

Documento per uso interno – Utilizzo consentito solo a personale autorizzato. Divulgazione non permessa senza approvazione

Nel caso in cui l'incidente sia momentaneamente in corso rivolgiti subito al Team Leader o alla dirigenza.

Procedi seguendo le indicazioni fornite all'interno del documento Incident Response

Compila il documento: Segnalazione di un Incidente

G3 S.p.A. adotta un processo di gestione degli incidenti di sicurezza delle informazioni che è conforme agli standard internazionali ISO/IEC 27001 e TISAX (Trusted Information Security Assessment Exchange), garantendo la protezione delle informazioni aziendali e la resilienza operativa. Ogni incidente viene trattato con un approccio strutturato che comprende l'identificazione, la valutazione, la risposta, il recupero e la comunicazione, in modo da minimizzare i rischi e assicurare la conformità normativa.

Identificazione dell'incidente

- Strumenti avanzati e pratiche di monitoraggio e rilevamento sono in uso per identificare attività sospette e possibili vulnerabilità, sia in tempo reale che retrospettivamente, in modo da garantire un rilevamento proattivo degli incidenti.
- Ogni dipendente, consulente e collaboratore di G3 S.p.A. è tenuto a segnalare tempestivamente qualsiasi anomalia che possa indicare un incidente di sicurezza, come definito nei requisiti di monitoraggio di ISO/IEC 27001 e nei criteri di rilevamento TISAX. Per la segnalazione degli incidenti è presente un documento da compilare in caso di incidente informatico.
    - Leggi:

        - Segnalazione di un incidente
        - Politica di Sicurezza di G3
        - Risk Management
        - Incident response

Valutazione dell’incidente

- Al momento della segnalazione, il team di sicurezza informatica esegue una valutazione dell’impatto dell'incidente, in linea con le procedure di gestione del rischio previste dalla ISO/IEC 27001 e TISAX.
- Gli incidenti vengono classificati in base alla loro gravità e impatti sulla sicurezza delle informazioni, all’interno di categorie predefinite per garantire una gestione adeguata e coerente con gli standard di sicurezza.
    - Leggi:
        - Risk Management
        - Incident Response

Risposta all’incidente

- Il team di risposta agli incidenti di G3 S.p.A. attiva le azioni correttive immediate in conformità con il piano di risposta agli incidenti documentato, che include il contenimento, l'isolamento e la neutralizzazione delle minacce.
- Le azioni di risposta sono progettate per garantire il ripristino della sicurezza e la minimizzazione dei danni, riducendo al minimo l'esposizione dei dati sensibili e proteggendo le risorse aziendali. Le risposte sono allineate con le politiche di continuità operativa e i requisiti di sicurezza della catena di approvvigionamento.

Recupero

- G3 S.p.A. avvia prontamente le procedure di recupero per ripristinare i sistemi compromessi e le informazioni, seguendo le linee guida di ripristino e continuità della ISO/IEC 27001. Il recupero include la restaurazione da backup sicuri e la validazione della sicurezza dei sistemi ripristinati.
- Durante la fase di recupero, il team verifica che tutte le vulnerabilità siano state corrette e che i sistemi siano protetti da rischi futuri, garantendo che i dispositivi e le applicazioni siano conformi alle normative di sicurezza.
    - Leggi:
        - Business Continuity Plan (BCP) G3

Comunicazione e Notifica

- In caso di incidente, G3 S.p.A. informa tempestivamente tutte le parti interne ed esterne interessate, come previsto dalle normative applicabili.
- La comunicazione viene effettuata in modo trasparente e tempestivo con tutte le parti interessate, inclusi i clienti, le autorità competenti e i partner, per garantire che tutte le misure necessarie siano adottate.

    - Leggi:
        - Segnalazione di un incidente
        - Incident Response
        - Risk Management

Documentazione dell'incidente

- Ogni incidente viene documentato in modo completo e dettagliato, comprendendo la causa, le azioni intraprese, i sistemi e i dati coinvolti e l'impatto complessivo, in conformità con i requisiti di audit trail della ISO/IEC 27001 e le linee guida TISAX.
- La documentazione viene conservata in modo sicuro per garantire la conformità alle normative legali e la tracciabilità delle azioni, permettendo una revisione completa durante gli auditing interni ed esterni.
    - Leggi:
        - Piano di Monitoraggio e Audit

Analisi post-incidente e miglioramento continuo

- Una volta che l'incidente è stato risolto, viene effettuata un'analisi post-incidente per esaminare le cause profonde, le lacune nei processi e le migliorie necessarie. Questo processo segue le procedure di miglioramento continuo della ISO/IEC 27001 e gli standard di gestione dei rischi di TISAX.
- L'analisi include l'aggiornamento delle politiche di sicurezza, delle procedure di risposta agli incidenti e l'adozione di misure preventive per evitare incidenti futuri, contribuendo al miglioramento costante della sicurezza delle informazioni.
    - Leggi:
        - Piano di Monitoraggio e Audit - G3
        - Piano di Implementazione e Monitoraggio - G3

Audit e conformità

G3 S.p.A. si impegna a garantire la compliance alle normative sotto citate in ogni fase del processo di gestione degli incidenti, inclusi audit periodici per assicurare l'efficacia delle misure adottate:

- ISO/IEC 27001
- TISAX AL 2
- ISO 9001
- IATF
- ISO 14001

Ogni incidente, e la relativa gestione, è soggetta a revisione da parte di auditor interni ed esterni, con lo scopo di migliorare continuamente i processi di sicurezza e garantire l'efficacia delle risposte agli incidenti.

La gestione del rischio avverrà secondo le procedure della Politica di Sicurezza di G3 S.p.a. di Vedi:

- Incident Response
- Risk Management.

Segnalazione di un incidente Informatico:

Il dipendente

Il Dipendente di G3 S.p.a. Che noterà l'avvenuto incidente segnalerà seguendo la procedura sottoriportata:

1) Contattare il Team leader designato, la dirigenza e procedere come di seguito:
    a) Contatto verbale
        i) Segnalazione dell'incidente al Team Leader
            (1) Il Team Leader procederà ad assicurarsi che siano adottate le procedure ufficiali
    b) Contatto telefonico
        i) Utilizza i numeri per la segnalazione di un incidente in G3 S.p.A.
            (1) Segnalazione diretta alla dirigenza:
                (a) [+0039] 348- 529-4608
            (2) Segnalazione al CISO
                (a) + [0039] 095 3787462
                (b) + [0039] 350 059 0978
    c) Contatto tramite E-mail
        i) Segnalazione dell'incidente alla direzione:
            (1) stefano.gualtieri@g3spa.it
        ii) Segnalazione dell'incidente al CISO
            (1) incident@generaltechcenter.com

Il Team Leader si occuperà direttamente o indirettamente della segnalazione tempestiva ai partner commerciali qui di seguito:

- CIRT@Ford.com

2) Compilazione del documento di segnalazione di Incidente Informatico, il documento va utilizzato come segue:
    a) Inserire Data e Ora dell'incidente
    b) Compilare il documento seguendo le domande poste ed ulteriori dettagli
    c) Inoltrare il documento alla dirigenza o al team leader del proprio settore.

Nota:In caso di incidente il Team Leader si occuperà dell'eventuale compilazione o della presa visione della corretta compilazione del documento di Segnalazione di un incidente, così come dell'inoltro alla dirigenza del documento cartaceo o dell'inoltro tramite i seguenti canali di comunicazione diretta instaurati:

- E-mail:stefano.gualtieri@g3spa.it
- Telefono:[+0039] 348- 529-4608

Leggi:

- Ruoli e Responsabilità
- Piano di Formazione e Consapevolezza

La dirigenza

La Dirigenza di G3 S.p.A. ed i Team Leader tutti si impegnano a trattare con la massima serietà ogni incidente segnalato.

La dirigenza ed i team leader tutti si impegnano a reagire come segue in caso di incidente informatico:

1. Raccolta dei documenti di segnalazione
2. Analisi della perdita stimata
3. Contatti con i team informatici e di sicurezza informatica
    a. Contattare il team di tecnici informatici di G3 S.p.a
        - Segnalare l'incidente e inoltrare il documento relativo alla segnalazione
        - Telefono: [0039] 0522 305200
        - E-mail: daniele.davoli@cdainformatica.it
    b. Contattare il team di sicurezza informatica:
        - Segnalare l'incidente e inoltrare il documento relativo alla segnalazione
        - Telefono: [0039] 3500590978
        - E-mail: rosariozappala@proton.me

Il Team IT

Il team IT procederà come di seguito, in conformità e secondo le best practices della ISO 27001 ed in sintonia con le best practices TISAX.

1. Analisi dei dati ricevuti
    a. Analisi della situazione attuale tramite i seguenti metodi:
        - E-Mail
        - Documento di Segnalazione dell'incidente ricevuto
        - Contatto telefonico
        - Presa visione dell'incidente
2. Intervento Manuale

   a. Il team IT si occuperà di stabilire come procedere per mettere in sicurezza le informazioni contenute all'interno dei server fisici. Per farlo seguiranno la procedura riportata di seguito.
3. Contatto con il CISO:
   a. Riportare le informazioni ottenute
   b. Inviare un Report delle operazioni svolte

Procedura completa del Team Tecnico per mettere in sicurezza i server fisici

---

1. Isolamento e contenimento iniziale
   a. Disconnessione dei server compromessi dalla rete per evitare ulteriori danni.
   b. Identificazione dei sistemi e dei dati potenzialmente coinvolti nell'incidente.
   c. Limitazione degli accessi fisici ai server compromessi a personale qualificato e autorizzato.
   d. Configurazione di un ambiente isolato per analisi forense, se richiesto.
2. Creazione di copie forensi
   a. Creazione di un'immagine completa dei dischi rigidi per preservare l'integrità delle prove.
   b. Copia dei file di log di sistema, applicazioni, e rete in un ambiente sicuro per ulteriori analisi
   c. Verifica che le copie siano utilizzabili senza alterare i dati originali.
3. Analisi tecnica dell'incidente
   a. Il team tecnico esamina:
      - I log di sistema e i flussi di rete per identificare attività sospette o malevoli.
      - La cronologia delle modifiche e delle configurazioni di sistema.
      - La presenza di malware, exploit o altri tipi di vulnerabilità sfruttate.
      - Eventuali segnali di esfiltrazione di dati o accessi non autorizzati.
4. Contenimento avanzato
   a. Rimozione di eventuali malware o codici malevoli identificati.
   b. Modifica di credenziali e chiavi di accesso compromesse (es.: password di sistema, chiavi SSH, certificati).
   c. Blocco degli indirizzi IP o domini associati a attività malevoli.
   d. Implementazione di regole temporanee sui firewall per impedire ulteriori accessi non autorizzati.
5. Ripristino dei sistemi
   a. Identificazione e selezione dei backup validi, verificando che siano privi di compromissioni.
   b. Ripristino dei dati nei server, seguendo un ordine di priorità stabilito in base alla criticità dei servizi.
   c. Applicazione di patch e aggiornamenti ai sistemi operativi e software coinvolti.
   d. Ripristino della connessione dei server alla rete, una volta completati i controlli di sicurezza.

6. Monitoraggio e verifica post-ripristino
    a. Monitoraggio continuo dei sistemi per rilevare eventuali anomalie o attività sospette.
    b. Test di funzionalità per garantire che i servizi siano stati completamente ripristinati.
    c. Convalida che tutti i dati sensibili siano integri e protetti.
7. Comunicazione con le parti interessate
    a. Aggiornamento regolare del cliente o delle parti coinvolte sull'andamento delle operazioni.
    b. Consegna di un rapporto preliminare che descriva le attività svolte e i risultati ottenuti.
    c. Coordinamento con il team legale o di compliance, se necessario, per notificare eventuali violazioni di dati.
8. Analisi post-incidente
    a. Raccolta delle lezioni apprese durante la gestione dell'incidente.
    b. Creazione di un rapporto completo, includendo:
        - La causa principale dell'incidente.
        - Le azioni intraprese per contenerlo e risolverlo.
        - Raccomandazioni per prevenire incidenti futuri.

Leggi:

- Incident Response
- Disaster Recovery
- Business Continuity Plan (BCP)
- Piano di implementazione e monitoraggio
- Piano di monitoraggio e Audit
- Risk Management

Il CISO

Il CISO è responsabile di gestire e coordinare le operazioni di risposta agli incidenti informatici. Il processo sarà strutturato in base alle linee guida della ISO 27001 e TISAX per garantire una gestione efficace, sicura e conforme degli incidenti.

La procedura che sarà seguita include:

1. Raccolta e Analisi dei Dati
    a. Coordinamento con il Team IT: Il CISO dirigerà il Team IT nella raccolta dei dati pertinenti, come log di sistema, segnalazioni di vulnerabilità e incidenti precedenti, in conformità con i requisiti di documentazione.

   b. Valutazione dell'incidente: Verrà condotta una valutazione preliminare per determinare la gravità, la natura e l'ambito dell'incidente. La raccolta dei dati e la prima analisi devono essere documentate come parte del processo di gestione dell'incidente.
2. Identificazione e Contenimento
   a. Identificazione delle cause: Il CISO supervisionerà l'identificazione precisa delle cause dell'incidente, tra cui possibili attacchi informatici, errori umani o tecnici.
   b. Misure di contenimento: Saranno attivate misure per contenere e limitare il danno, come l'isolamento dei sistemi compromessi, applicando pratiche di controllo accessi definite nelle politiche aziendali di sicurezza.
   c. Rimozione delle vulnerabilità: Il Team dirigerà l'implementazione di soluzioni per rimuovere malware, bloccare accessi non autorizzati e correggere le vulnerabilità identificate.

   d. Applicazione di patch: Verifica che tutte le patch di sicurezza siano applicate in modo tempestivo
   e. Ripristino dai backup sicuri: Il CISO supervisionerà il recupero dei sistemi compromessi utilizzando backup sicuri, secondo le politiche e le procedure previste all'interno del Disaster Recovery - Documento facente parte della Politica aziendale di G3 S.p.a.
   f. Test post-ripristino: Verifica che i sistemi ripristinati siano sicuri e operativi, eseguendo test completi per garantire che non ci siano tracce di compromissione.
   g. Documentazione dell'incidente: L'incidente sarà completamente documentato, includendo dettagli su cause, azioni intraprese e impatti.
   h. Relazione finale: Verrà redatto un report dettagliato che descrive l'incidente, le risposte adottate, e le raccomandazioni per migliorare la sicurezza, che sarà condiviso con i responsabili aziendali e le parti interessate.
   i. Analisi delle cause profonde: Verrà eseguita un'analisi delle cause profonde dell'incidente per identificare eventuali lacune nei controlli di sicurezza.
   j. Piano di azione correttiva: Il CISO coordinerà l'adozione di misure correttive per migliorare la sicurezza e prevenire futuri incidenti.
   k. Aggiornamento delle procedure: Le politiche di sicurezza, i piani di recupero e le procedure di risposta agli incidenti saranno aggiornate in base alle lezioni apprese.
   l. Comunicazione interna ed esterna: Se necessario, verranno attivate le procedure di comunicazione con le parti interessate, inclusi i clienti, le autorità di protezione dei dati e altre entità, come previsto dalle normative GDPR o altre regolamentazioni pertinenti.
   m. Notifica agli enti competenti: In caso di violazione dei dati personali, la comunicazione con le autorità competenti e le notifiche agli utenti coinvolti verranno gestite in conformità con le leggi vigenti e le best practices.

6. Ruoli e Responsabilità

- Direzione: Segnalazione dell'incidente e attuazione dei piani e delle procedure definite all'interno del sistema di gestione della sicurezza delle informazioni aziendale (SGSI)
- Responsabile della Sicurezza delle Informazioni (CISO): Supervisione generale del processo.
- Dipendenti: Segnalazione tempestiva di eventi sospetti.
- IT Operations: Supporto tecnico per il contenimento e il recupero.

7. Documentazione e Reporting

- E' presente un registro degli incidenti con le seguenti informazioni:
    - Data e ora dell'incidente
    - Descrizione dell'evento
    - Azioni intraprese
    - Impatti riscontrati
    - Esiti del post-incidente
- Conservazione delle evidenze per future analisi e audit

Questo documento definisce le procedure da seguire in caso di incidente, ma include anche misure di protezione per G3 in caso di inoperatività forzata dovuta a catastrofi naturali o eventi che potrebbero paralizzare le attività produttive dell'azienda.

Il Piano di Continuità Operativa di G3 è stato progettato per garantire una risposta rapida ed efficace a qualsiasi emergenza, assicurando la resilienza delle operazioni aziendali. La decentralizzazione delle risorse IT, il supporto di un'azienda esterna per la sicurezza informatica e la capacità di ripristino entro 24-48 ore rendono G3 pronta ad affrontare eventi critici con rapidità ed efficienza, proteggendo i dati aziendali e garantendo il ritorno alla piena operatività nel più breve tempo possibile.

Nel caso in cui non fosse possibile ripristinare rapidamente la produzione, G3 attuerà piani di emergenza che prevedono la decentralizzazione della produzione stessa, affidandola a terzi. Il supporto di aziende esterne con cui G3 ha stipulato accordi strategici è un pilastro fondamentale della nostra strategia di continuità operativa. Tali accordi assicurano la produzione continua dei nostri prodotti, anche in caso di danni a strutture, macchinari o in seguito a disastri o incidenti gravi che ostacolano la capacità di G3 di proseguire con la produzione.

Identificazione dei Controlli ISO 27001 adottati:

Controlli ISO/IEC 27001 Annex A:

A.5.1.2 Politica di sicurezza dell'informazione

- Definizione di una politica formale per la gestione degli incidenti.

A.5.2.1 Organizzazione della gestione della sicurezza delle informazioni

- Creazione di un team di risposta agli incidenti (IRT) e assegnazione di ruoli e responsabilità.

A.5.3.1 Comunicazione sulla sicurezza delle informazioni

- Definizione delle procedure di comunicazione interna ed esterna in caso di incidenti.

A.6.1.1 Gestione degli asset

- Identificazione e classificazione degli asset informativi per valutare l'impatto degli incidenti.

A.6.2.2 Classificazione dell'informazione

- Classificazione delle informazioni per determinare le misure di protezione necessarie.

A.7.1.1 Controllo degli accessi

- Implementazione di misure per limitare l'accesso ai sistemi e ai dati, incluse azioni di contenimento.

A.8.1.1 Sicurezza dei sistemi

- Misure tecniche per proteggere i sistemi, come patch e configurazioni sicure.

A.8.2.3 Gestione delle vulnerabilità

- Scansione e correzione delle vulnerabilità per prevenire attacchi.

A.9.2.1 Continuità del servizio

- Implementazione di piani di recupero e continuità operativa per ripristinare i servizi dopo un incidente.

A.11.2.1 Gestione degli incidenti

- Processo completo di gestione degli incidenti, dalla rilevazione alla risoluzione.

A.12.4.1 Preparazione alla continuità

- Attività per garantire la continuità operativa in caso di incidente.

A.16.1.1 Responsibilities and Procedures

- Definizione di ruoli e procedure per la gestione degli incidenti.

A.16.1.2 Reporting Information Security Events

- Meccanismi per segnalare eventi di sicurezza.

A.16.1.4 Assessment of and Decision on Information Security Events

- Valutazione degli eventi di sicurezza e decisioni sulle azioni da intraprendere.

Riferimenti alle Normative TISAX

Conformità ai requisiti TISAX per la gestione degli incidenti

- Garantire la sicurezza della catena di approvvigionamento, protezione delle informazioni sensibili e continuità operativa.
- Documentazione dettagliata e tracciabilità delle azioni intraprese per ogni incidente.

Protezione e comunicazione conforme alle linee guida TISAX

- Comunicazione trasparente con clienti, partner e autorità, in linea con le best practice di sicurezza.

Valutazione del rischio e gestione della sicurezza

- Integrazione delle procedure di incident management con le pratiche di risk management previste dai requisiti TISAX.

Audit e conformità

- Revisione degli incidenti per assicurare l’efficacia delle misure adottate e per garantire che le risposte siano conformi alle linee guida TISAX.

Riferimenti Altri Normativi

GDPR (Articoli 33-34)

- Notifica alle autorità competenti e comunicazione agli interessati in caso di violazione dei dati personali.

ISO/IEC 27035

- Linee guida per la gestione degli incidenti di sicurezza delle informazioni.

ISO/IEC 27001:2022 – Gestione della sicurezza delle informazioni

- Normativa base che regola la gestione degli incidenti in tutte le sue fasi.