

LNCC.BR RFC 2350

## 1. Informações do Documento

Este documento contém uma descrição da ETIR LNCC de acordo com a RFC 2350.

### 1.1 Data da última atualização

Versão 1.0, publicada em 26/08/2024.

### 1.2 Lista de distribuição para notificações

Não há lista de distribuição para notificações de novas versões deste documento.

### 1.3 Locais onde este documento pode ser encontrado

A versão atual deste documento pode ser encontrada em:

[https://www.gov.br/lbcc/pt-br/acesso-a-informacao/institucional/politica-de-seguranca-1/etir\\_lbcc-rfc2350\\_port.pdf](https://www.gov.br/lbcc/pt-br/acesso-a-informacao/institucional/politica-de-seguranca-1/etir_lbcc-rfc2350_port.pdf)

A chave usada para assinar é a chave ETIR LNCC.BR listada em 2.8.

## 2. Informações de contato

### 2.1 Nome da Equipe

ETIR LNCC - Equipe de Tratamento e Respostas a Incidentes Cibernéticos.

### 2.2 Endereço

ETIR LNCC

Rua Getúlio Vargas, 333 – Quitandinha, Petrópolis – RJ

CEP 25651-075

### 2.3 Fuso Horário

America/Sao\_Paulo (GMT-0300).

### 2.4 Número de Telefone

Não se aplica. ETIR LNCC não aceita relatos de incidentes por telefone.

### 2.5 Número de Fax

Não se aplica.

## 2.6 Outras Telecomunicações

Não se aplica

## 2.7 Correio Eletrônico

As notificações sobre incidentes cibernéticos devem ser enviadas para <etir@lncc.br>.

## 2.8 Chaves públicas e outras informações de criptografia

Chave PGP ETIR LNCC

PGP Key ID: 8C1AD5D5B21AE1CE

Fingerprint: 27E6 4F2D 9303 25F1 0A50 32C9 8C1A D5D5 B21A E1CE

e pode ser encontrada em:

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

## 2.9 Membros da Equipe

Nenhuma informação pública é fornecida sobre os membros do ETIR LNCC.

## 2.10 Outras Informações

Para informações adicionais sobre como entrar em contato com o ETIR LNCC, consulte:

<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 para Campanhas de Conscientização, podem ser encontrados em:

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

## 2.11 Principal ponto de contato

O principal meio de contato, para assuntos administrativos, com o ETIR LNCC é através do e-mail <etir@lncc.br>.

ETIR LNCC funciona de segunda a sexta-feira, das 08:00 às 17:00, GMT-0300.

### 3. Apresentação

#### 3.1 Declaração da Missão

Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Instituto LNCC.

#### 3.2 Abrangência Operacional (Público-alvo)

ETIR responde por incidentes de segurança de informática relacionados à comunidade acadêmica do LNCC. Isso abrange o domínio Incc.br e as seguintes faixas de IP:

Bloco IPV4 146.134.0.0/16 e AS262534.

#### 3.3 Sponsorship and/or Affiliation

ETIR LNCC foi criado em 23 de fevereiro de 2021, através da Portaria 116/202/SEI-LNCC, pelo Diretor do LNCC.

#### 3.4 Autoridade

ETIR LNCC tem autoridade para agir em todos os incidentes que causem, ou possam causar, prejuízo à confidencialidade, integridade e disponibilidade das TIC e dos ativos de informação do LNCC.

### 4. Políticas

#### 4.1 Types of incidents and level of support

ETIR LNCC atua em estreita colaboração com CTIR GOV, CERT.BR, CAIS-RNP e todos os órgãos de segurança pertencentes à Administração Pública Federal Brasileira.

#### 4.2 Cooperação, interação e divulgação de informações

ETIR LNCC O LNCC trata todas as informações como confidenciais por padrão, mas utilizará as informações compartilhadas para ajudar a resolver incidentes de segurança. As informações podem ser distribuídas para outras equipes/organizações conforme a necessidade. As informações serão anonimizadas sempre que possível. O ETIR LNCC adere ao padrão TLP de acordo com as Definições e Orientações do FIRST:

<https://www.first.org/tlp/docs/v2/tlp-pt-br.pdf>.

As informações marcadas com as tags WHITE, GREEN, AMBER, AMBER+STRICT ou RED serão tratadas adequadamente, conforme definido no padrão.

### 4.3 Comunicação e Autenticação

Para comunicação normal que não contenham informações confidenciais, o ETIR LNCC utiliza métodos convencionais como e-mail não criptografado. Consulte as seções 2.7. Para informações confidenciais, o uso de criptografia PGP é fortemente encorajado (ver seção 2.8).

## 5. Serviços

### 5.1 Resposta a Incidentes

O ETIR LNCC presta assistência a todos durante a resposta a incidentes de segurança, desde administradores de sistemas até usuários finais. O ETIR LNCC colabora em todas as fases do tratamento, desde a triagem inicial, até à coordenação entre diferentes entidades quando relevante, procurando ativamente participar na resolução. Focamos na nossa comunidade acadêmica, ou seja, nos incidentes cuja origem ou destino é o LNCC.

#### 5.1.1 Triagem de incidentes

O ETIR LNCC ajudará a validar, avaliar, correlacionar e priorizar o incidente.

#### 5.1.2 Coordenação de incidentes

O ETIR LNCC trata incidentes de segurança de informática no contexto da comunidade acadêmica e das organizações, ou seja, incidentes onde o LNCC é origem ou alvo dos ataques.

#### 5.1.3 Resolução de incidentes

Análise de sistemas comprometidos;

Eliminação da causa de um incidente de segurança e dos seus efeitos;

Ajuda na restauração dos sistemas e serviços afetados ao seu estado anterior ao incidente de segurança;

Responder a incidentes de segurança cibernética;

## 5.2 Atividades Pró-Ativas

O ETIR LNCC promove ações de prevenção que visam ajudar o nosso público alvo a prevenir e a melhor lidar com incidentes cibernéticos. Nesse contexto, são executadas as seguintes iniciativas:

- Validação e notificação de vulnerabilidades;
- Publicação de conhecimentos relevantes como Alertas, Recomendações e Campanhas de Sensibilização para os nossos colaboradores(usuários).

## 6. Formulários para notificações de incidentes

Não há formulários disponíveis. Consulte a seção 2.7.

## 7. Isenções de Responsabilidade

Embora sejam tomadas todas as precauções na preparação das informações e notificações, o ETIR LNCC não assume qualquer responsabilidade por erros ou omissões, ou por danos decorrentes das informações fornecidas.