LNCC.BR RFC 2350

1. Document Information

This document contains a description of ETIR LNCC.br according to **RFC 2350**.

1.1 Date of Last Update

This is version 1.0, published 2024/08/26.

1.2 Distribution List for Notifications

There is no distribution list for notifications of new versions of this document.

1.3 Locations Where This Document May Be Found

The current version of this document can be found at

https://www.gov.br/lncc/pt-br/acesso-a-informacao/institucional/politica-de-seguranca-1/etir_lncc-rfc2350-eng.pdf

The key used for signing is the ETIR LNCC.BR key as listed under 2.8.

2. Contact Information

2.1 Name of the Team

In English: ETIR LNCC – Cyber Incident Treatment and Response Team.
In Brazilian Portuguese: ETIR LNCC – Equipe de Tratamento e Respostas a Incidentes Cibernéticos.

2.2 Address

ETIR LNCC

Rua Getúlio Vargas, 333 – Quitandinha, Petrópolis – RJ

CEP 25651-075

2.3 Time Zone

America/Sao_Paulo (GMT-0300).

2.4 Telephone Number

Not applicable. ETIR LNCC does not accept incident reports via telephone.

2.5 Facsimile Number

None available.

2.6 Other Telecommunication

Not applicable.

2.7 Electronic Mail Address

Incident reports should be sent to <etir@lncc.br>.

2.8 Public Keys and Other Encryption Information

The ETIR LNCC has a PGP key, whose KeyID is 8C1AD5D5B21AE1CE and whose fingerprint is 27E6 4F2D 9303 25F1 0A50 32C9 8C1A D5D5 B21A E1CE

and can be found at

https://www.gov.br/lncc/pt-br/acesso-a-informacao/institucional/politica-de-seguranca-1/chave-pgp-lncc.pdf

2.9 Team Members

No public information is provided about ETIR LNCC members.

2.10 Other Information

For additional information about how to contact ETIR LNCC, see:

https://www.gov.br/lncc/pt-br/acesso-a-informacao/institucional/politica-de-seguranca-1/equipe-de-prevencao-tratamento-e-resposta-a-incidentes-ciberneticos-etir

Links to alerts and recommendations can be found at:

https://www.gov.br/lncc/pt-br/centrais-de-conteudo/campanhas-de-conscientizacao/gestao-de-seguranca-da-informacao

2.11 Points of Customer Contact

The preferred method for contacting the ETIR LNCC for administrative matters is via email at etir@lncc.br.

ETIR LNCC operates from Monday through Friday, from 08:00 to 17:00, GMT-0300.

3. Charter

3.1 Mission Statement
Cyber Incident Prevention, Handling and Response Center of LNCC Institute.

3.2 Constituency

ETIR LNCC answers for computer security incidents related to the academic community of LNCC. This covers the domain lncc.br and the following IP ranges:

IPV4 Block 146.134.0.0/16 and AS262534.

3.3 Sponsorship and/or Affiliation

ETIR LNCC was formally created on February 23, 2021, through Ordinance Number 116/202/SEI-LNCC, by the Director of LNCC.

3.4 Authority

ETIR LNCC has the authority to act on all incidents that cause, or could cause, detriment to the confidentiality, integrity and availability of LNCC ICT(Information and communications technology) and information assets.

4. Policies

4.1 Types of incidents and level of support
ETIR LNCC works closely with CTIR GOV, CERT.BR, CAIS-RNP and all security agency belonging to the Brazilian Federal Public Administration.

4.2 Co-operation, interaction and disclosure of information

ETIR LNCC treats all information as confidential by default, but will use the information shared to help solve security incidents. Information might be distributed forward to other teams/organizations on a need-to-know basis. Information will be anonymized whenever it is feasible. ETIR LNCC adheres to the Information Sharing Traffic Light Protocol according to the

FIRST Standard Definitions and Usage Guidance: **https://www.first.org/tlp/docs/tlp-a4.pdf**. Information that is labelled with the tags WHITE, GREEN, AMBER, AMBER+STRICT or RED will be handled appropriately.

4.3 Communication and authentication

For normal communication not containing sensitive information ETIR LNCC uses conventional methods like unencrypted e-mail. Please refer to sections 2.7. For sensitive information, the use of PGP encryption is strongly encouraged (see section 2.8).

5. Services

5.1 Incident response

ETIR LNCC gives assistance to everyone during a security incident response, from systems administrators to end users. ETIR LNCC collaborates on all stages of the response, from initial triage, to coordination between different entities when relevant, while actively seeking to participate in the resolution. We focus on our academic community, that is, incidents whose origin or destiny is LNCC.

5.1.1 Incident triage

ETIR LNCC will help validate, assess, correlate, and prioritize the incident.

5.1.2 Incident coordination

ETIR LNCC handles computer security incidents in the context of the academic community and organizations, that is, incidents where LNCC is the origin or target of the attacks.

5.1.3 Incident resolution

Analysis of compromised systems;

Elimination of the cause of a security incident and its effects;

Aid in restoring affected systems and services to their status before the security incident;

Respond cybersecurity incidents;

5.2 Proactive activities

ETIR LNCC promotes prevention actions which aim to help our constituency to prevent as well as better handle computer security incidents. In that context, the following initiatives are executed:

- Validation and notification of vulnerabilities;
- Publication of relevant knowledge as Alerts, Recommendations and Awareness campaigns for users.

6. Incident reporting forms

There are no forms available. Please refer to section 2.7.

7. Disclaimers

While every precaution is taken in the preparation of information and notifications, ETIR LNCC assumes no responsibility for errors or omissions, or for damages resulting from the use of the information provided.