SUMÁRIO

1 Objetivo

Este documento define o procedimento que deve ser seguido pelos colaboradores do LNCC e demais partes interessadas ao reportarem possíveis: (i) não conformidades em relação ao Sistema de Gestão de Segurança da Informação (SGSI), (ii) riscos à segurança da informação e (iii) oportunidades de melhorias para a segurança da informação.

2 Campo de aplicação

Esta norma se aplica a todas as unidades organizacionais do LNCC que atuam nos processos que fazem parte do escopo certificado em conformidade à ABNT NBR ISO/IEC 27001. Este documento é de distribuição pública e destina-se a todos os colaboradores do LNCC e as partes interessadas.

3 Responsabilidade

3.1 O Gestor de Segurança da Informação é o responsável por elaborar, manter atualizado e aprovar o procedimento de notificação de não conformidades.

3.2 O SECIN é o responsável por realizar a divulgação do procedimento para os colaboradores e demais partes interessadas.

3.3 Os colaboradores e demais partes interessadas são responsáveis por realizar a notificação de não conformidade, riscos e oportunidades de melhorias, quando de sua identificação.

4 Documentos de referência

Os documentos a seguir, no todo ou em parte, são referenciados neste documento e fornecem requisitos, diretrizes ou orientações que são indispensáveis à sua aplicação. Para referências datadas, aplicam-se somente as edições citadas. Para referências não datadas, aplicam-se as edições mais recentes do documento, incluindo emendas.

ISO/IEC 27000:2018	Information technology — Security techniques — Information security management systems — Overview and vocabulary
ABNT NBR ISO/IEC 27001:2022	Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos
ABNT NBR ISO/IEC 27002:2022	Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Aprova o Glossário de Segurança da Informação (https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370)
Portaria MCTI nº 6572, de 22 de novembro de 202	Regimento Interno do Laboratório Nacional de Computação Científica (https://www.gov.br/lncc/pt-br/acesso-a-informacao/institucional/regimento-interno)
Política de Segurança da Informação do LNCC	Institui a Política de Segurança da Informação (PSI), no âmbito do Laboratório Nacional de Computação Científica (LNCC), com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação (https://www.gov.br/lncc/pt-br/acesso-a-informacao/institucional/politica-de-seguranca-1/politicas-de-seguranca-da-informacao/politicas-de-seguranca-da-informacao-psi)
Política de Segurança da Informação do Supercomputador Santos Dumont	Declaração formal do Laboratório Nacional de Computação Científica (LNCC) a respeito do seu compromisso com a proteção dos ativos de informação de sua propriedade e sua guarda no que tange ao Supercomputador Santos Dumont. (https://www.gov.br/lncc/pt-br/acesso-a-informacao/institucional/politica-de-seguranca-1/politicas-de-seguranca-da-informacao/politica-de-seguranca-da-informacao-do-lncc-santos-dumont)

5 Documentos complementares

Os documentos a seguir serão utilizados, no todo ou em parte, para viabilizar a aplicação das informações documentadas do

SGSI, devendo estar citados no corpo do texto normativo e disponíveis para uso.

37-MAR	Metodologia da Avaliação de Riscos

6 Siglas

SGSI Sistema de Gestão de Segurança da Informação

Nota: As siglas das UO do LNCC podem ser acessadas no Regimento Interno do Laboratório Nacional de Computação Científica (https://www.in.gov.br/en/web/dou/-/portaria-mcti-n-7.061-de-24-de-maio-de-2023-485541159).

7 Termos e definições

Risco	No sentido amplo, trata-se da possibilidade de ocorrência de um evento que pode impactar o cumprimento dos objetivos. Pode ser mensurado em termos de impacto e de probabilidade.
Risco de segurança da informação	Risco potencial associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização.
Incidente de segurança	Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

Para os efeitos deste documento, aplicam-se os termos e definições a seguir, baseados nas normas de referência, Portaria GSI/PR nº 93/2021 e ISO/IEC 27000:2018, que devem ser interpretados somando-se as descrições. Em caso de divergência, prevalecem o termo e a definição estabelecidos na Portaria GSI/PR nº 93/2021.

8 Realizando uma notificação de não conformidade

8.1 A notificação de não conformidade deve ser feita por meio do envio de e-mail ao Sistema de Gestão de Segurança da Informação, sgsi@lncc.br, por todos os colaboradores ou partes interessadas do SGSI, que identificarem ou suspeitarem de possíveis:

a) não conformidades do Sistema de Gestão de Segurança da Informação (SGSI) em relação à ISO/IEC 27001 e outras normativas;

b) riscos à segurança da informação;

c) oportunidades de melhoria para a segurança da informação; ou

d) outras ações que possam contribuir com a melhoria contínua do SGSI.

8.1.1 Sempre que possível, a notificação deve conter uma descrição clara do evento observado, bem como informações sobre o impacto potencial à segurança da informação e uma estimativa da probabilidade de ocorrência. Tais informações contribuem para a priorização e o tratamento adequado do evento reportado.

8.2 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.

8.3 Vulnerabilidades técnicas

8.3.1 Vulnerabilidades técnicas devem ser encaminhadas como notificação de não conformidade da mesma forma definida no item 8.1.

8.3.2 O Gestor de Segurança da Informação deve avaliar a vulnerabilidade técnica e, de acordo com o caso concreto, registrar, se pertinente, a não conformidade.

8.3.2.1 Quando necessário, o Gestor de Segurança da Informação deve envolver o proprietário do ativo e as partes interessadas.

9 Recebendo e tratando a notificação

9.1 Ao receber as notificações encaminhadas ao e-mail do Sistema de Gestão de Segurança da Informação (sgsi@lncc.br), o Gestor do SGSI deve avaliá-las, identificando e notificando o proprietário do ativo, para análise e resposta quanto ao conteúdo da notificação.

9.2 O Gestor de Segurança deve encaminhar as notificações de riscos ao agente responsável pela gestão de riscos de segurança da informação. O agente responsável pela gestão de riscos deve providenciar a análise, avaliação e registro do risco. Após essa etapa, será definido o plano de tratamento, incluindo a seleção de controles apropriados, com base no Anexo A da ISO/IEC 27001:2022, a aprovação do plano pelo proprietário do risco e sua implementação.

9.3 Os riscos, devem ser gerenciados conforme descrito no documento 37-MAR, observado o definido no CAPÍTULO III (Gestão de Riscos de Segurança da Informação) da Instrução Normativa GSI/PR Nº 3, de 28 de maio de 2021.

9.4 Quando confirmada uma não conformidade, o proprietário do ativo deve providenciar a identificação da causa raiz e a elaboração do planejamento das tratativas ser acompanhado pelo Gestor de Segurança da Informação, que deverá também

avaliar a eficácia das ações implementadas, garantindo que os objetivos de mitigação foram alcançados. Os resultados dessa avaliação devem ser registrados.

9.5 O Gestor de Segurança da Informação deve utilizar as reuniões do Comitê de Segurança da Informação para realizar a apresentação das notificações de oportunidades de melhoria para a segurança da informação e outras ações que possam contribuir com a melhoria contínua do SGSI.

9.5.1 Com o apoio do Comitê, o gestor de segurança, deve avaliar a viabilidade, os impactos e os benefícios esperados dessas ações, com base em critérios definidos, e acompanhar sua implementação quando aprovadas, com registro de sua eficácia.

9.6 Todas as notificações recebidas, análises realizadas, avaliações de riscos, planos de ação, decisões sobre tratamento e resultados da verificação de eficácia devem ser registrados e mantidos como informação documentada, em conformidade com os requisitos do SGSI.

10 Análise crítica

Este documento deve ser analisado criticamente, quanto à sua eficácia e adequação ao SGSI do LNCC, sempre que necessário, ao menos, uma vez ao ano.

11 Histórico da revisão e Quadro de aprovação

Revisão	Data	Itens Revisados
1.0	27/05/2020	Versão Original
2.0	19/08/2021	Atualização da estrutura e revisão do conteúdo
3.0	03/05/2023	Adequação a novo padrão de formatação; adequação das logomarcas utilizadas; atualização da estrutura e revisão do conteúdo
4.0	11/06/2024	Análise crítica do documento, revisão e atualização das normativas. Remoção da seção “Política de Transição”.
5.0	04/08/2025	Adequação do documento à versão de 2022 da norma ABNT NBR ISO/IEC 27001

Quadro de Aprovação		
	Nome	**Atribuição**
Elaborado por	Luís Rodrigo de O. Gonçalves	Gestor de Segurança da Informação
Verificado por	Rhamine Carin Vieira	Colaboradora da COTIC
Aprovado por	Luís Rodrigo de O. Gonçalves	Gestor de Segurança da Informação

Documento assinado eletronicamente no Processo SEI nº 01209.000061/2020-55