



Guía rápida para responder ante un incidente de seguridad

(DIRIGIDA A PERSONAL NO
TÉCNICO)



Objetivo de la guía

Esta guía tiene como propósito brindar al personal no técnico una ruta clara, sencilla y práctica para reconocer y actuar ante un incidente de seguridad de la información.

Está diseñada para minimizar daños, proteger la información de la empresa y facilitar una respuesta oportuna, sin necesidad de tener conocimientos técnicos avanzados.



Índice

1. ¿Qué es un incidente de seguridad?

2. ¿Por qué es importante saber cómo actuar?

3. ¿Cómo reconocer un incidente de seguridad?

4. Pasos para responder ante un incidente

Paso 01 Mantén la calma y evita actuar por impulso

Paso 02 No apagues ni desconectes el equipo (a menos que te lo indiquen)

Paso 03 Reporta inmediatamente al área correspondiente

Paso 04 No compartas la información del incidente

Paso 05 Sigue las instrucciones del equipo de respuesta

5. Recomendaciones adicionales

6. Información de contacto y apoyo



01

¿Qué es un
incidente de
seguridad?



¿Qué es un incidente de seguridad?

Es cualquier evento que compromete o pone en riesgo la confidencialidad, integridad o disponibilidad de la información.

Ejemplos comunes:

- Archivos o sistemas inaccesibles sin explicación
- Correos con enlaces sospechosos o errores ortográficos
- Programas que se abren solos o mensajes de error inusuales
- Pérdida o robo de equipos
- Ingreso no autorizado a cuentas o sistemas



02

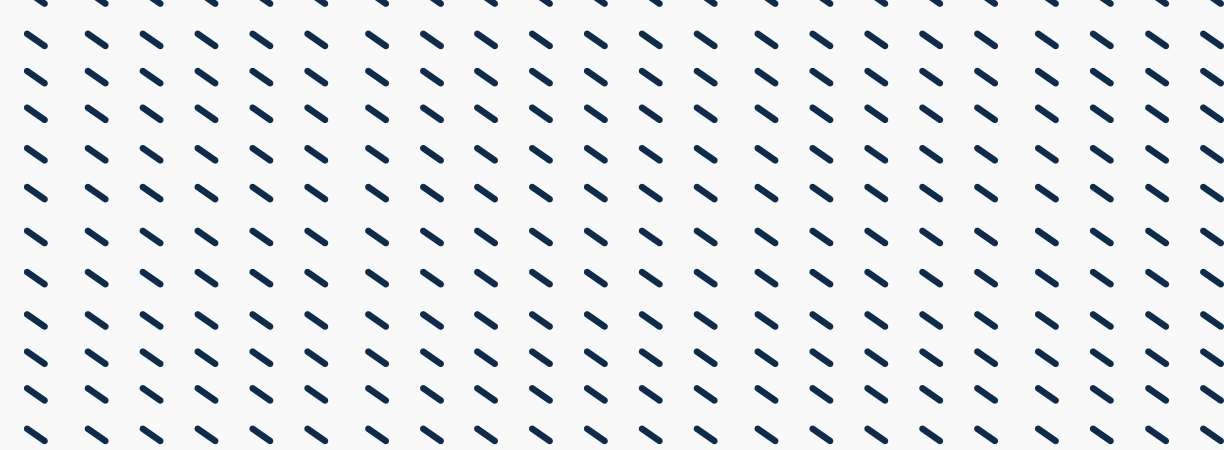
¿Por qué es
importante
saber cómo
actuar?



¿Por qué es importante saber cómo actuar?

Una respuesta rápida y ordenada puede:

- Prevenir que el daño se extienda
- Evitar la pérdida de información valiosa
- Proteger a otros colaboradores
- Facilitar el trabajo del equipo técnico
- Reducir el impacto legal, reputacional o económico



03 ¿Cómo reconocer un incidente de seguridad?



¿Cómo reconocer un incidente de seguridad?

Algunas señales de alerta:

- Mensajes de ransomware o bloqueo de pantalla
- Archivos cifrados o renombrados repentinamente
- Cambios inesperados en configuraciones
- Correos sospechosos solicitando contraseñas o datos
- Notificaciones de inicio de sesión desde ubicaciones inusuales



04

Pasos para responder ante un incidente

Paso 1: Mantén la calma y evita actuar por impulso

No intentes “arreglarlo” por tu cuenta. Apagar, desconectar, borrar o reenviar puede complicar el análisis del incidente.



Paso 2: No apagues ni desconectes el equipo (a menos que te lo indiquen)

El equipo técnico puede necesitar rastrear qué ocurrió. Solo desconéctalo si ves que el daño se está propagando muy rápido y te lo han autorizado previamente.



Paso 3: Reporta inmediatamente al área correspondiente

Envía un correo, mensaje o llama según el protocolo interno.

Incluye:

- Qué ocurrió
- Hora en que lo notaste
- Qué hiciste antes y después
- No tengas miedo de “alarmar”; es mejor prevenir.



Paso 4: No compartas la información del incidente

Evita divulgar el problema en chats, redes sociales o conversaciones informales. Esto puede exponer más información o generar confusión.



Paso 5: Sigue las instrucciones del equipo de respuesta

Es posible que te pidan:

- Detener el uso del equipo
- Cambiar contraseñas
- Desconectar algún dispositivo
- Entregar capturas o evidencia
- Sigue cada paso tal como se indica. Anota lo que haces.





05

Recomendaciones adicionales



Recomendaciones adicionales

- Ten siempre a la mano los datos de contacto del área de TI o seguridad.
- Familiarízate con los procedimientos internos.
- Si recibes capacitación en concientización, participa activamente.
- No ignores señales inusuales, aunque parezcan pequeñas.
- Recuerda: no se castiga reportar un incidente; se agradece.



06

Información de contacto y apoyo



Información de contacto y apoyo

Guardianes del Golfo

- **info@guardianesdelgolfo.com**
- **+52 22 95 91 22 46**
- **www.guardianesdelgolfo.net**

¿Tu empresa necesita un protocolo accesible y campañas de concientización?

Contáctanos y diseñamos un plan a tu medida.