Gestione degli incidenti e delle crisi

Rev.	Data Emissione	Modifica	Redazione RSGI	Verifica/Approvazione DG
0	01.03.2025			

1. SCOPO

Lo scopo della presente procedura è di definire la gestione degli incidenti e delle crisi in conformità ai requisiti definiti dalla ISO 27001.

2. APPLICABILITÀ ED ECCEZIONI

La procedura si applica a tutto il perimetro di Justbit

3. DOCUMENTI DI RIFERIMENTO

ISO 9001:2015
ISO 27001:2022

4. ABBREVIAZIONI

RSGI	Responsabile Sistema di Gestione Integrato
SGI	Sistema di Gestione Integrato

5. DISPOSIZIONI PROCEDURALI

L'ambito di questa politica include tutti i componenti, prodotti e servizi erogati da Justbit, (sito web di www.justbit.it), la rete e le applicazioni e in generale qualsiasi sistema o applicazione di competenza. Le procedure di segnalazione degli incidenti si applicano a dipendenti, collaboratori e altre terze parti rilevanti ai fini della sicurezza nel perimetro di riferimento dell'Azienda.

I dipendenti di Justbit devono essere informati della diversa procedura di segnalazione degli eventi che potrebbero avere un impatto sulla sicurezza dei servizi di Justbit Tutti sono tenuti a segnalare eventuali eventi di sicurezza delle informazioni e punti deboli che potrebbero riscontrare su prodotti e servizi di Justbit

Altre terze parti possono sempre segnalare eventuali eventi sospetti al punto di contatto di Justbit per gli incidenti di sicurezza.

Il punto di contatto predefinito è il RSGI o un suo delegato. Le segnalazioni vanno indirizzate all'indirizzo email [info@justbit.it].

Segnalazioni di incidenti relativi alla sicurezza delle informazioni

La segnalazione e il monitoraggio degli incidenti forniscono i mezzi con cui è possibile rilevare, agire e analizzare incidenti indesiderati (come infezioni da virus, intrusioni intenzionali e tentativi di furto di informazioni). I dipendenti di Justbit e di terze parti devono segnalare eventuali incidenti di sicurezza delle informazioni il più rapidamente possibile. Un punto di contatto dovrebbe essere predefinito e dovrebbe essere conosciuto in tutta

Justbit e nelle terze parti affiliate (dipendenti e manager). Questo punto di contatto dovrebbe essere sempre disponibile per la segnalazione di incidenti e inoltre fornire una risposta adeguata e tempestiva.

Ogni dipendente, collaboratore, cliente deve essere a conoscenza del punto di contatto per la gestione incidenti e seguire i passaggi seguenti per segnalare l'evento dell'incidente:

- Menzionarlo al suo responsabile o al referente della sicurezza e compila immediatamente il modulo di segnalazione degli incidenti fornendo tutti i dettagli importanti (tipo di evento, ad esempio non conformità, perdita del servizio, violazione ecc.)
- Il dipendente non autorizzato non deve intraprendere alcuna azione immediata che possa causare danni alle informazioni, ai sistemi e/o servizi.
- Informare il punto di contatto per l'evento fornendo il modulo di segnalazione degli incidenti
- Il punto di contatto dovrebbe essere in grado di:
    - Identificare se questo evento costituisce un incidente di sicurezza delle informazioni
    - Definire un team di gestione degli incidenti appropriato.
    - Fornire un feedback adeguato e informare coloro che hanno segnalato l'incidente di sicurezza quando esso è stato risolto e chiudere la segnalazione.

Le procedure di segnalazione precise varieranno a seconda della natura e dell'entità dell'incidente. Di seguito si riassumono alcune tipologie:

La gestione degli incidenti varia da caso a caso. Il responsabile del SGSI e dei sistemi ICT deve essere informato tempestivamente e indirizzare le situazioni non definite in manuali operativi e best practice conosciuti dagli operatori. Di seguito alcune tematiche di riferimento:

- Uso inappropriato - Uso improprio dei sistemi di informazione: nel caso in cui un dipendente abbia utilizzato in modo improprio i sistemi informativi, le procedure per affrontare questo problema dovrebbero includere le risorse umane, il manager di linea del sospettato e un rappresentante della sicurezza delle informazioni.
- Accesso non autorizzato: nel caso in cui un dipendente abbia ottenuto un accesso non autorizzato, le procedure per affrontare questo problema coinvolgere le risorse umane, il responsabile del sospettato e il responsabile della sicurezza delle informazioni. Se l'accesso non autorizzato è stato eseguito da una fonte esterna e se è in corso un evento criminale potrebbe essere opportuno denunciare l'incidente al dipartimento di polizia (contattare sempre le forze di polizia che dispongono di squadre specializzate che si occupano di incidenti di sicurezza informatica). Un rapporto al dipartimento di polizia dovrebbe essere studiato prima e considerare quale impatto avrebbe un rapporto della polizia sulla reputazione pubblica di Xxx srl.

- Furto: per definizione il furto è un evento criminale e l'atto corretto è denunciarlo alla polizia. Prima di riferire alla polizia, tuttavia, il rapporto della polizia dovrebbe essere studiato in anticipo e considerare l'impatto che un rapporto della polizia avrebbe sulla reputazione pubblica di Justbit Se un collaboratore è coinvolto nel furto, è necessario raccogliere le prove appropriate prima di qualsiasi azione.
- Guasti del sistema informativo e perdita di servizio: la segnalazione degli errori di sistema è fondamentale per il poter effettuare adeguatamente il ripristino. Il team di risposta agli incidenti dovrebbe decidere a chi segnalare l'incidente e come gestire la segnalazione. Come per tutte le segnalazioni di incidenti, la natura e l'impatto dell'evento determina le azioni successive. Se l'incidente ha un impatto su Justbit e sui clienti questi dovrebbero essere inclusi nello schema di segnalazione.
- Violazioni di riservatezza e integrità: per lo più le violazioni provengono da entità interne o da terze parti aziendali. In tal caso, il team di gestione degli incidenti dovrebbe raccogliere tutte le prove e agire legalmente sulla base dei contratti e degli accordi con la persona sospettata o con i terzi.
- Virus, Denial of Service, Data Breach, Ransomeware, altri incidenti standard: la gestione dipende dai sistemi impattati. Il responsabile sicurezza provvede a gestire con tool interni, tema di specialistici o attraverso l’assistenza prevista dai vendor e fornitori di servizi.

Se queste violazioni hanno un impatto sui dati dei clienti, l'incidente dovrebbe essere affrontato con diplomazia, informando i clienti della violazione e prevenendo qualsiasi impatto sulla relazione dell'azienda con i clienti.

In caso di incidenti che implichino la violazione di dati personali (data breach), è necessario attivare anche le procedure previste dal GDPR. In particolare, il titolare del trattamento deve notificare l’incidente all’autorità di controllo entro 72 ore dal momento in cui ne viene a conoscenza, e – se il rischio è elevato – informare tempestivamente anche gli interessati. Vedi documento PS02 – Politica della Sicurezza delle Informazioni per maggiori dettagli.

Passi operativi per la gestione di un incidente

Quella che segue è una serie di passaggi pratici che devono essere seguiti da Justbit e dal team operativo per la gestione degli incidenti di sicurezza delle informazioni. Le azioni sono suddivise in fasi preparatorie e fasi di risposta.

I. **Fasi preparatorie**

- Raccogliere i dettagli di contatto di tutte le persone che potrebbero essere richieste in caso di incidente grave. Copie multiple di queste informazioni devono essere archiviate fuori sede e i principali responsabili degli incidenti le tengono a portata di mano
- Identificare quali record o log esistono per l'incidente
- Analizzare e identificare la causa dell'incidente. Determina l'incidente come classificato nella sezione precedente

- Determina se l'evento proviene da un attacco interno o esterno
- Tenere un elenco di quelle persone / organizzazioni esterne che devono essere contattate nel caso di incidente rilevante.
- L'analisi dell'impatto aziendale dovrebbe essere eseguita con le conseguenze sui servizi e del Business dell'Azienda.
- Justbit effettua test di simulazione annuali per la gestione incidenti, simulando scenari quali attacco ransomware, compromissione email o guasto infrastrutturale. I risultati sono documentati e analizzati nel Riesame della Direzione.

II. **Risposta agli incidenti**

- Tutte le azioni di emergenza intraprese devono essere documentate in dettaglio
- Se l'incidente influisce sulla capacità di Justbit di fornire servizi, informare i clienti il prima possibile (probabilmente preferiranno essere informati in anticipo piuttosto che dover affrontare una consegna successiva o annullata)
- Nel rapporto sugli incidenti devono essere contenuti i tempi, la durata e il luogo. Segnala inoltre se l'incidente è in corso
- Stabilire se il sistema deve essere isolato o se i percorsi di accesso devono essere rimossi per evitare ulteriori danni
- Valutare il danno causato determinando l'entità del danno e della penetrazione, intervistando testimoni o parti interessate, raccogliendo prove a sostegno e raccogliendo prove dei dipendenti (ad es. Registri delle risorse umane)
- Pianificare e attuare azioni correttive per prevenire il ripetersi
- Tutte le azioni di emergenza devono essere segnalate alla direzione ed essere riviste frequentemente
- Eseguire attività di ripristino (è utile mantenere il software di imaging come parte standard del toolkit di gestione IT in quanto può essere utilizzato per il ripristino delle informazioni). In caso di incidente tecnico (come l'hacking), eseguire gli aggiornamenti tecnici appropriati, introdurre patch, eseguire una revisione della configurazione, rafforzare la protezione della rete, esaminare i dispositivi di rilevamento delle intrusioni
- Ripristino dei servizi e della disponibilità di Justbit nei tempi richiesti. I tempi dovrebbero essere stabiliti in base alla valutazione della perdita di servizi interni o esterni e ai termini e alle condizioni previste.
- L'integrità e il controllo dei servizi di Justbit devono essere confermati con il minimo ritardo.
- Rivedere la politica se necessario, determinare le questioni relative alle risorse umane e ai contratti, rivedere gli accordi di outsourcing e rivedere o negoziare clausole di responsabilità e garanzie
- Stabilire se l'incidente deve essere denunciato alla polizia
- Gestisci i problemi di reputazione con dipendenti, clienti e fornitori.

Raccolta delle prove

Se l'azione successiva per affrontare un incidente di sicurezza è un'azione legale contro una persona o un'organizzazione, le prove devono essere raccolte e presentate alla giurisdizione competente.

Durante la raccolta dei dati, il team di gestione degli incidenti dovrebbe considerare quanto segue:

1. Valutare se i dati possono essere utilizzati come prova in tribunale. Assicurarsi che le informazioni fornite siano conformi agli standard pubblicati

2. Misurare la qualità e l'integrità delle prove raccolte. Durante la raccolta delle prove, il team di gestione degli incidenti deve rispecchiare le immagini o le copie di tutti i dati rimovibili. Archivia le informazioni su dischi rigidi o in memoria. Registra tutte le azioni di copia. Le informazioni originali e i file di registro devono essere conservati in un luogo sicuro all'interno dell'azienda.

Per i documenti cartacei, i documenti originali devono essere conservati in un luogo sicuro e deve essere registrato il nome della persona che ha trovato il documento, il luogo e l'ora in cui è stato trovato il documento e che ha assistito alla scoperta. I documenti originali non devono essere forniti a nessuna indagine Forense.

In caso di incidente di sicurezza delle informazioni, il team di gestione degli incidenti dovrebbe identificare chi ha fatto cosa e quando lo ha fatto.

I dati del computer sono estremamente volatili e questo rende difficile conservarli in un modo che soddisfi i normali criteri per le prove giudiziarie. Per fare ciò è necessaria una combinazione di strumenti IT, tecniche di indagine e comprensione giuridica. Le prove potrebbero essere: abuso della posta elettronica, frode, violazione dei diritti di proprietà intellettuale, uso improprio del computer. Tutti i dati e fatti devono essere scrupolosamente registrati mantenendo l'integrità probatoria. L'approccio dovrebbe essere strettamente collegato al concetto di "scena del crimine" delle forze dell'ordine e dovrebbe considerare molti fattori come: prove e note cartacee, geometria e configurazione dell'hardware, modelli di utilizzo del sistema, log di prossimità, log CMS, log httpd del sito web.

Una persona autorizzata del team di gestione degli incidenti dovrebbe supervisionare la copia delle informazioni sulle prove. Dovrebbe essere registrato il nome del supervisore del processo di copia, l'ora e il luogo del processo di copia, il nome della persona che ha eseguito l'azione di copia e gli strumenti che sono stati utilizzati durante il processo di copia.

I seguenti principi dovrebbero applicarsi a tutte le indagini forensi. Questi dovrebbero essere considerati prima di intraprendere un processo di gestione degli incidenti:

- Non entrare nel sistema sospetto senza pensarci. Le prove fragili potrebbero essere distrutte, ovvero interrompere l'esecuzione di processi informatici che sono di per sé prove dell'evento
- Sigillare l'area e impedire l'accesso alle apparecchiature sospette e alla sua posizione. Impedire l'accesso del computer a sistemi sospetti, compreso l'accesso remoto

- Registrare le circostanze dell'incidente utilizzando osservazioni firmate da testimoni con timbri di data e ora
- Conserva le prove. Identificare prima tutti i potenziali dati di origine come registri, record del firewall, registri di posta elettronica, quindi controllare tutti i registri degli eventi come chi ha accesso e se i client sono protetti
- Raccogliere una serie di prove come registri di accesso fisico e record dei visitatori
- Acquisire copie di immagini dei sistemi sospetti. (es .: server di sviluppo privato)
- Controllare gli orari su tutti i dispositivi rilevanti e controllare i registri rilevanti per vedere se gli orari dell'orologio sono stati modificati. Usa sempre GMT come standard per tutti gli orari

Determinare se l'evento incidente diventa una crisi

Un piano di gestione delle crisi genera ordine dal caos e quindi ha bisogno di una forte leadership da parte di dipendenti ben formati e provati di Justbit

Una crisi è una situazione anormale, o addirittura una percezione, che esula dall'ambito delle attività quotidiane e che minaccia il funzionamento, la sicurezza e la reputazione di Justbit

Utilizzando la gestione delle crisi in Justbit S.p.A, il team di gestione delle crisi può gestire un impatto più ampio, come le relazioni pubbliche e consentirgli di avviare la ripresa.

Ruoli del team di gestione delle crisi

Il team di gestione delle crisi dovrebbe:

- Stabilisci cosa è successo
- Valuta l'impatto
- Risolvere eventuali conflitti di interesse
- Identificare e dare la priorità alle azioni richieste
- Mantieni il controllo
- Preparare un brief per il Board e per il resto dell'attività (costituisce la base di un messaggio comune da comunicare a organizzazioni esterne)

I ruoli dei manager all'interno del team di gestione delle crisi dovrebbero essere basati sui loro ruoli quotidiani. I manager dovrebbero indicare esattamente quali sono questi ruoli e responsabilità, per garantire che nulla di importante sia stato omesso.

Processo di gestione delle crisi

Quando si risponde a una crisi, i manager sono normalmente rappresentati nel team di gestione delle crisi. La crisi dovrebbe essere trattata come una questione di gestione operativa che viene semplicemente intrapresa in circostanze estreme. Il quadro di gestione delle crisi per la risposta può essere basato sulle fasi di gestione degli incidenti di cui sopra. Deve anche riflettere sulle linee di comunicazione esistenti, sia all'interno dell'azienda che con altre organizzazioni che potrebbero essere interessate. Questo

approccio, se sviluppato in collaborazione con i manager operativi di Justbit confermerà la proprietà dei piani e preparerà il quadro proposto per l'implementazione pratica.

Piani di gestione delle crisi

I piani migliori sono i più semplici, eppure l'attenzione ai dettagli rimane estremamente importante. I documenti dovrebbero essere pianificati in dettaglio e includere quanto segue:

- Persone coinvolte e loro compiti
- Metodi per identificare la crisi
- Metodi per coinvolgere il management
- Linee di comunicazione
- Meccanismi di rendicontazione
- Processo decisionale
- Livelli di controllo e limiti di autorità

La gestione delle crisi si occupa della risposta immediata a una crisi, ma garantisce anche il ripristino del sistema. Prima di una crisi, Justbit dovrebbe già eseguire le seguenti linee guida:

- Guarda attentamente l'organizzazione e valuta i possibili rischi
- Dovrebbe essere istituito un team di gestione delle crisi
- Formulare il piano di gestione delle crisi e indicare chiaramente:
    - I ruoli e le responsabilità di ogni membro
    - I ruoli di altre persone coinvolte nei loro compiti
    - I metodi per coinvolgere il management
    - Le linee di comunicazione
    - I meccanismi di reporting
    - Le informazioni relative a qualsiasi Crisis Management Center