Incident Response Plan (IRP)

[NOME AZIENDA] [DATA ELABORAZIONE]

HISOLUTION SRL
Via della Canapiglia5,
56019 Vecchiano, PI, Italia
Tel: +39 050 6397401
info@hisolution.it

1. Introduzione

1.1 Introduzione

Questo piano di risposta agli incidenti è stato sviluppato per HiSolution seguendo le linee guida e le raccomandazioni standardizzate di NIST e CISA. Il piano è stato revisionato e approvato dal team di risposta agli incidenti di HiSolution e dal management aziendale. Poiché il panorama delle minacce e la nostra attività sono in continua evoluzione, il piano sarà aggiornato di conseguenza.

Il documento descrive i componenti principali del processo di gestione degli incidenti, tra cui:

- Valutazione della gravità di un incidente
- Definizione dei ruoli e delle responsabilità
- Implementazione di una strategia di comunicazione
- Identificazione, contenimento ed eliminazione efficace delle minacce
- Riduzione dei danni e ripresa delle normali operazioni
- Documentazione e raccolta delle prove forensi per la revisione post-incidente
  Aggiornamento, test e miglioramento del piano di risposta agli incidenti di HiSolution

1.2. Obiettivo

QuestoPiano di Risposta agliIncidenti mira a delineare un metodo sistematico per affrontare gli incidenti di cybersicurezza, garantendo un contenimentorapido, un'indagine approfondita, l'eradicazione completa, il recupero e la rendicontazione accurata per ridurre l'impattosulle operazioni aziendali.

1.3. Ambito

Il Piano di Risposta agli Incidenti di Cybersicurezza copre tutti gli asset informatici di HiSolution, comprese le applicazioni aziendali, i sistemi di produzione e la proprietà intellettuale. Esso sostituisce i piani di sicurezza per singole unità aziendali, che dovranno essere allineati a questo piano centrale. Ad esempio, una risposta efficace agli incidenti richiede collaborazione tra il CSIRT (Computer Security Incident Response Team) e il Team per la Protezione dei Dati.

Qualsiasi sospetto incidente di cybersicurezza deve essere immediatamente segnalato al Security Operations Center (SOC).

La segnalazione tempestiva è essenziale affinché HiSolution possa rispondere in modo efficace e contenere rapidamente l'incidente, inclusi i sistemi coinvolti e gli eventuali dati personali. Un incidente può essere accidentale o intenzionale e può avere impatti su tutte le aree operative, inclusi riservatezza, integrità e disponibilità. I possibili incidenti includono:

Incidente	Descrizione
Malware	Software progettato per danneggiare o compromettere computer, reti o dispositivi
Ransomware	Malware che cripta i dati e richiede il pagamento di un riscatto, spesso si diffonde tramite campagne di phishing o vulnerabilità software
Accesso non autorizzato	Accesso non consentito a un sistema, rete o dati. Può avvenire tramite hacking, sfruttamento di vulnerabilità o uso di credenziali rubate
Esfiltrazione di dati	Acquisizione illegale di informazioni sensibili da un computer o rete, spesso eseguita tramite malware o vulnerabilità dei sistemi
Compromissione della supply chain	Violazione della sicurezza attraverso lo sfruttamento delle vulnerabilità della catena di fornitura, inclusi fornitori terzi, fornitori di software o partner di servizi

Phishing	Attacco informatico che prevede l'invio di e-mail ingannevoli per indurre gli utenti a rivelare informazioni sensibili, cliccare su link dannosi o scaricare software malevoli
Compromissione dell'e-mail aziendale	Tipo specifico di phishing in cui gli attaccanti utilizzano frodi via e-mail per ingannare i dipendenti inducendoli a divulgare informazioni riservate, trasferire fondi o concedere accessi privilegiati
Minaccia interna	Minaccia proveniente dall'interno dell'organizzazione, spesso da parte di dipendenti, collaboratori o partner commerciali che hanno accesso a informazioni e sistemi riservati
Minaccia persistente avanzata (APT)	Attacco informatico prolungato e mirato, in cui un attaccante non autorizzato si infiltra nella rete e rimane inosservato per un periodo prolungato
Asset compromesso	Risorsa (computer, rete o dati) che ha subito una violazione della sicurezza, consentendo l'accesso o il controllo non autorizzato da parte di un attaccante
DDoS (Distributed Denial of Service)	Attacco che sfrutta numerosi sistemi compromessi per sovraccaricare un obiettivo con traffico eccessivo, esaurendone le risorse

1.4. Governance

Il Team di Cybersicurezza è responsabile dell'implementazione di questo piano, come definito nel Sistema di Gestione della Sicurezza delle Informazioni di HiSolution. Il piano è stato sviluppato con il contributo e l'approvazione del management aziendale.

1.5. Formazione e Test

Il responsabile del Programma di Risposta agli Incidenti, in coordinamento con il CISO, è responsabile di garantire che ciascuna unità aziendale abbia accesso e abbia completato la formazione relativa a questo piano. Verranno organizzate esercitazioni periodiche per testare l'efficacia del piano.

Esercitazioni simulate

Le esercitazioni tabletop devono essere effettuate almeno una volta all'anno. Esse devono simulare scenari realistici e testare tutti gli aspetti del piano e del team di risposta agli incidenti.

I partecipanti dovrebbero includere membri del CSIRT e rappresentanti dei principali dipartimenti coinvolti, come IT, Sicurezza, Legal e fornitori terzi. Le esercitazioni dovrebbero fornire indicazioni utili per aggiornare e migliorare il piano di risposta agli incidenti di HiSolution.

Risorse utili:

- Pacchetti di esercitazione CISA
- Best Practice Sophos
- Template tabletop forniti da Sophos su richiesta

1.6. Lista di controllo IR per i Dipartimenti

L'obiettivo del processo IR (Incident Response) è quello di stabilire un metodo affidabile per costituire un team IR (Team di Risposta agli Incidenti) opportunamente dimensionato, specifico per ciascun incidente. Ogni dipartimento deve mantenere un protocollo di escalation documentato e le relative procedure, per garantire una gestione fluida e interfunzionale del processo IR, come descritto nella checklist riportata di seguito.

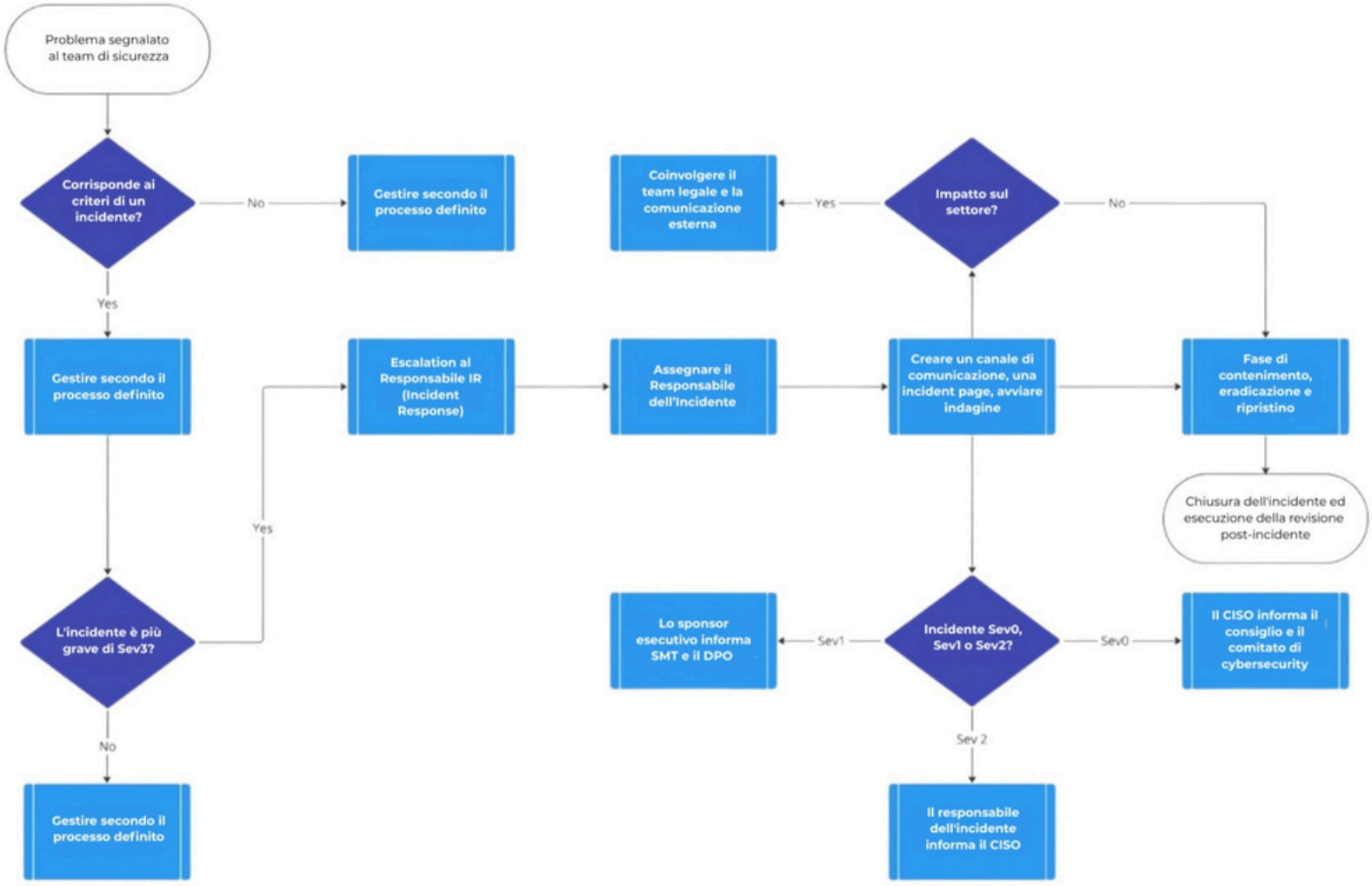
Voce	Descrizione
Referenti IR dipartimentali	Responsabili dell'attuazione dei processi IR nel dipartimento
Team IR dipartimentale	Gruppo responsabile delle attività di risposta
Criteri di escalation	Allineati ai livelli di gravità definiti nel piano
Processi e playbook	Linee guida operative per la gestione degli incidenti
Test dei processi	Per garantire l'efficacia continua delle procedure

1.7. Obiettivi

- Identificazione e contenimento rapidi degli incidenti
- Riduzione dei danni alle funzioni aziendali
- Rapida eradicazione e recupero delle operazioni
- Comunicazione efficace e rendicontazione degli incidenti
- Revisione post-incidente per un miglioramento continuo

1.8. Processo di gestione IR

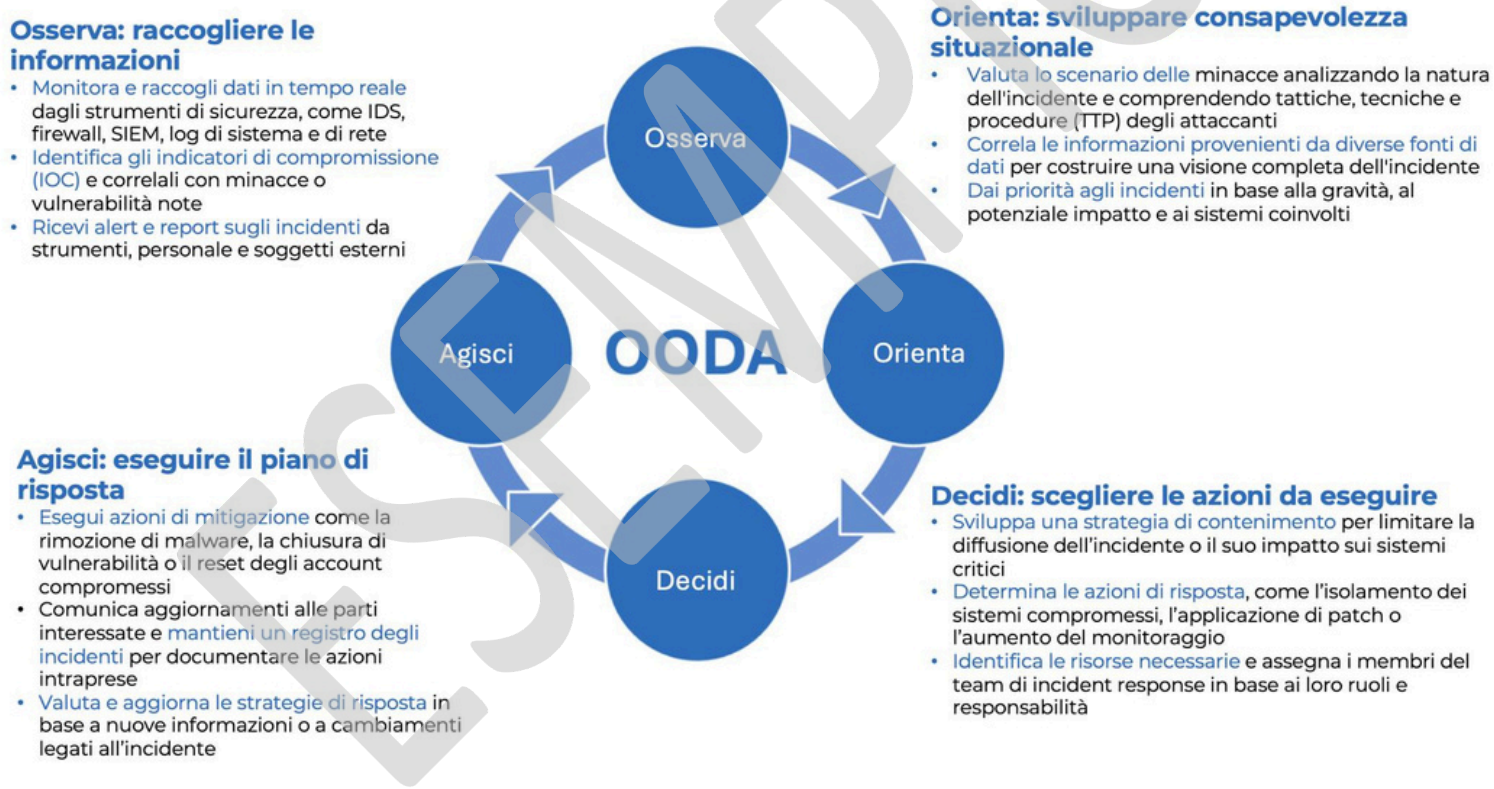
Il processo di gestione degli incidenti (IR handling process) rappresenta un approccio organizzato che garantisce continuità, efficienza e collaborazione tra tutte le parti coinvolte. (Vedi figura di seguito)



1.9. Il ciclo OODA

Gestire un incidente può essere stressante e ostacolare decisioni rapide e accurate. Il ciclo OODA (Osservare, Orientarsi, Decidere, Agire) offre un quadro strutturato per migliorare la consapevolezza della situazione e il processo decisionale.

Applicare il ciclo OODA nella risposta agli incidenti consente una gestione efficiente ed efficace degli eventi informatici. Esso fornisce un metodo organizzato e iterativo per affrontare minacce complesse.



2. Classificazione della gravità

Definire i livelli di gravità è essenziale per costruire un sistema efficace di classificazione degli incidenti all'interno di un piano di risposta agli incidenti (Incident Response – IR). Tale classificazione consente di:

- Dare priorità alle azioni di risposta
- Allocare in modo efficiente le risorse
- Applicare protocolli di comunicazione chiari

Gli incidenti ad alta gravità ricevono attenzione immediata, l'allocazione delle risorse necessarie, il rispetto dei requisiti normativi e la guida di miglioramenti strategici, rafforzando così la resilienza dell'organizzazione contro incidenti futuri.

2.1. Valutazione della gravità

IlSecurity Operations Center (SOC) di HiSolution valuta gli incidenti sulla base di criteri specifici per l'analisi della minaccia. Successivamente, il Manager della Risposta agli Incidenti (Incident Response Manager) assegna un livello di gravità.

Icriteri utilizzati per assegnare un punteggio agli incidenti includono:

- Impatto funzionale: valutazione del grado in cui l'incidente ha compromesso le funzioni operative aziendali
- Impatto informativo: determinazione della sensibilità e criticità delle informazioni coinvolte
- Attività osservata: identificazione delle azioni malevoli rilevate o sospette
- Caratterizzazione e attribuzione dell'attore: determinazione dell'identità e dell'intento dell'aggressore, quando possibile
- Localizzazione dell'attività osservata: identificazione delle aree geografiche o infrastrutturali coinvolte
- Capacità di recupero: misura in cui è possibile ripristinare i sistemi interessati
- Impatto potenziale: stima dei possibili effetti sull'attività aziendale, sulla reputazione e sugli obblighi normativi

Sebbene i criteri di valutazione della gravità garantiscano coerenza, il Manager IR e lo Sponsor Esecutivo hanno l'autorità di modificare il livello di gravità assegnato a un incidente, qualora lo ritengano necessario.

Durante tutto il processo di gestione dell'incidente, la gravità viene rivalutata continuamente e modificata, se opportuno.

2.2. Severity Classification

Laseguente matrice di classificazione della gravità descrive gli obiettivi di tempo di risposta per gli incidenti di cybersicurezza, sulla base dell'impatto previsto degli incidenti sulla sicurezza delle informazioni aziendali di HiSolution.

Iltempo di risposta viene misurato a partire dal momento in cui all'incidente viene assegnato un livello di gravità.

Gravità	Descrizione	Dettagli	Tempo di risposta
0 – Critico	Incidente critico con impatto potenzialmente esistenziale sull'azienda	Furto o esposizione di grandi volumi di dati altamente sensibili relati	Ivmi am celideinattio o dipende
1 - Alto	Incidente importante con impatto molto elevato	Funzionalità ▪ Un servizio rivolto ai client è inattivo o a rischio	2 ore
		Informazioni ▪ Perdita di dati ad alto impatto (es. dati di clienti o dipendenti, codice sorgente, dati finanziari) ▪ Violazione di riservatezza o privacy	
		Recuperabilità ▪ Presenza di Ransomware su molti sistemi critici	
		Reputazione ▪ Probabile copertura mediatica	

		▪ Sicurezza dei clienti compromessa	
2 -Medio	Incidente rilevante con impatto significativo	Funzionalità ▪ Un servizio essenziale non è accessibile per alcuni clienti o dipendenti	48 ore
		Informazioni ▪ Violazione della riservatezza di dipendenti o fornitori ▪ Violazione di normative (es. GDPR, PCI, HIPAA)	
		Recuperabilità ▪ Ransomware su sistemi che ospitano dati a impatto aziendale medio	
		Reputazione ▪ Possibile o effettiva diffusione sui social media	
		Esempio ▪ Lista dei client o dipendenti esfiltrata	
3 – Basso	Incidente minore con impatto contenuto	Funzionalità ▪ Disagio minore per clienti o dipendenti, disponibile una soluzione temporanea	2 settimane
		Informazioni ▪ Compromissione di pochi individui e di dati a basso rischio (es. indirizzi e-mail aziendali)	
		Recuperabilità ▪ Impatto minimo ma comunque funzionale sulle prestazioni	
		Esempio ▪ E-mail di phishing segnalata ma non eseguita	

Richiedi GRATIS, l'Incident Response Plan (IRP) con il servizio HiCompliance!

SBLOCCA ORA

HISOLUTION SRL
Via della Canapiglia5,
56019 Vecchiano, PI, Italia
Tel: +39 050 6397401
info@hisolution.it