Chilean Government CSIRT RFC 2350

1. - Document information

1.1. Date of last update: version 1.0, published on October 19th, 2021.

1.2. Distribution list: There is no distribution channel to notify modifications in this document. Changes will be announced via a notice on https//www.csirt.gob.cl

1.3. Document location: The latest version of this document is located at:

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

1.4. Document authentication: This document was electronically signed by CSIRT Gob.

2. Contact information

2.1. Team name: CSIRT de Gobierno, Cybersecurity Incident Response Team of the Government of Chile, under the authority of the Undersecretary of the Interior.

2.2. Address: Teatinos 92, 6th floor, Santiago, Chile.

2.3. Time zone: GMT-4.

2.4. Phone number: (+562) 24863850.

2.5. Fax number: Not applicable.

2.6. Other notifications: soc@interior.gob.cl

2.7. Email addresses

- Incident information exchanges: soc@interior.gob.cl
- Other requests csirt@interior.gob.cl
- Communications department: comunicaciones@interior.gob.cl
- International department: international@csirt.gob.cl
- Legal department: legal@csirt.gob.cl

2.8. Public keys and information encryption: Not available.

2.9. Team members: Not available.

2.10. Additional information: The general information about the services provided by the Chilean Government CSIRT and about the organ itself, are available at: https//www.csirt.gob.cl

2.11. Service hours: The Chilean Government's CSIRT is available every day, at every time, during 365 days every year.

2.12. Community contact points:

Communication between CSIRT personnel and those entities it gives support to is conducted mainly via:

- Website incident record contact form: www.csirt.gob.cl
- Email: soc@interior.gob.cl
- Incident record phone number: 1510

3. Constitution

3.1. Mission: Our mission is to reduce the cyber risks on the Chilean government's networks, counselling the different departments that are part of them, acting as a strategic partner in the defence against threats and collaborating to give better safety and robustness to the infrastructure of the State.

Our objectives are:

- To provide information and assistance to the Connectivity Network of the State (Red de Conectividad del Estado) and, in general, to the Government's cyberspace.
- To manage a national and international cooperation system in matters of cybersecurity, with the aim of reducing risk and formulating a response to them when they materialize.
- To promote the best practices in matters of cybersecurity within the Administration.
- To further Critical Information Infrastructure Protection (CIIP) in Chile, alongside that of its key resources.
- To push for the strengthening of the legal framework regarding cybercrime.
- To promote awareness in matters of cybersecurity.

Our strategic institutional objective:

- To support and strengthen the Government's technological action, broadening the use of information and communication technologies in the public administration through the maintenance and control of the State Connectivity Network.

3.2. Communities it serves: All bodies of the Administration of the State defined by the document by the name Instructivo Presidencial No. 8 (https://transparenciaactiva.presidencia.cl/instructivos/Instructivo-2018-008.pdf), as well as to those strategic private institutions, universities and NGOs which have entered into an agreement with our CSIRT.

3.3. Reports to: The Chilean Government CSIRT is part of the Networks and Computer Safety Division at the Undersecretary of the Interior.

3.4. Authority: The authority of the Chilean Government CSIRT originates from:

- Resolución Exenta N° 5.006, 2019, that creates the Networks and Computer Safety Division of the Undersecretary of the Interior.
- Resolución Exenta N° 11.536, 2020 that modifies the Resolución Exenta N° 5006, from the Undersecretary of the Interior.

4. Policies

4.1. Type of incident and level of support:

The cyber incident nomenclature used by the Chilean Government CSIRT is detailed in the Incident Typification Guide, which can be accessed here (guide in Spanish):

https://www.csirt.gob.cl/media/2021/10/Guia-de-notificacion-ciberincidentes.pdf.

The Chilean Government CSIRT collaborates with every public body and strategic company with which it has entered into a collaboration agreement, aiding them in the detection, notification, evaluation, response, treatment and learning from information security incidents or cyber incidents that their systems might suffer.

The level of support given by the Chilean Government CSIRT and its response time depends on the danger and criticality of the incident, as described in the following classification:

https://www.csirt.gob.cl/media/2021/10/Guia-de-notificacion-ciberincidentes.pdf.

The Chilean Government CSIRT also offers information on the state of the cybersecurity to the public, with the aim to reduce technical, human and organizational vulnerabilities. To that effect, it gives alerts and notifies the public of the following events:

- Threat and vulnerability alerts, either detected by the CSIRT or denounced by third parties to us.
- Alerts related to relevant incidents.
- Vulnerabilities in the products of the main providers
- Weekly public awareness campaigns.
- Threat reports.
- CiberSucesos, our monthly magazine
- Research on new trends
- Commands for self-diagnostics.
- ISO 27.0002 control implementation controls

4.2 Cooperation, Interaction and the sharing of information.

The information handled by the Chilean Government CSIRT is treated with the utmost privacy, as indicated by established policies and stablished procedures, and in regards to the form it can be shared, it is based upon the TLP protocol, accepted internationally.

4.3. Communications

The available ways to communicate with the Chilean Government CSIRT are as follows:

- Incident information exchanges: soc@interior.gob.cl
- Other requests csirt@interior.gob.cl
- Communications department: comunicaciones@interior.gob.cl
- International department: international@csirt.gob.cl
- Legal department: legal@csirt.gob.cl

5. Services

- Monitoring websites for cases of defacement through the self-developed tool called “Andes defacement”.
- Notifying of possible fraudulent websites registered at NIC.cl, through the self-developed tool called “La Campana”.
- Scanning and pentesting websites.
- Alerting institutions when incidents or possible risks are detected because of a system vulnerabilities analysis.
- Researching about new technologies and tools producing new documentation on the subjects.
- Gathering information on vulnerabilities, doing analysis that allow the detection of possible risks.
- Promoting best practices and habits within users of the system.
- Continually training users of the systems and cybersecurity professionals.
- Promoting and generating cybersecurity protocols and routines, mainly targeting users, administrators and relevant system actors.
- To make systems resilient, we are developing a series of reactive actions and offering fast responses to the Government community, such as:
    - Give response to incidents notified by monitoring systems or from the direct record by the bodies of the Administration.
    - Delivering responses to vulnerabilities detected within different devices or the vulnerability analysis sending alert messages.
- Giving assistance in situ in case of it being necessary to perform a forensic or investigative analysis.
- If critical information security incidents tale place, taking the necessary steps to recover from the contingency.
- Performing follow-up check-ups of the fulfilment of mitigation measures of detected and informed vulnerabilities though different ways by the bodies of the Administration of the State.
- Putting into effect different action plans developed according to Instructivo Presidencial No. 8.
- Fulfilling and looking after the fulfilling of what is mandated by different Governmental decrees and enacted legislation by organs of the Government with which it interacts.

Further detail of these services is included in the guide “Marco de servicios del CSIRT de Gobierno” available at: https://www.csirt.gob.cl/media/2021/10/Marco-de-servicios-del-CSIRT-de-Gobierno.pdf.

6. Incident notification alternatives:

Incident notification can be done by:

- Website incident record contact form: www.csirt.gob.cl
- Email: soc@interior.gob.cl
- Incident record phone number: 1510

7. Disclaimer:

The Chilean Government CSIRT is not responsible by any improper use of the information hereby contained.