

PASOS PARA NOTIFICAR UN CIBERINCIDENTE EN CUMPLIMIENTO DEL DECRETO 273.

PASO 1: MANTENGA LA CALMA Y REÚNA INFORMACIÓN

Mantenga la calma y reúna el máximo de información posible sobre el incidente que está ocurriendo o que los ha afectado. Algunos datos que son de utilidad:

- El tipo de incidente que se cree está actuando, por ejemplo, un ransomware. Apóyese en la “taxonomía de incidentes” de la “guía de notificación”.
- Una primera impresión de la afectación o impacto que el incidente tiene en su institución. Inicialmente puede ser una impresión cualitativa. Vea algunos ejemplos en “la tabla de afectación de incidentes” de la “guía de notificación”.
- Solo si, de acuerdo con el incidente que esté afectándolos y si es sencillo de obtener, recopilar los indicadores de compromiso básicos, tales como: nombres de archivos, IP’s, email o hashes involucrados en la actividad maliciosa (idealmente una muestra del malware).
- Los datos de contacto para que el CSIRT coordine la asistencia según la pertinencia del caso.
- Los datos del punto de contacto de sus proveedores tecnológicos pertinentes al incidente y las plataformas afectadas.

PASO 2: CONTACTE AL CSIRT

Conéctese al sitio <http://www.csirt.gob.cl> y seleccione “NOTIFICAR UN INCIDENTE”. Al hacer clic se desplegará un formulario que debe completar con la información solicitada (datos de la persona que reporta datos de la entidad afectada, activos comprometido y descripción).

En la parte de “Descripción de incidente”, usted debe elaborar una breve descripción del incidente. Piense en un párrafo corto que resuma lo que se está viviendo en el momento con foco en el incidente de ciberseguridad y los impactos percibidos, según la línea temporal de la detección.

Si por alguna razón su plataforma de acceso a internet está comprometida, puede llamar al CSIRT al teléfono **1510** o al **+56 2 2486 3850**, las 24 horas del día, todos los días del año.

En el caso de que su sistema de telefonía también esté afectado, intente reportar mediante otro teléfono móvil (no conectado a la WIFI institucional) y que le permita navegar hacia el sitio web <https://www.csirt.gob.cl>.

PASO 3: VERIFIQUE QUE HA RECIBIDO UN TICKET DEL CSIRT

Asegúrese de que el CSIRT le ha enviado un email con el número de ticket que confirme, a efectos de trazabilidad, que el incidente ha sido reportado en los tiempos establecidos por el [Decreto 273](#).

PASO 4: ESTÉ ATENTO ANTE UN EVENTUAL CONTACTO DEL CSIRT

Instruya a los puntos de contacto establecidos para que estén disponibles para comunicarse con el CSIRT, organización que dispondrá de su estructura técnica para apoyar, según la disponibilidad de recursos, las primeras fases de la gestión del incidente.

Y RECUERDE DOS COSAS:

- Actualizar la información sobre el incidente al CSIRT hasta que este haya sido cerrado.
- Denunciar a la Policía o Fiscalía si el incidente constituye un delito informático de acuerdo con la [ley](#).

CONTACTO Y REDES SOCIALES DE CSIRT