EQUIPO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD INFORMÁTICA

CSIRT

Subsecretaría del Interior
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

SOBRE EL DECRETO 273
y la notificación de incidentes

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

DECRETO 273

- Artículo 1°
- Artículo 2°
- Artículo 3°
- Artículo 4°

DECRETO 273

Artículo 1°

Artículo 2°

Artículo 3°

Artículo 4°

Notificación de incidentes de ciberseguridad.

Los **jefes de servicio** de los Ministerios y demás organismos de la Administración centralizada y descentralizada del Estado **deberán comunicar los incidentes** de ciberseguridad que les **afecten**, al Ministerio del Interior y Seguridad Pública, mediante su **notificación** al Centro de Respuesta ante Incidentes de Seguridad Informática ("**CSIRT**"), en el sitio web: https://csirt.gob.cl.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

DECRETO 273

- Artículo 1°
- Artículo 2°
- Artículo 3°
- Artículo 4°

Plazo para la notificación.

La comunicación anterior deberá realizarse tan pronto se constate su ocurrencia, no pudiendo ser este **plazo** superior a **3 horas desde que se tome conocimiento**.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

DECRETO 273

- Artículo 1°
- Artículo 2°
- Artículo 3°
- Artículo 4°

Información sobre amenazas a los órganos de la administración del Estado.

Los jefes de servicio establecidos en el artículo 1, dentro del ámbito de sus facultades, y **respecto de los contratos** que se celebren con posterioridad a la entrada en vigencia del presente decreto, **deberán exigir a los proveedores** de servicios de tecnologías de la información, **que compartan la información sobre las amenazas y vulnerabilidades** que puedan afectar a las redes, plataformas y sistemas informáticos de los órganos de la administración del Estado, al igual que las **medidas de mitigación aplicadas** a éstas, así como las **políticas y prácticas de seguridad** de la información incorporadas en los servicios prestados.

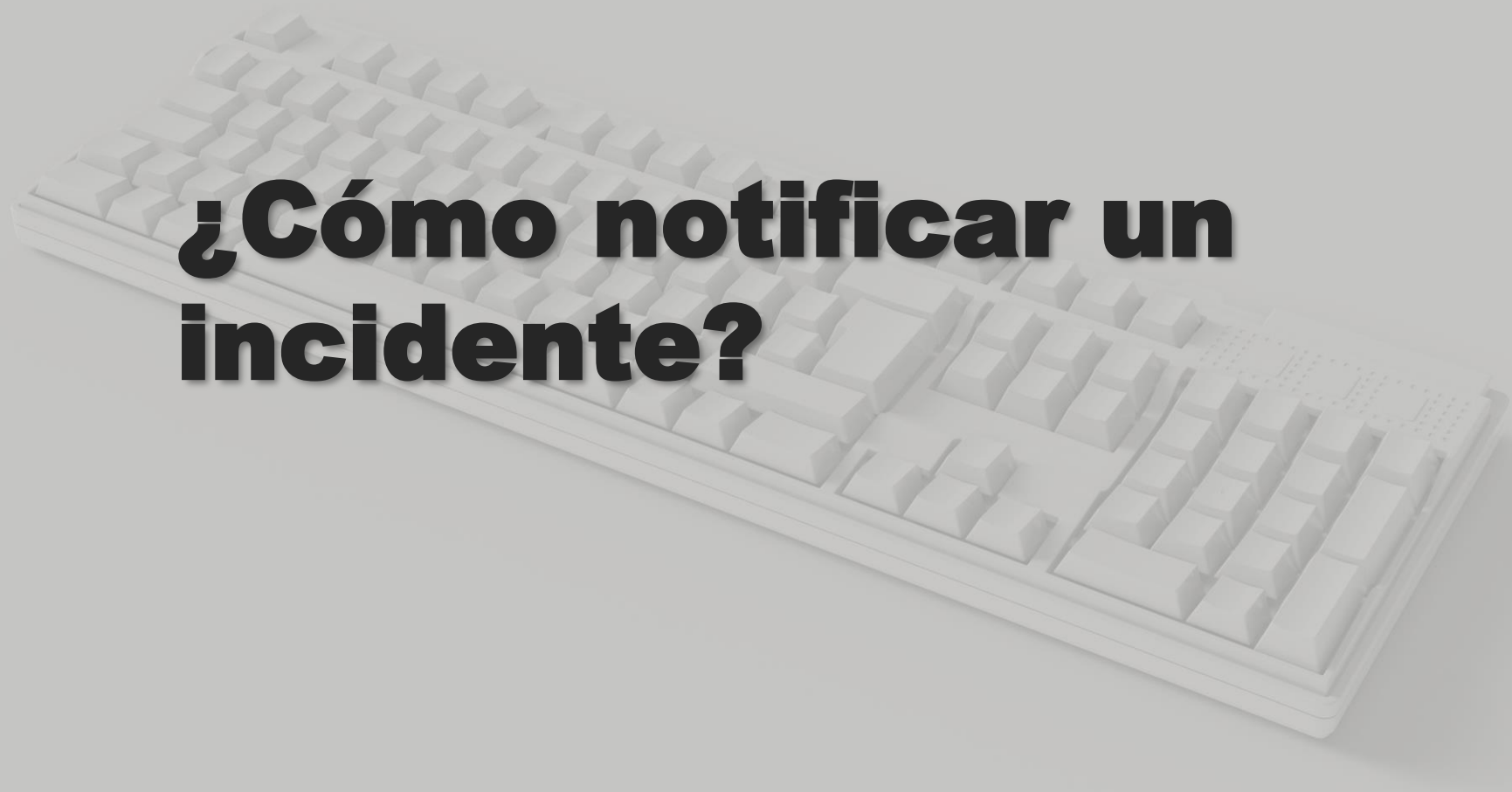
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

DECRETO 273

- Artículo 1°
- Artículo 2°
- Artículo 3°
- Artículo 4°

Búsqueda preventiva de vulnerabilidades.
Para mejorar la seguridad de las redes y sistemas informáticos de su respectiva institución, los jefes de servicio indicados en el artículo 1º, **pueden solicitar a los equipos técnicos del CSIRT su revisión y análisis**, incluyendo la **búsqueda preventiva de vulnerabilidades** informáticas, otorgando las facilidades que sean necesarias para ello.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática



¿Cómo notificar un incidente?

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

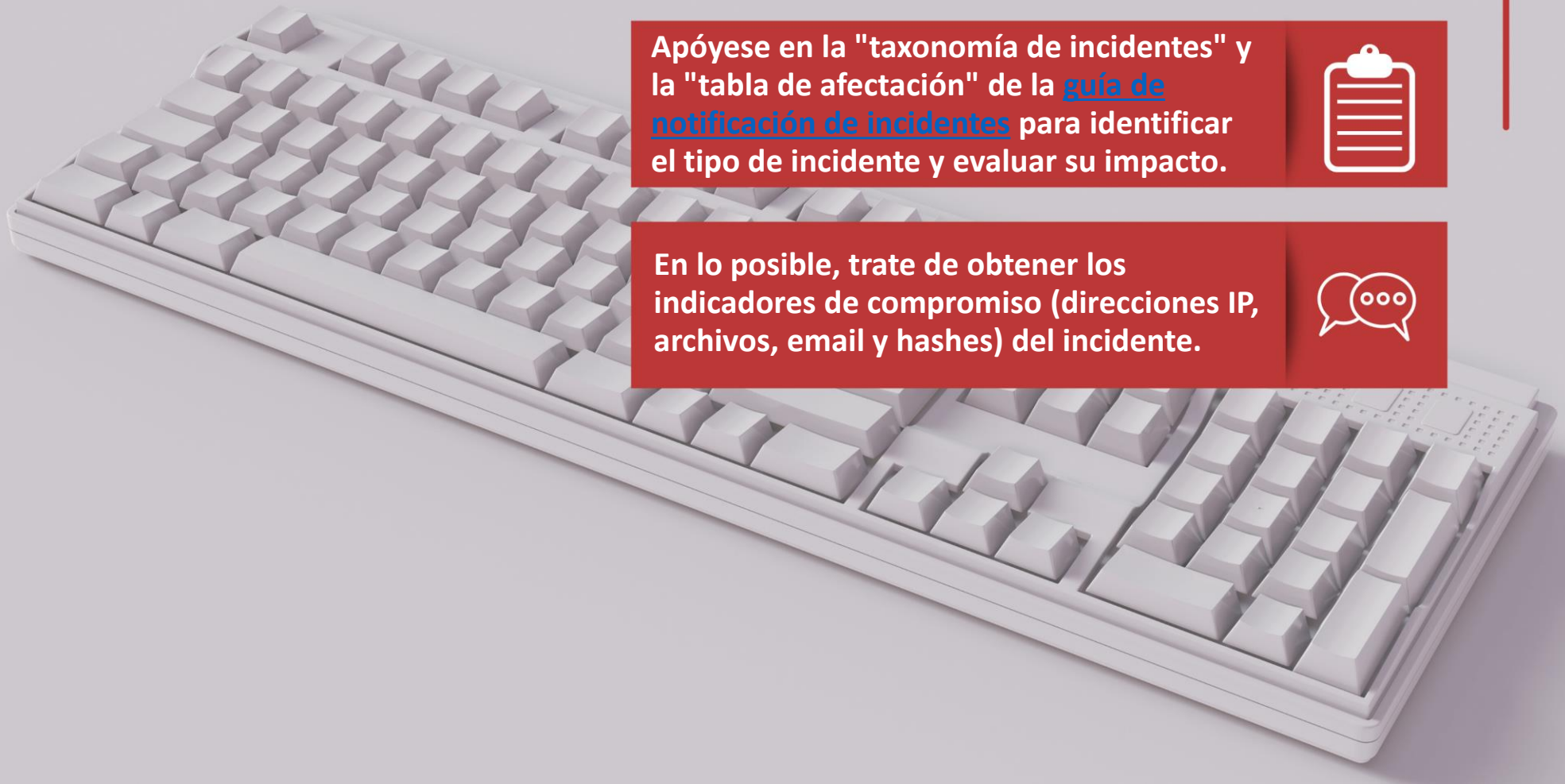
PASO 1

MANTENGA LA CALMA Y REÚNA INFORMACIÓN

Asegúrese de contar con los contactos de CSIRT y de sus proveedores.

Apóyese en la "taxonomía de incidentes" y la "tabla de afectación" de la guía de notificación de incidentes para identificar el tipo de incidente y evaluar su impacto.

En lo posible, trate de obtener los indicadores de compromiso (direcciones IP, archivos, email y hashes) del incidente.



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

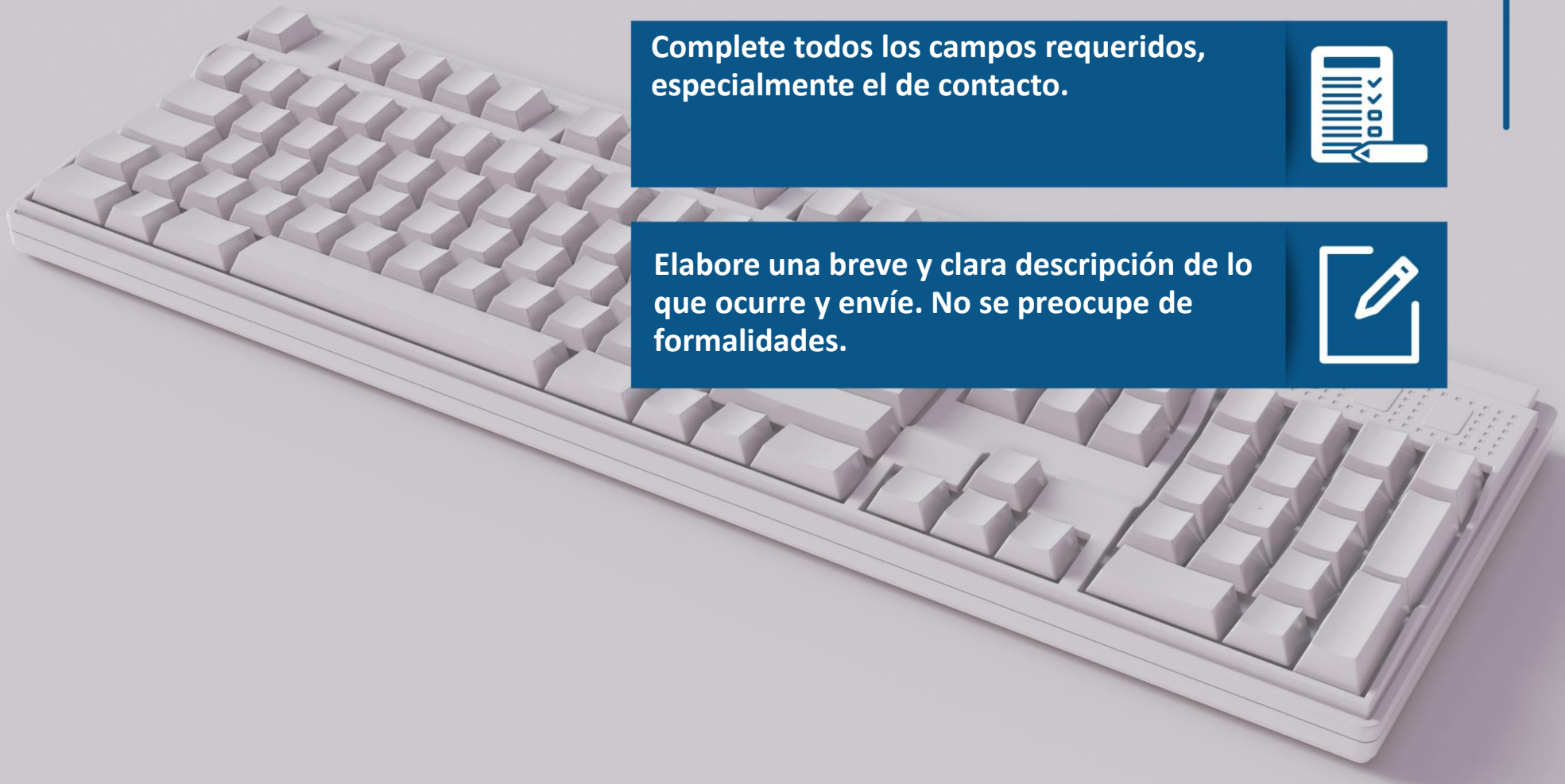
PASO 2

CONTACTE AL CSIRT

Diríjase al formulario de notificación de incidentes disponible en www.csirt.gob.cl

Complete todos los campos requeridos, especialmente el de contacto.

Elabore una breve y clara descripción de lo que ocurre y envíe. No se preocupe de formalidades.



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

PASO 3

VERIFIQUE QUE HA RECIBIDO UN TICKET DEL CSIRT

Luego de enviar el formulario, revise en su correo de contacto que ha recibido un ticket sobre el incidente.

Este ticket es importante para la trazabilidad del incidente.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

PASO 4

ESTÉ ATENTO ANTE EVENTUAL CONTACTO DEL CSIRT

Instruya a los puntos de contacto establecidos en el formulario que deben estar preparados para comunicarse con el CSIRT

El CSIRT podrá disponer de su estructura técnica y humana para apoyar la primera parte de su gestión de respuesta

CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática