

# Procedimiento para el Reporte de Incidentes de Seguridad en Blatorh Group



## Control de Cambios de Documento

Cualquier modificación o cambio al presente Documento se deberá reflejar a continuación:

<b>Versión:</b>	1.0	<b>Fecha:</b>	01/08/2024
<b>Responsable:</b>	Angeles Simal / Pablo Bascoy	<b>Revisado por:</b>	Francisco Torres
<b>Motivo:</b>	Confección inicial del documento		
<b>Versión:</b>		<b>Fecha:</b>	
<b>Responsable:</b>		<b>Revisado por:</b>	
<b>Motivo:</b>			

## Compromiso de Confidencialidad

El presente documento es de propiedad intelectual de BlatoRH Group, en adelante la **Consultora** o **BlatoRH**, y proporciona al **Destinatario** (Cliente, Consultor, u otro que lo reciba), con carácter de confidencial.

Este documento no podrá ser copiado bajo ninguna circunstancia, de manera total o parcial a excepción de que la Consultora proporcione por escrito la respectiva autorización.

El Destinatario como la Consultora utilizaran este documento para dejar constancia y en conocimiento del Destinatario, respecto de las políticas y procedimientos de BlatoRH.

El Cliente al recibir este documento, acepta y asume la obligación de respetar la presente cláusula de confidencialidad y respeto de la propiedad intelectual.

La Consultora y el Destinatario se comprometen a no divulgar la información que se encuentre en este documento.

## Alcance

### 1. Identificación del Incidente

- ☐ **Definición de Incidente:** Un incidente de seguridad se refiere a cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de la información, ya sea por acceso no autorizado, pérdida de datos, fuga de información o cualquier otra amenaza.
- ☐ **Tipos de Incidentes Comunes:**
  - o **Fuga de datos:** Información confidencial compartida o accesible por personas no autorizadas.
  - o **Acceso no autorizado:** Ingreso a sistemas o información sin los permisos adecuados.
  - o **Malware o ataques:** Infecciones de software malicioso que afecten la seguridad de los sistemas.

### 2. Notificación Inmediata

- ☐ **Responsabilidad de Notificación:** El consultor que detecte el incidente debe notificarlo inmediatamente a su supervisor directo y al equipo de seguridad de la información de Blatorh Group.
- ☐ **Canales de Notificación:**
  - o **Correo electrónico:** Enviar un correo al equipo de seguridad de la información con el asunto "Reporte de Incidente de Seguridad" y los detalles del incidente.
  - o **Teléfono o mensajería interna:** Utilizar los medios de comunicación internos para asegurarse de que el equipo de seguridad reciba la notificación lo antes posible.

### 3. Documentación del Incidente

- ☐ **Información Requerida:**
  - o **Descripción del incidente:** Explicar lo sucedido, incluyendo cómo se detectó el incidente y su impacto inicial.
  - o **Fecha y hora:** Registrar la fecha y hora exactas en que se detectó el incidente y cuándo se notificó.
  - o **Sistemas o información afectados:** Detallar qué sistemas o datos se vieron comprometidos.
  - o **Acciones tomadas:** Describir cualquier acción inmediata tomada para mitigar el impacto del incidente (por ejemplo, desconectar un sistema, cambiar contraseñas, etc.).

## 4. Evaluación Inicial

- ☐ **Responsabilidad de Evaluación:** El equipo de seguridad de la información realizará una evaluación inicial para determinar la gravedad del incidente y el alcance del daño.
- ☐ **Criterios de Evaluación:**
  - o **Gravedad:** Determinar si el incidente es menor, moderado o crítico.
  - o **Alcance:** Identificar cuántos sistemas, datos o personas se ven afectados por el incidente.
  - o **Impacto:** Evaluar el impacto potencial en la operación de Blatorh Group y sus clientes.

## 5. Respuesta y Mitigación

- ☐ **Implementación de Medidas de Contención:** El equipo de seguridad implementará medidas para contener el incidente y evitar que se propague o cause más daño.
- ☐ **Desconectar sistemas comprometidos:** Si es necesario, aislar sistemas que hayan sido comprometidos.
- ☐ **Restablecimiento de contraseñas:** Forzar el cambio de contraseñas para cuentas que hayan sido afectadas.
- ☐ **Monitoreo:** Iniciar un monitoreo constante de los sistemas para detectar actividades sospechosas adicionales.

## 6. Comunicación Interna y Externa

- ☐ **Informe Interno:** Preparar un informe interno detallando el incidente, las acciones tomadas y los próximos pasos, y distribuirlo a los líderes de Blatorh Group.
- ☐ **Notificación a Clientes:** Si el incidente afecta a clientes, notificarles de manera oportuna, proporcionando detalles relevantes y las acciones que se están tomando para mitigar el riesgo.
- ☐ **Confidencialidad:** Asegurar que toda comunicación con los clientes respete las políticas de confidencialidad y no revele más información de la necesaria.

## 7. Recuperación y Restauración

- ☐ **Restauración de Sistemas:** Una vez contenido el incidente, proceder a restaurar los sistemas y datos a su estado normal.
- ☐ **Revisión de Backups:** Verificar la integridad de los backups y, si es necesario, restaurar desde una copia de seguridad segura.
- ☐ **Validación:** Asegurar que todos los sistemas vuelvan a estar operativos y que no haya vulnerabilidades remanentes.

## 8. Análisis Post-Incidente

- ☐ **Revisión y Análisis:** El equipo de seguridad debe realizar una revisión completa del incidente para entender las causas raíz y cómo se puede prevenir en el futuro.
  - **Lecciones Aprendidas:** Documentar las lecciones aprendidas y mejorar los procedimientos y políticas de seguridad.
  - **Actualización de Políticas:** Basado en el análisis, actualizar las políticas de seguridad de Blatorh Group para prevenir incidentes similares.

## 9. Reporte Final y Archivo

- ☐ **Elaboración de un Reporte Final:** Crear un reporte final que incluya todos los detalles del incidente, desde su detección hasta la resolución y las lecciones aprendidas
- ☐ **Archivo Seguro:** Guardar el reporte en un lugar seguro y accesible para futuras referencias y auditorías.


## 10. Formación y Mejora Continua

- ☐ **Capacitación:** Realizar sesiones de formación con los consultores y empleados para asegurar que todos estén al tanto del procedimiento de reporte de incidentes y cómo deben actuar.
- ☐ **Simulacros de Incidentes:** Llevar a cabo simulacros periódicos para evaluar la preparación del equipo y mejorar la respuesta a incidentes reales.

## Conformidad

A continuación se deja constancia de la Conformidad de BlatoRH y el Destinatario, en relación a lo especificado en el presente Documento.

### Por BlatoRH Group

<i>Firma</i>	
<i>Aclaración</i>	Leonardo Blau
<i>Puesto/Cargo</i>	Director
<i>Fecha</i>	01/08/2024

### Por Destinatario

<i>Firma</i>	
<i>Aclaración</i>	
<i>Empresa</i>	
<i>Puesto/Cargo</i>	
<i>Fecha</i>	

