Laboratório Nacional de Computação Científica
UNIDADE DE PESQUISA DO MCTI

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES

PÁTRIA AMADA BRASIL GOVERNO FEDERAL

# Sistema de Gestão de Segurança da Informação

# Procedimento notificação de não conformidade

| | |
|---|---|
| **Controle Interno** | 29-PNNC |
| **Classificação** | Nível de Acesso: ( **X** ) Público () Restrito ( ) Sigiloso<br>Tipo de Acesso: ( ) Interno ( **X** ) Externo |
| **Grupo Responsável** | Gestor de Segurança da Informação |
| **Autor(es)** | Luís Rodrigo de Oliveira Gonçalves |
| **Versão** | 2.0 |
| **Data do Documento** | 19 de agosto de 2021 |
| **Número de Páginas** | 4 |
| **Controles da ISO** | 6.1 – Ações para contemplar riscos e oportunidades |

**Diretor**
Fábio Borges de Oliveira

**Coordenação de Tecnologia da Informação e Comunicação – COTIC**
Wagner Vieira Léo

**Setor de Governança de Tecnologia da Informação - SESTI**
Rogério Albuquerque de Almeida

**Gestão de Segurança da Informação - GSI**
Luís Rodrigo de O. Gonçalves

## Histórico das Versões

| Versão | Data | Descrição | Revisor(es) |
|---|---|---|---|
| 1.0 | 27/05/2020 | Documento Inicial. | Luís Rodrigo de O. Gonçalves |
| 2.0 | 19/08/2021 | Atualização da estrutura e revisão do conteúdo | Luís Rodrigo de O. Gonçalves |

## Sumário



## 1. Apresentação

Este documento define o procedimento a ser adotado pelos colaboradores e demais partes interessadas de forma que possam reportar possíveis: (i) não conformidades do ambiente em relação ao Sistema de Gestão de Segurança da Informação (SGSI), (ii) riscos à segurança da informação, (iii) oportunidades de melhorias para a segurança da informação e (iv) outras ações que possam contribuir com a melhoria contínua do SGSI.

No contexto deste procedimento, de forma geral, devemos entender risco como sendo a possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos do Laboratório Nacional de Computação Científica. Aplicando o conceito de risco à segurança da informação ele deve sem entendido como sendo o potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

Como exemplo de um risco podemos imaginar um cenário onde temos um desktop, ou um laptop, que não possui uma ferramenta de controle de malware. Este equipamento está vulnerável ao ataque de vários malwares que podem ser “acionados” acidentalmente por um

dos seus usuários. Neste caso temos o “risco” de um “ataque de um ransonware” que pode comprometer a disponibilidade dos dados contidos no equipamento ou na rede da instituição;

## 1.1 Escopo

O procedimento descrito neste documento aplica-se ao ambiente do Supercomputador Santos Dumont e aos ativos da informação, localizados no CPD e gerenciados pela equipe de suporte do LNCC.

## 1.2 Distribuição e público-alvo

Este documento é de distribuição pública e destina-se a todos os colaboradores do LNCC e as partes interessadas no escopo descrito na seção 1.1 - Escopo.

## 1.3 Documentação relacionada

Estão relacionadas a este procedimento as seguintes documentações:

- Política de Segurança da Informação do LNCC.
- Glossário de Segurança da Informação, definido na portaria No 93, de 26 de setembro de 2019 do Gabinete de Segurança Institucional da Presidência da República, disponível em https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de- setembro-de-2019-219115663. Este documento contém a padronização de parte dos termos utilizados no SGSI do LNCC no escopo definido anteriormente.

## 1.4 Manutenção do documento

Este documento deve ser revisado ao menos uma vez ao ano.

# 2. Realizando uma notificação

Os colaboradores ou as partes interessadas que identificarem ou suspeitarem de possíveis: (i) não conformidades do Sistema de Gestão de Segurança da Informação (SGSI) em relação à ISO/IEC 27001 e outras normativas , (ii) riscos à segurança da informação, (iii) oportunidades de melhorias para a segurança da informação e (iv) outras ações que possam contribuir com a melhoria contínua do SGSI; devem realizar a comunicação da mesma utilizando-se o endereço de e-mail do Sistema de Gestão de Segurança da Informação (sgsi@lncc.br)

Os colaboradores ou as partes interessadas não devem realizar qualquer tipo de teste para confirmar uma não conformidade ou um risco. Apenas as equipes devidamente autorizadas podem realizar análises e correções no ambiente descrito na Seção 1.1 - Escopo.

# 3. Recebendo e tratando a notificação

Ao receber as notificações encaminhadas ao e-mail do Sistema de Gestão de Segurança da Informação (sgsi@lncc.br), cabe ao gestor encaminhá-las aos responsáveis.

As notificações de riscos de segurança da informação devem ser encaminhadas ao agente responsável pela gestão de riscos de segurança da informação. Cabe ao agente responsável pela gestão de riscos providenciar a análise, avaliação e registro do risco. Os riscos serão gerenciados conforme descrito no CAPÍTULO III (Gestão de Riscos de Segurança da

Informação) da Instrução Normativa GSI/PR Nº 31, de 28 de maio de 2021.

As notificações de não conformidade serão analisadas pelo gestor de segurança, quando confirmadas serão tratadas conforme plano de ação a ser elaborado em conjunto com a equipe responsável pela não conformidade e aprovado pela direção.

As notificações de oportunidades de melhoria para a segurança da informação e outras ações que possam contribuir com a melhoria contínua do SGSI, serão encaminhadas ao Comitê de Segurança da Informação e serão discutidas em uma das reuniões do mesmo comitê.

## 4. Glossário

| | | |
|---|---|---|
| **LNCC** | : | Laboratório Nacional de Computação Científica |
| **SGSI** | : | Sistema de Gestão de Segurança da Informação |
| **RISCO** (conceito geral) | : | possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos, sendo mensurado em termos de impacto e de probabilidade; |
| **Risco de Segurança da Informação** | : | potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização; |

Fábio Borges de Oliveira
Diretor do LNCC

Luís Rodrigo de O. Gonçalves
Gestor de Segurança da Informação

[1] **IN03/DSIC/GSI/PR** - https://www.in.gov.br/en/web/dou/-/instrucao-normativa-gsi/pr-n-3-de-28-de-maio-de-2021-322963172