RFC 2350 | Chilean Government CSIRT (CSIRT de Gobierno)

1.- Document information

1.1. Date of last update: Version 2.0, published on January 22, 2024.

1.2. Distribution list: There is no distribution channel to notify modifications to this document. Changes will be announced in the CSIRT website, at https//www.csirt.gob.cl.

1.3. Document location: The latest version of this document can be found on:

· Spanish: https://www.csirt.gob.cl/media/2021/10/RFC2350.pdf

· English: https://www.csirt.gob.cl/media/2021/10/RFC2350-en.pdf

1.4. Document authentication: This document is digitally signed by the Chilean Government CSIRT.

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: 92 Teatinos, 6th floor, Santiago, Chile 8340521.

2.3. Time zone: (GMT-4)

2.4. Phone number: +562 2486 3850

2.5. Fax number: Not applicable.

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

2.7. Email addresses:

- To report incidents: incidents@interior.gob.cl
- To request technical information: csirt-comunicaciones@interior.gob.cl
- To request legal information: csirt-legal@interior.gob.cl

2.8. Public keys and information encryption:

Available for the following email address: incidents@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. Team members: Not available.

2.10. Additional information: All public information about CSIRT and the services it provides are available at https//www.csirt.gob.cl

2.11. Service hours: CSIRT is available continuously through email and phone, 24 hours a day, 365 days the year.

2.12. Community contact points:

CSIRT staff may be contacted through:

- Our website: www.csirt.gob.cl. There is a web form to report incidents online.
- Our email to report incidents: incidentes@interior.gob.cl and incidents@interior.gob.cl
- Our short phone number, available anywhere within the country: 1510

3. Constitution

3.1. Mission: To coordinate the response to major cybersecurity incidents in the country and to provide technical support to public organizations which are facing cybersecurity incidents.

Our goals are:

- To respond to, to help to respond to, and to supervise responses to major cyberattacks or cybersecurity incidents; that is, incidents at a national level.
- To request information about cybersecurity incidents from organizations which have been attacked, as well as about vulnerabilities, action plans, and any other information related to cybersecurity planning and response.
- To share early alerts, notices and information on risks and incidents with the community.
- To train and educate cybersecurity officers in anything that may help to improve their capacities to respond to cyberattacks.
- To be a liaison to other CSIRT (o equivalent organizations) around the world.
- To cooperate with and to provide technical assistance to other governmental CSIRT.

3.2. Community to whom we serve: All public organizations defined in the Presidential Instruction number 8 (https://transparenciaactiva.presidencia.cl/instructivos/Instructivo-2018-008.pdf), as well as private institutions, universities and NGOs that have signed collaboration agreements with CSIRT.

3.3. Reports to: The Chilean Government CSIRT is part of the National Cybersecurity Coordination Office (Coordinación Nacional de Ciberseguridad), within the Undersecretary of the Interior (Subsecretaría del Interior).

3.4. Authority: The Chilean Government CSIRT originates its authority 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. Incident types and level of support:

The cyber incident taxonomy we use can be accessed here (guide in Spanish):

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

CSIRT collaborates with all public agencies, and with private companies with which it has signed a collaboration agreement. CSIRT provides help in the detection, notification, evaluation and response to cybersecurity incidents.

The specific help that the CSIRT can provide, and its response time, depends on the criticality of the incident. For more information, consult the document referenced above.

CSIRT also offers general information on cybersecurity to the public. Our goal is to reduce the number and criticality of technical, human and organizational vulnerabilities. We provide information about:

- Threat and vulnerability alerts, either detected by the CSIRT or informed by third parties to us.
- Alerts of relevant incidents.
- Vulnerabilities in products from main providers.
- Weekly cybersecurity awareness campaigns for the public.
- Threat reports.
- Research on new cyberthreat trends.

4.2. Cooperation, engagement and the sharing of information.

The information received, collected and managed by the Chilean Government CSIRT is confidential, and it is neither published nor shared with anyone, as defined by its Privacy and Confidentiality Policy, published on our website.

4.3. Communication

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

- Incident information: incidents@interior.gob.cl
- Other requests: csirt-comunicaciones@interior.gob.cl
- Legal: csirt-legal@interior.gob.cl

5. Services

- Website vulnerability scanner.
- Auditing.
- Pentesting.
- Website availability monitoring.
- Malicious artifact analysis and forensic analysis.
- Incident and vulnerabilities alerts.
- Cyberawareness and best practices campaigns.
- Cyberawareness training for public employees.
- Sharing of Indicators of Compromise.
- Intrusion detection and prevention.
- Anti-DDoS proteciton.
- Web Application Firewall (WAF) protection.
- Preemptive threat blocking.
- DNS Revolver.

- ".gob.cl" domain names creation.

6. Incident notification alternatives:

Incidents may be notified through:

- Our website: www.csirt.gob.cl. There is a web form to report incidents online.
- Our email to report incidents: incidentes@interior.gob.cl and incidents@interior.gob.cl.
- Our short phone number, available anywhere within the country: 1510

7. Disclaimer:

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

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.01.22 11:30:48 -03'00'