
TIC
¿Si tengo un incidente de seguridad digital cómo debo actuar?
COLCERT

## Si la entidad/organización detecta un incidente de Seguridad Digital, debe:

1. **Activar el Equipo de respuesta a incidentes interno** e iniciar con el procedimiento establecido por la entidad/organización.
2. **Verificar la afectación del entorno TI,** analizar logs de plataformas de seguridad, servidores, redes y aplicaciones, correlacionar eventos, identificar patrones y crear matriz de diagnóstico y seguimiento.
3. **Evaluar con base en el análisis de riesgo y clasificación de activos** de información los niveles de impacto (alto, medio bajo).
4. **Clasificar el incidente teniendo en cuenta: i)** Características de la afectación en sistemas de información o infraestructura TI **ii)** patrones de comportamiento detectados y **iii)** afectación en la información (ver taxonomía COLCERT).
5. **Establecer el nivel de prioridad de atención según los criterios: i)** Impacto y **ii)** Urgencia de la atención.

## Cierre

**Reportar el incidente una vez sea gestionado y cerrado** en el **formulario** publicado en la página de inicio del portal web ColCERT.

**Registrar las lecciones aprendidas, ajustar controles y medidas de seguridad** para el cierre de brechas identificadas.

**Activar planes de contingencia y plan de continuidad para recuperación de la operación** mientras se restablece la infraestructura y servicios de TI.

**Realizar acciones de contención, erradicación, recuperación y post incidente** bajo el liderazgo y coordinación del CISO/Encargado de Seguridad Digital de la entidad/organización.

**Menos graves y Menor**

## ¿El incidente, es clasificado como?

**Muy Grave o Grave**

**Reportar el Incidente al COLCERT,**
**para apoyo y coordinación de su gestión;**
**Enviar formato de reporte establecido.**

## Canales de atención:

**Buzón de correo:** contacto@colcert.gov.co
**Línea directa:** +57 601 344 2222
**Sitio web:** https://www.colcert.gov.co

**Realizar validación estado del incidente, con el CISO y/o encargado para identificar infraestructura afectada, acciones de:** contención, erradicación, recuperación y post incidente, realizadas.

**Identificar y definir necesidad de acompañamiento presencial o seguimiento virtual** y acciones de coordinación para la contención, erradicación, recuperación y post incidente.

**Iniciar la coordinación y actuaciones con** la Fiscalía General de la Nación y Centro Cibernético Policial - CECIP para inicio de investigación judicial. (actos urgentes – instauración de denuncia, recolección de Elementos Materiales Probatorios y Evidencia Física - (evidencia digital)

**Si afecto BD que contiene datos personales,** realizar el reporte del incidente a la Super Intendencia de Industria y Comercio SIC.

**Realizar mesas de trabajo para identificación de necesidades:**

- **Direccionamiento** plan de acción gestión del incidente.
- **Entrega de capacidades** para erradicación, recuperación y post- incidente.
- **Coordinación apoyos** con industria y aliados.
- **Coordinación con capacidades del Estado** (Instancias Ciber).
- **Coordinación entidades de Gobierno** frente a cumplimientos y apoyos.
- **Coordinación con homólogos** locales, regionales y globales.

## Cierre COLCERT

**Realizar una mesa técnica para revisar lecciones aprendidas, cumplimiento plan de acción,** ajuste matriz de riesgos e implementación de controles.

**Realizar seguimiento y acompañamiento actividades de recuperación y post-incidente** hasta el cierre y recuperación de la operación.

**Establecer protocolo y canal de comunicación** para interlocución mesas de trabajo con el equipo de la entidad/organización.