RFC 2350 del CSIRT de Gobierno

1.- Información del documento

1.1. Fecha de la última actualización: versión 2.0, publicada el 19 de enero de 2024.

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.pdf

· Inglés: https://www.csirt.gob.cl/media/2021 /10/RFC2350-en.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: incidentes@interior.gob.cl

2.7. Direcciones de Correo Electrónico:

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

2.8. Claves Públicas y cifrado de información:

Disponible para el correo incidentes@interior.gob.cl

-----BEGIN PGP PUBLIC KEY BLOCK-----

mDMEZafa0xYJKwYBBAHaRw8BAQdAQAUGs5PR6cyHDe2WqWZV3qn7kgFoP5najgN4
8ndQW4O0LUluY2lkZW50ZXMgQ1NJUlQgPGluY2lkZW50ZXNAaW50ZXJpb3IuZ29i
LmNsPoiZBBMWCgBBFiEE8UZXgln8sT7kAROj1cuYy0X8tBkFAmWn2tMCGyMFCQPD
yR0FCwkIBwICIgIGFQoJCAsCBBYCAwECHgcCF4AACgkQ1cuYy0X8tBmU7wEAlFWT
3hs5XoL0mqBHQDu6LAf6uF/oNQ2rVSDcooX3C6QA/j3XEne9vnJjpPl4j6t/yF8A
3JW6dUrDRaWIv1gpm+oLuDgEZafa0xIKKwYBBAGXVQEFAQEHQHYLetKFGBBZInrr
o3M6l6WM5YzZznQOBEhBqc67D6IHAwEIB4h+BBgWCgAmFiEE8UZXgln8sT7kAROj
1cuYy0X8tBkFAmWn2tMCGwwFCQPDyR0ACgkQ1cuYy0X8tBmdswD/Yfjy0sPpPmsI
gKN1IEiywBEN/kTFcsDqGAh20E33j4wBAOPzrVgFATSHVevBwiHSlhpbMGJSGuJ5
xsdI9Nx6afgL
=zAaM
-----END PGP PUBLIC KEY BLOCK-----

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: incidentes@interior.gob.cl
- Numero de emergencia de registro de incidentes: 1510

3. Constitución

3.1. Misión:

Coordinar la respuesta a incidentes de ciberseguridad de efecto significativo en el país, y apoyar técnicamente a los Organismos de Administración del Estado en los incidentes que afecten su capacidad de seguir operando.

Nuestros objetivos son:

- Responder ante ciberataques o incidentes de ciberseguridad.
- Servir de punto de enlace con Equipos de Respuesta a Incidentes de Seguridad Informática extranjeros o sus equivalentes para el intercambio de información de ciberseguridad, siempre dentro del marco de sus competencias.
- Prestar colaboración o asesoría técnica a los CSIRT que pertenezcan a organismos de la Administración del Estado en la implementación de políticas y acciones relativas a ciberseguridad.
- Supervisar incidentes a escala nacional.
- Realizar entrenamiento, educación y capacitación en materia de ciberseguridad.
- Requerir a las instituciones afectadas o a los CSIRT correspondientes, información anonimizada de incidentes de ciberseguridad y vulnerabilidades encontradas y los planes de acción respectivos para mitigarlos.
- Difundir alertas tempranas, avisos e información sobre riesgos e incidentes para la comunidad.

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), así 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 Coordinación Nacional de Ciberseguridad de la Subsecretaría 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
- Investigaciones de tendencias

4.2. Cooperación, Interacción y divulgación de la Información:

La información manejada por el 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: incidentes@interior.gob.cl
- Consultas de carácter general: csirt-comunicaciones@interior.gob.cl
- Contacto legal: csirt-legal@interior.gob.cl

5. Servicios

- Escaneo de sitios web
- Auditoría
- Pentesting
- Monitoreo disponibilidad de sitios web
- Análisis de artefactos maliciosos y análisis forense
- Alertas de incidentes y vulnerabilidades
- Campañas de concientización y buenas prácticas
- Capacitación para funcionarios
- Intercambio de indicadores de compromiso
- Detección y prevención de intrusiones
- Protección Anti DDoS
- Protección Web Aplication Firewall (WAF)
- Bloqueo preventivo de amenazas
- DNS Resolver
- Creación de dominios ".gob.cl"

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: incidentes@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.