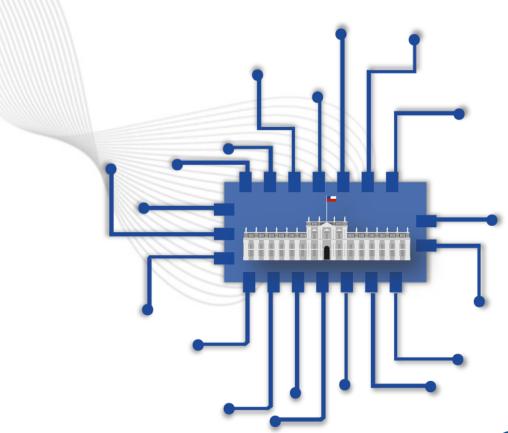


National Cybersecurity Policy

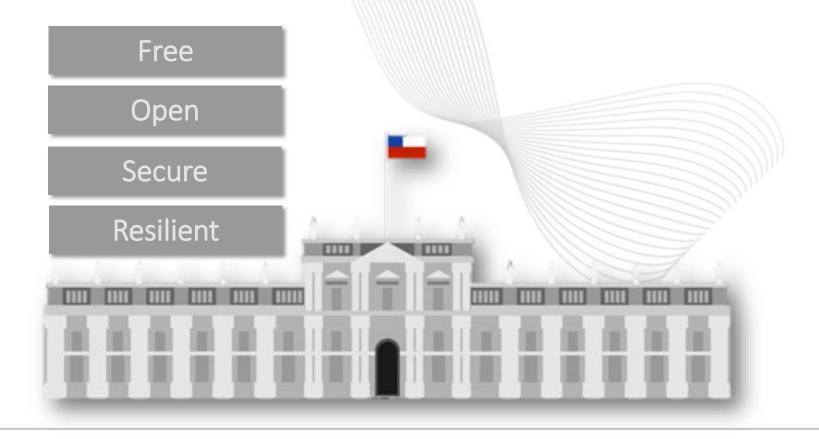






Cybersecurity Policy: State compromise









A Robust and Resilient Infrastructure

Safeguard the Rights of People in Cyberspace

В

C Awareness: education, good practices and responsibility

Cooperation and participation in International Cybersecurity Forums

Industry Development in Cybersecurity





A Robust and Resilient Infrastructure

В

C

D

F

Cybersecurity Law

Update Decree 83

Cybersecurity in public tender

CII Standards

Software Standards

Cyber Incident Platform

SER Cyber request

CII minial risk

Incident Report Matrix

Cyber on Emergency Systes

Exhange info standards

Resilient telecom

Dcto 5996 and DS 1299 (+C)



Key Issues Safeguard the Rights of В People in Cyberspace Cybercrime Law Cybercrime Report Matrix Strengthen Forensic Analysis Personal Data Law (+ A) Join the Europe Cybercrime Convention (+ D)





Information Dissemination Point on Citizen Cybersecurity Cybersecurity Month Awareness campaign B Good Practice Guides Intersectoral Table Cybersecurity Training Awareness: education, good practices and responsibility Senior Citizens Campaign D Awarnesess Campaign with **Education Ministry** Multisectoral Collaboration (NGO, Emp., Uni.) (+ A and B) Cybersecurity Drills (+ A) National Surveys (+ B) Training Public Officials



División de Redes y Seguridad Informática.

Support multilateral and regional consultations

Bilateral mechanisms, agendas and consultations

International Cyberspace and Security Policy

Interagency Working Group cyberspace issues

Exchange experiences to implement and evaluate strategies and policies

Cooperation and participation in Internationa Cybersecurity Forum A

В

C

E





Analyze public sector procurement regime

Cybersecurity Industry Characterization Study

Study Tax Incentives Adoption Standards

Incorporate Standards in Suppliers (+ A)

State sponsorship of projects (+C)

Promote Human Capital Development (+ C)

Export Cyber Products and Services (+ D)

Industry Development in Cybersecurity

В

D



Milestones 2018 Lazarus Group, sponsored by North Korea, attacks the chilean bank system. That encourages the creation of the CSIRT. 2019 (March) A major Emotet attack was the first threat successfully coordinated by CSIRT together with the economic sector 2019 (October) After the social outbreak, hacktivist actions against the Government are incited 2020, Challenges in times of pandemic and elections

Threats and Risks





State Groups

Malware



Cybercriminals

- Phishing
- Malware
- Ransomware



Hacktivists

- DDoS
- Defacement
- Data Leak



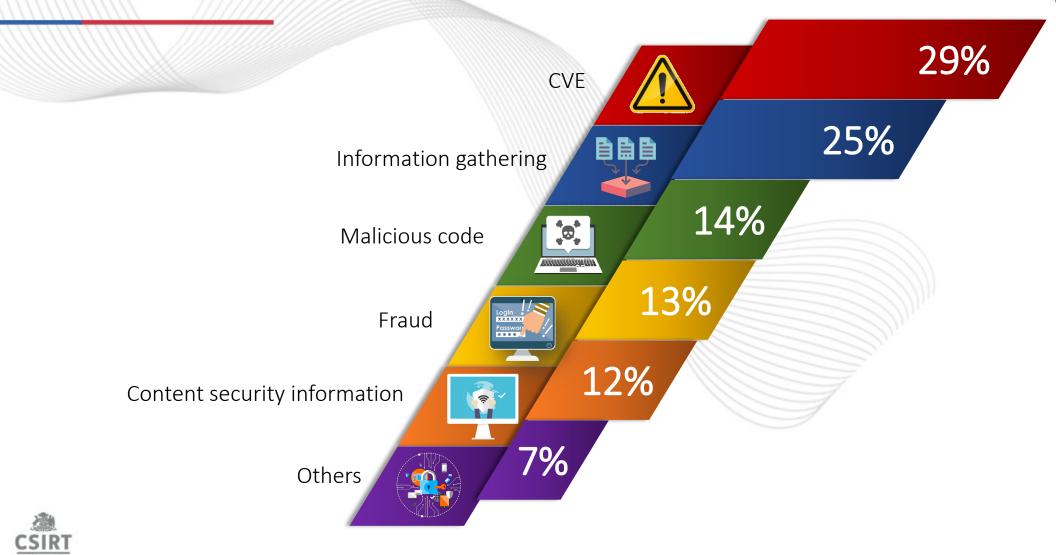
Vulnerabilities

- Home network Security
- Use of personal computers
- Connection hikes



Main threats





^{*}Estadística en base a los tickets del CSIRT, excluyendo aquellos generados en gestión interna de CSIRT

Strategy







Objectives of the CSIRT of Chile



Prevent, manage and respond to information security incidents

Provide information and assistance to State Institutions

Advice on risk analysis

Vulnerability Management



Coordinate and support responses to events or incidents.



Provide information and assistance to the RCE and government cyberspace.



Promote good practices within the State administration



Execute Presidential Instruction No. 8 to improve internal standards.



Legal Frame









¡Thanks!



