrette scelte in autonomia, comunicando al **Responsabile Sicurezza** le eventuali azioni che saranno intraprese e raccordandosi, secondo quanto precedentemente indicato, con **l'Ufficio legale dell'Ateneo.**

3.9.3 Rimozione

Le operazioni di rimozione sono volte all'eliminazione definitiva del problema o della vulnerabilità utilizzata per compromettere un sistema coinvolto in un incidente e riportarlo a un livello di sicurezza elevato.

Le attività che sono solitamente eseguite in questa fase possono essere di diverso tipo, per esempio:

- aggiornamento di release dei sistemi operativi o del software presente al fine di rimuovere eventuali vulnerabilità di sicurezza;
- rimozione di eventuali servizi o software che, utilizzati in modo malevolo, possono compromettere il sistema stesso (hardening);
- in alcuni casi, come, ad esempio, per le infezioni da virus/malware, può essere più semplice e meno oneroso economicamente, ricostruire l'intera macchina reinstallando il software a partire dal sistema operativo.

Le operazioni di rimozione possono essere particolarmente onerose in quanto potrebbe essere necessario:

- acquisire nuovo hardware o licenze software;
- utilizzare risorse interne o esterne per l'esecuzione delle operazioni di rimozione;
- eseguire dettagliati test di funzionamento sui sistemi e sulle applicazioni interessate dall'incidente.

La valutazione dell'impatto tecnico ed economico delle operazioni di rimozione deve essere eseguita dal **CSIRT**, eventualmente coinvolgendo tutti i soggetti interessati e fornendo tramite un report di dettaglio, le indicazioni degli eventuali costi da sostenere e dei tempi necessari al ripristino, affinché sia possibile proporre l'adozione degli atti amministrativi necessari ad attuare le azioni consigliate.

Poiché l'operazione di contenimento a lungo termine non è da considerarsi risolutiva del problema, ma solo ed esclusivamente un'azione a titolo temporaneo, l'Ateneo si

impegna a contenere i tempi necessari per poter procedere alla fase di rimozione ai tempi tecnici strettamente necessari alla definizione dell'intervento, al reperimento delle relative risorse economiche e alle operazioni di approvvigionamento.

3.9.4 Ripristino

In questa fase le operazioni eseguite mirano principalmente a verificare che i sistemi coinvolti nell'incidente siano stati correttamente riattivati e che siano nuovamente sicuri, per considerare l'incidente effettivamente chiuso.

È necessario ottenere un elevato grado di certezza che quanto accaduto non possa ripetersi; per questo motivo si rende necessario definire con il dovuto dettaglio tutte le fasi di riattivazione di un sistema coinvolto, sia nei modi che nei tempi attesi per il ripristino, sia nei controlli da effettuare per certificare il ritorno alla normalità.

3.10 Attività post-incidente

La decisione del momento in cui un sistema coinvolto in un incidente possa ritornare in produzione è in carico al **Responsabile Sicurezza** che, in collaborazione con gli eventuali gruppi di supporto tecnici coinvolti, definisce un piano di riattivazione dei diversi servizi impattati dall'incidente.

In alcuni casi specifici, può essere necessario riattivare i sistemi in un periodo non lavorativo (es. nelle ore notturne oppure nei fine settimana) per dare la possibilità alle strutture che hanno in carico la gestione dei sistemi stessi di operare senza che siano presenti richieste di accesso da parte di utenti che non siano quelli deputati all'esecuzione di eventuali test di funzionamento.

Onde verificare che le operazioni di ripristino siano avvenute correttamente, si rende necessario monitorare il corretto funzionamento dei sistemi per un periodo di tempo adeguato, per cui potrebbe esservi la necessità di attivare ulteriori controlli utilizzando gli strumenti di monitoraggio in uso, oppure aumentando il livello di profondità degli eventi da registrare nei file di log applicativi o dei sistemi operativi.

Sarà il **Responsabile Sicurezza** a richiedere la modifica o l'implementazione di nuove regole di monitoraggio ai soggetti preposti.

Tutti gli incidenti di sicurezza devono essere documentati. Al momento della stesura della presente politica, gli incidenti presenti in archivio sono quelli del **Registro degli incidenti** gestito dal **CSIRT**.
Documentazione integrativa, unitamente alle evidenze degli incidenti, deve essere debitamente archiviata.

Sono documentati e archiviati, in modalità distinguibile rispetto ai restanti incidenti di sicurezza, tutti i Data breach, seppure non notificati all'Autorità Garante e/o agli interessati, così come previsto dalla **Data Breach Policy**.

Dal punto di vista tecnico le operazioni di chiusura dell'incidente, consistono nella dichiarazione della fine dello stato di incidente e nella compilazione del report relativo all'incidente stesso da parte del **Responsabile Sicurezza**.

Il report, firmato digitalmente dal **Responsabile Sicurezza**, tramite procedura di hashing, a garanzia della sua integrità, dovrà essere inviato in forma riservata sotto forma di relazione sull'esito dell'incidente di sicurezza al Titolare e ai Dirigenti/Direttori responsabili dei Servizi coinvolti.

Il report deve essere conservato in un repository ad accesso limitato, **per cinque anni** o per tutto il tempo ritenuto necessario (ad esempio allo svolgimento di indagini, nel caso di conseguenze penali, o perlomeno alla definitiva rimozione delle cause scatenanti l'incidente).

In seguito alla chiusura dell'incidente, dovranno essere valutate tutte le operazioni eseguite per la gestione dello stesso, evidenziando sia i punti in cui queste sono state eseguite in armonia con le procedure e le aspettative, sia eventuali problemi sorti durante lo svolgimento delle operazioni.

È fondamentale che i punti critici rilevati durante l'esecuzione delle operazioni siano immediatamente condivisi con i componenti del **Gruppo** e si provveda nel più breve tempo possibile a predisporre quanto può essere necessario per eliminarli o mitigarli, migliorando quindi sia la procedura tecnica di gestione sia la capacità di operare della struttura preposta, sia agendo sulle infrastrutture e i sistemi.

Di seguito alcuni esempi di punti critici che possono essere rilevati:

- mancanza delle competenze tecniche per operare correttamente su un sistema o applicazione;
- mancanza degli opportuni strumenti tecnici;
- errori nella valutazione della gravità dell'incidente o nelle sue capacità di diffusione;
- errori o difficoltà nell'interazione con soggetti interni;
- errori nella comunicazione verso terze parti o verso dipendenti e collaboratori

In particolare, può essere utile porsi le seguenti domande:

- La procedura di gestione incidenti è stata correttamente eseguita? È risultata adeguata al contesto?
- Si sono presentati aspetti che hanno rallentato la risoluzione dell'incidente?
- Si sono presentati elementi che si ritiene siano da cambiare in modo da rendere il processo di gestione degli incidenti più efficace ed efficiente?
- È necessario aggiornare il metodo di analisi della gravità a valle dell'incidente?
- Sono necessarie delle azioni correttive da intraprendere in fase di mitigazione dei rischi onde evitare che l'incidente possa accadere nuovamente?

- È necessario modificare le policy aziendali dal punto di vista tecnico (es.: aggiungere file con una determinata estensione tra quelli bloccati dal sistema antivirus)?
- È necessario aggiornare e/o migliorare gli interventi formativi al fine di istruire il personale aziendale sulle problematiche inerenti la sicurezza e la privacy dei dati?
- Sono necessarie risorse addizionali (es.: personale, tools, strumenti hardware o software) per rendere il processo di gestione degli incidenti più efficace ed efficiente?
- Sono necessarie modifiche e/o riconfigurazioni del software (es.: aumentare frequenza di aggiornamento delle firme dei software antivirus e/o anti-intrusione e, modificare il livello di dettaglio fornito dai sistemi di difesa perimetrali)?

Scopo di tale operazione è quello di verificare che il processo di gestione incidenti sia risultato adeguato a fronteggiare la situazione e far sì che le considerazioni che ne scaturiscono diventino patrimonio comune all'interno del **Gruppo**.

Per questo motivo, entro breve termine dalla chiusura formale di un incidente, il **Responsabile Sicurezza** convoca le eventuali figure che sono state parte attiva nella gestione dell'incidente, con l'obiettivo di valutare collegialmente l'efficacia della procedura di gestione degli incidenti e definire in un apposito verbale le considerazioni e le operazioni che possano portare a migliorare l'intera procedura.

4 Allegati

4.1 Rapporto incidente di sicurezza

Premessa

Breve descrizione dell'incidente, dei sistemi coinvolti, degli utenti su cui l'incidente ha impatto, della durata dell'incidente, delle modalità attraverso le quali si è venuti a conoscenza dell'incidente.

Descrizione dettagliata dell'incidente – compilare il modulo allegato

MOD01_Report Incidente di Sicurezza.

Note

Eventuali considerazioni sull'incidente, suggerimenti, adeguamenti da effettuare, ecc.

4.2 Riferimenti ad altre politiche di Ateneo

- Decreto del Rettore n. 253 del 6 maggio 2019 - Regolamento Privacy Completo e Allegato "Procedura di gestione della violazione dati (Data Breach)"
- Testo completo del Regolamento Privacy di Ateneo, con particolare riferimento all'art.27 dove si menziona il Gruppo di Sicurezza ICT e all'art.30 che menziona le procedure di Data Breach.