LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA
Av. Getúlio Vargas, nº 333, - Bairro Quitandinha,
CEP 25651-075, Petrópolis - RJ - http://www.lncc.br

Procedimento de notificação de não conformidade			
CÓDIGO	**VERSÃO**	**TIPO DE ACESSO**	**NÍVEL DE ACESSO**
29-PNNC	5.2	Externo	Público
CONTROLES DA ABNT NBR ISO/IEC 27001:2022			**PUBLICADO EM**
Cláusula 10 - Melhoria 5.28 - Notificação de eventos de segurança 6.1 – Ações para abordar riscos e oportunidades			04/09/2026

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.

3. RESPONSABILIDADE

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

3.2 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. PUBLICAÇÃO E DIVULGAÇÃO

Este documento é de distribuição pública e destina-se a todos os colaboradores do LNCC e demais partes interessadas no Sistema de Gestão de Segurança da Informação .

5. 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)
Regimento Interno do Laboratório Nacional de Computação Científica	Portaria MCTI Nº 7.061, de 24 de maio de 2023 (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)

6. 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

68-RPNCOM	Diretrizes para Registro e Planejamento de Tratativas de Não Conformidades e Oportunidades de Melhoria

7. 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).

8. TERMOS E DEFINIÇÕES

Não Conformidade	Não conformidade é definida formalmente como o não atendimento a um requisito. Trata-se de qualquer desvio em relação a expectativas, regras ou critérios estabelecidos, que podem ser declarações, obrigações implícitas ou mandatórias.
Oportuniade de Melhoria	No contexto de Sistemas de Gestão e Processos (ISO/IEC 27001 e ISO 27003), representa um ponto de aprimoramento onde, embora um processo ou controle já atenda formalmente aos requisitos vigentes (não havendo descumprimento ou não conformidade), identifica-se a possibilidade clara de torná-lo mais eficiente, seguro, automatizado, econômico ou menos suscetível a erros. Na perspectiva Prática e de Controle, trata-se de uma situação positiva em que o ganho é provável e sobre a qual a organização possui um nível razoável de controle.
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, 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.

9. REALIZANDO UMA NOTIFICAÇÃO

9.1 Todos os colaboradores e partes interessadas do Sistema de Gestão de Segurança da Informação (SGSI) devem realizar notificações por meio do e-mail institucional sgsi@lncc.br sempre que identificarem ou suspeitarem de:

a) Não conformidades do SGSI em relação à norma ISO/IEC 27001 ou a outras normativas aplicáveis;
b) Riscos que possam comprometer a segurança da informação;
c) Oportunidades voltadas à melhoria contínua da segurança da informação; ou
d) Quaisquer outras ações que favoreçam o aprimoramento contínuo do SGSI.

9.1.1 Sempre que possível, a notificação deve apresentar uma descrição detalhada do ocorrido e os impactos potenciais à segurança da informação, facilitando a priorização e a adoção das medidas cabíveis.

9.2 É vedado aos colaboradores ou partes interessadas a execução de testes por conta própria para verificar a existência de riscos ou não conformidades. As análises, investigações e correções no ambiente técnico devem ser realizadas exclusivamente pelas equipes formalmente autorizadas.

10. RECEBENDO E TRATANDO A NOTIFICAÇÃO

10.1 Ao receber as notificações encaminhadas ao endereço de correio eletrônico do Sistema de Gestão de Segurança da Informação (sgsi@lncc.br), o Gestor de Segurança deve examiná-las para confirmar se configuram uma não conformidade. Caso se confirme a ocorrência, o proprietário do ativo correspondente deve ser imediatamente notificado para que adote as providências cabíveis, em estrita conformidade com o documento 68-RPNCOM (Diretrizes para Registro e Planejamento de Tratativas de Não Conformidades e Oportunidades de Melhoria).

10.2 O Gestor de Segurança deve repassar as notificações de riscos ao agente formalmente encarregado da gestão de riscos de segurança da informação, o qual deverá conduzir os procedimentos subsequentes conforme estipulado no documento 37-MAR (Definição da Metodologia da Avaliação de Riscos).

10.3 O Gestor de Segurança da Informação deve aproveitar as reuniões ordinárias do Comitê de Privacidade e Segurança da Informação para apresentar as notificações de oportunidades de melhoria e outras iniciativas voltadas ao aprimoramento contínuo do SGSI. Com o auxílio do Comitê, o gestor deverá analisar a viabilidade técnica, os reflexos operacionais e as vantagens decorrentes dessas ações, fundamentando-se em critérios previamente estabelecidos, além de supervisionar a implantação das medidas aprovadas e registrar a eficácia dos resultados obtidos.

10.4 Todos os registros de notificações recebidas, análises efetuadas, avaliações de risco, planos de ação, deliberações sobre o tratamento de desvios e os resultados da verificação de eficácia devem ser devidamente catalogados e preservados como informação documentada, atendendo integralmente aos requisitos normativos do SGSI.

11. ANÁLISE CRÍTICA

Este documento deve ser analisado criticamente quanto à sua eficácia e adequação ao SGSI do LNCC, sempre que necessário e, no mínimo, a cada 12 meses.

12. 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
5.1	30/10/2025	Ajuste no formato do documento para o SEI

5.2	04/09/2026	Revisão das seções "Realizando uma notificação" e "Recebendo e tratando a notificação" para promover o alinhamento com os demais documentos do SGSI.

Quadro de Aprovação		
	Nome	**Atribuição**
Elaborado por:	Luís Rodrigo de O. Gonçalves	Gestor de Segurança da Informação
Verificado por:	Diogo Pereira da Silva Santos	Tecnologista

Documento assinado eletronicamente por **Diogo Pereira da Silva Santos**, **Tecnologista**, em 04/09/2026, às 14:15 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Luis Rodrigo De Oliveira Gonçalves**, **Gestor de Segurança da Informação**, em 04/09/2026, às 16:49 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.mcti.gov.br/verifica.html, informando o código verificador **14027409** e o código CRC **AD4067FE**.