TLP: WHITE

RFC 2350 – CSIRT Public Profile

INSSIDE
INFORMACION INTELIGENTE

1. Team Information

- **Team Name:** CSIRT INSSIDE
- **Location:** Buenos Aires, Argentina

2. Point of Contact

- **Postal address:**
  INSSIDE Cybersecurity
  Carlos Pellegrini 719, C1189 Cdad. Autónoma de Buenos Aires, Argentina
- **Phone:** +54 11 52738800
- **Email:** csirt@insside.net
- **Website:** https://www.insside.net/
- **Opening hours:** Monday to Friday from 9:00 a.m. to 6:00 p.m. (GMT-3)

3. Mission Statement

INSSIDE's CSIRT has the mission of managing and responding effectively to security incidents that affect the organization's technological assets, protecting the confidentiality, integrity and availability of information, and collaborating with other national and international entities in the field of cybersecurity.

4. Authority

4.1 Authority Source

The authority of the CSIRT derives from:

- Executive mandate granted by the CEO.
- Organizations' current policies.

4.2 Nature of the Authority

Depending on the type of stakeholder and the context, the CSIRT exercises different types of authority:

- **Advisory Authority:**
  The CSIRT may issue non-binding recommendations and guidelines to its community of interest in relation to risk mitigation, threat intelligence, and prevention best practices.

- **Operational Authority:**
  The CSIRT is authorized to:
  - Access relevant security event logs and data during incident investigation.
  - Coordinate response actions with IT managers or system owners (e.g., containment, eradication).
  - Notify users of vulnerabilities and request mitigation actions.
- **Executive Authority (if applicable):**
  In urgent or critical cases, the CSIRT may:
  - Apply emergency containment actions (e.g., isolation of network segments, forced password reset).
  - Temporarily suspend access to compromised systems or accounts.
  - Require users to report high-severity incidents.

4.3 Escalation Procedures

The CSIRT follows an escalation scheme based on severity levels:

- **Incidents of low or moderate severity:**
  They are managed directly by the CSIRT in coordination with the responsible IT units.
- **High or critical severity incidents:**
  These are escalated to the crisis committee or to the person/department designated by the client or the organization.
- **Crisis situations:**
  They activate the organization's Crisis Management or Business Continuity plans.

4.4 Limitations of Authority

The CSIRT:

- It has no authority over third-party systems, unless there are formal agreements in place.
- It cannot apply disciplinary measures; these cases are referred to Human Resources or the Legal area.
- It will not act outside the limits defined by legal or contractual obligations.

5. Policies

- **Confidentiality:** All information shared with the CSIRT will be handled confidentially.
- **TLP (Traffic Light Protocol):** TLP is used to classify and handle information.
- **Disclosure of information:** Information will be shared only with authorized third parties and with the explicit consent of the sender, unless legally obliged.
- **Collaboration:** Cooperation with other CSIRTs, CERTs, governmental, sectoral and private bodies is encouraged.

6. Services Provided

Category	Service	Purpose
Information Security Incident Management	Receiving information security incident reports	Receive and process reports of potential security incidents from users, security event management services, or third parties.
	Information Security Incident Analysis	Analyze and understand a confirmed security incident.
	Analysis of forensic evidence and artifacts	Analyze and understand artifacts related to a confirmed security incident, considering the need to preserve forensic evidence.
	Mitigation and recovery	Contain the security incident as much as possible to limit the number of casualties, reduce losses, recover from damage, prevent further attacks, and remediate exploited vulnerabilities.
	Information Security Incident Coordination	Ensure timely notifications and accurate distribution of information; maintain the flow of

		information and the monitoring of activities of the entities involved in the response; guarantee the execution of the plan.
	Crisis management support	Provide expertise and contacts with other security experts, CSIRTs, and CSIRT communities to help mitigate a crisis situation.
Vulnerability Management	Vulnerability Discovery/Research	Finding, learning about, or researching new (previously unknown) vulnerabilities; they can be discovered by the vulnerability management area or through other CSIRT activities.
	Receiving vulnerability reports	Receive and process information about vulnerabilities reported by users or third parties.
	Vulnerability analysis	Analyze and understand a confirmed vulnerability.
	Vulnerability Disclosure	Disseminate information about known vulnerabilities to users so that they can prevent, detect, and mitigate/remediate such vulnerabilities.
	Vulnerability Response	Act on information of known vulnerabilities to prevent, detect and mitigate/remediate their impact.
Situational Awareness	Data acquisition	Collect data that helps improve visibility into internal or external activities that may affect the organization's security posture.
	Analysis and synthesis	Assess when the situation is not in line with expectations (for example, when certain assets may

		be about to experience a damaging event).
	Communication	Notify users or other entities in the security community about changes in the environment's risks.
Knowledge Transfer	Raising awareness	Improve users' overall security posture and help them detect, prevent, and recover from incidents; ensure that they are better prepared and educated.
	Training and education	Provide training and training to users and CSIRT staff on cybersecurity, information assurance and incident management issues.
	Exercises	Conduct exercises to evaluate and improve the effectiveness and efficiency of cybersecurity services and functions.
	Technical and regulatory advice	Ensure that user policies and procedures include appropriate considerations on incident management, enabling them to better manage risks, and strengthening the CSIRT.

7. How to Report an Incident

- **Email:** csirt@insside.net
- **Suggested subject:** [INCIDENT] Brief description
- **Suggested format:**
  - Date and time of detection
  - Event Description

  - IPs and domains involved
  - Relevant logs (if applicable)
  - Contact Person
- **Encryption (Optional):** The use of PGP is recommended to send sensitive information (see Section 9).

8. Disclaimer

The INSSIDE CSIRT takes all precautions when preparing notifications and reports and does not assume any responsibility for the misuse of the information contained in this form.

10. Public Keys and Information Encryption

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: User ID: CSIRT Insside <csirt@INSSIDE.NET>

mDMEaDBqDhYJKwYBBAHaRw8BAQdAz9oaGevAYgTf9d1R/b6vdBVlHchT3LAz5mjg
5KwUvyS0IUNTSVJUIEluc3NpZGUgPGNzaXJ0QElOU1NJREUuTkVUPoiZBBMWCgBB
FiEEQsqCJ7tUCd0NMqln+waN6yBd+yMFAmgwag4CGwMFCQWlD2IFCwkIBwICIgIG
FQoJCAsCBBYCAwECHgcCF4AACgkQ+waN6yBd+yPtrQEAh0JXY0sEZ/Mz0dw/cFFa
ibxIF0Vr3medZcyit8KSgPUBAMPFCiAlb90nsgoYpPCIQVw2w8v8/MbRqwtw0AEG
e/8NuDgEaDBqDhIKKwYBBAGXVQEFAQEHQKcQG6NR6mFIIDUlaafKdWoQXwsEaEAW
Gc6qtRot/aZsAwEIB4h+BBgWCgAmFiEEQsqCJ7tUCd0NMqln+waN6yBd+yMFAmgw
ag4CGwwFCQWlD2IACgkQ+waN6yBd+yP0ogEAly4/hFrCyVv6laD5sz62ViT9P+gW
6p7LzKfKwoP0p1AA/1chIu910cpogNKAjp/Jtp90fUdm/IU/8du5nqB4BAUG
=Gbyq
-----END PGP PUBLIC KEY BLOCK-----
```