RFC 2350 del CSIRT de Gobierno

1.- Información del documento

1.1. Fecha de la última actualización: versión 1.0, publicada el 19 de octubre

1.2. Listas de Distribución: No existe un canal de distribución para notificar cambios en este documento. Los cambios son anunciados por medio de notificación en https//www.csirt.gob.cl

1.3. Ubicación del Documento: La última versión del documento se encuentra publicada en:

- Español: https://www.csirt.gob.cl/media/2021/10/RFC2350-final.pdf
- Inglés: https://www.csirt.gob.cl/media/2021/10/RFC2350-english.pdf

1.4. Autenticación del Documento: Este documento ha sido firmado digitalmente por CSIRT Gob

2. Información de Contacto

2.1. Nombre del Equipo: CSIRT de Gobierno, Equipo de respuesta ante incidentes de Seguridad Informática del Gobierno de Chile, dependiente de la Subsecretaria del Interior.

2.2. Dirección: Teatinos 92 piso 6, Santiago de Chile.

2.3. Zona Horaria: (GMT-4)

2.4. Número de Teléfono: (+562) 24863850

2.5. Número de Fax: No existente

2.6. Otras Comunicaciones: soc@interior.gob.cl

2.7. Direcciones de Correo Electrónico:

- Intercambio de información relativa a incidentes: soc@interior.gob.cl
- Consultas de carácter general: csirt@interior.gob.cl
- Contacto comunicacional: comunicaciones@interior.gob.cl
- Contacto internacional: international@csirt.gob.cl
- Contacto legal: legal@csirt.gob.cl

2.8. Claves Públicas y cifrado de información: No disponible

2.9. Miembros del Equipo: No disponible

2.10. Más Información: La información general sobre los servicios proporcionados por CSIRT Gob y sobre el propio organismo se encuentra publicada en el portal web: https//www.csirt.gob.cl.

2.11. Horario de Atención: El equipo de respuesta a incidentes está disponible en la modalidad 24x7x365.

2.12. Puntos de contacto para la comunidad:

La comunicación entre el Equipo CSIRT y los organismos a los que da soporte se realiza principalmente a través de:

- Formulario de registro de incidente en el sitio web: www.csirt.gob.cl
- Correo electrónico: soc@interior.gob.cl
- Numero de emergencia de registro de incidentes: 1510

3. Constitución

3.1. Misión: es reducir los riesgos cibernéticos en las redes del Gobierno de Chile, asesorando a las diferentes organizaciones que lo componen, actuar como socio estratégico en la defensa de las amenazas y colaborar para brindar mayor seguridad y robustez a las infraestructuras del Estado.

Nuestros objetivos son:

- Proveer información y asistencia a la Red de Conectividad del Estado y, en general, al Ciberespacio Gubernamental.
- Administrar un Sistema de Cooperación Nacional e internacional en materias de ciberseguridad, con el objetivo de reducir el riesgo y articular la respuesta a éstos cuando su materialización sea efectiva.
- Promover buenas prácticas en materia de ciberseguridad en la Administración Gubernamental.
- Promover la Protección de las Infraestructuras de Información Críticas País (CIIP por sus siglas en inglés) y Recursos Claves.
- Promover el fortalecimiento del marco jurídico en lo que se refiere a delitos Informáticos y Cibercrimen.
- Promover la concienciación en materias de ciberseguridad.

Nuestro objetivo estratégico institucional:

- Apoyar y fortalecer la acción tecnológica gubernamental, ampliando el uso de tecnologías de información y comunicación en la gestión pública, a través de la mantención y control de la Red de Conectividad del Estado.

3.2. Comunidad a la que brinda servicios: Todas los Órganos de la Administración del Estado referenciados en el Instructivo Presidencial N°8 (https://transparenciaactiva.presidencia.cl/instructivos/Instructivo-2018-008.pdf), asi como a las instituciones privadas estratégicas, universidades y ONG vinculadas vía convenio de colaboración al CSIRT.

3.3. Patrocinio / Afiliación: El CSIRT de Gobierno forma parte de la División de Redes y Seguridad Informática de la Subsecretaria del Interior.

3.4. Autoridad: La autoridad del CSIRT de Gobierno emana de:

- Resolución Exenta N° 5.006, de 2019, que dispone la creación de la División de Redes y Seguridad Informática, de la Subsecretaria del Interior.
- Resolución Exenta N° 11.536, de 2020 que modifica la Resolución Exenta N° 5006, de la Subsecretaria del Interior.

4. Políticas

4.1. Tipo de Incidentes y nivel de soporte:

La tipología de ciberincidentes sobre los que actúa el CSIRT de Gobierno, está contenida en la guía de clasificación de incidentes, disponible en el siguiente link https://www.csirt.gob.cl/media/2021/10/Guia-de-notificacion-ciberincidentes.pdf.

CSIRT de Gobierno, como CSIRT Gubernamental Nacional, colabora con todos los organismos públicos y empresas de interés estratégico vinculadas por convenio de cooperación en la detección, notificación, evaluación, respuesta, tratamiento y aprendizaje de incidentes de seguridad de información o ciberincidentes que puedan sufrir sus sistemas.

El nivel de apoyo que brinda el CSIRT y el tiempo de respuesta del mismo, dependerá del nivel de peligrosidad y criticidad del incidente, todo ello según la clasificación disponible en el siguiente link https://www.csirt.gob.cl/media/2021/10/Guia-de-notificacion-ciberincidentes.pdf.

CSIRT de Gobierno, también ofrece información sobre el estado de la ciberseguridad a su Comunidad, con el fin de reducir tanto las vulnerabilidades técnicas, como humanas y de organización. Para ello, notifica periódicamente la siguiente información:

- Alertas de amenazas/vulnerabilidades detectadas por el propio CSIRT o compartidas por terceras personas
- Alertas de incidente relevantes
- Vulnerabilidades los principales fabricantes
- Campañas semanales de concientización ciudadana
- Informes de amenazas
- Revista mensual CiberSucesos
- Investigaciones de tendencias
- Comandos para autochequeo
- Controles de implementación de los controles de la ISO 27.001

4.2. Cooperación, Interacción y divulgación de la Información:

La información manejada por CSIRT de Gobierno, es tratada con absoluta confidencialidad de acuerdo a las políticas y procedimientos establecidos y en cuanto a la forma como se comparte, se basa en el protocolo TLP, el cual es aceptado internacionalmente.

4.3. Comunicación

Los medios disponibles para la comunicación con el CSIRT de Gobierno son:

- Intercambio de información relativa a incidentes: soc@interior.gob.cl
- Consultas de carácter general: csirt@interior.gob.cl
- Contacto comunicacional: comunicaciones@interior.gob.cl
- Contacto internacional: international@csirt.gob.cl
- Contacto legal: legal@csirt.gob.cl

5. Servicios

- Monitorear sitios web por posible defacement a través de la herramienta de desarrollo propio "Andes defacement".
- Alertar inscripción sitios web en Nic de posibles sitios fraudulentos a través de la herramienta de desarrollo propio, "La Campana".
- Escanear y hacer pentesting a sitios web.
- Alertar o advertir a las instituciones cuando se detecten incidentes o ante posibles riesgos producto del análisis de vulnerabilidades del sistema.
- Investigar sobre nuevas tecnologías y herramientas generando documentación al respecto.
- Concentrar información sobre vulnerabilidades, realizando análisis que permitan detectar posibles riesgos.
- Promover buenas prácticas y hábitos de ciberseguridad entre los usuarios del sistema.
- Capacitar continuamente a los usuarios del sistema y a los profesionales de la ciberseguridad.
- Promover y generar protocolos y rutinas de ciberseguridad dirigido a los usuarios, administradores y actores relevantes de los sistemas.
- Para la resiliencia en los sistemas informáticos, CSIRT desarrolla una serie de acciones reactivas y ofrece respuestas rápidas a la comunidad de gobierno, entre las cuales están:
- Entregar respuesta a incidentes informados por los sistemas de monitoreo o por el registro directo de los órganos de la Administración del Estado.
- Entregar respuesta a vulnerabilidades detectadas a través de los distintos dispositivos o análisis de vulnerabilidades, enviando mensajes de alerta.
- Entregar asistencia in situ en caso de ser necesario para realizar análisis forense o investigativo.
- En el caso de la ocurrencia de incidentes de seguridad de la información que se consideren críticos, adoptar las medidas necesarias para salir de la contingencia.
- Realizar seguimiento al cumplimiento de mitigación de las vulnerabilidades detectadas e informadas por los distintos medios por parte de los órganos de la Administración del Estado.
- Ejecutar los diferentes planes de acción que exige el instructivo presidencial de Ciberseguridad
- Cumplir y velar por el cumplimiento de lo estipulado por los Decretos de Gobierno y la legislación vigente en los organismos del gobierno con los que interactúa.

El detalle de los servicios, está contenido en la guía "Marco de servicios del CSIRT de Gobierno" la que se encuentra disponible en el siguiente enlace https://www.csirt.gob.cl/media/2021/10/Marco-de-servicios-del-CSIRT-de-Gobierno.pdf.

6. Formas de notificación de incidentes:

La notificación de incidentes puede realizarse mediante:

- Formulario de registro de incidente en el sitio web: www.csirt.gob.cl
- Correo electrónico: soc@interior.gob.cl
- Numero de emergencia de registro de incidentes: 1510

7. Disclaimer:

El CSIRT de Gobierno no se responsabiliza del mal uso que pueda darse de la información aquí contenida.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.10.25 12:39:02 -03'00'