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

Campanha de Divulgação e Conscientização sobre Segurança da Informação			
CÓDIGO	**VERSÃO**	**TIPO DE ACESSO**	**NÍVEL DE ACESSO**
20-CDCSI	6.0	Externo	Público
CONTROLES DA ABNT NBR ISO/IEC 27001:2022			**PUBLICADO EM**
7.3 – Conscientização; A.6.3 - Conscientização, educação e treinamento em segurança da informação; A.5.20 - Abordagem da segurança da informação nos contratos de fornecedores - k); A.5.27 Aprendizado com incidentes de segurança da informação - c); A.8.7 Proteção contra malware - m); A.8.8 Gestão de vulnerabilidades técnicas - b)			18/12/2025

1. OBJETIVO

O objetivo principal deste documento é estabelecer e formalizar a Campanha Anual de Conscientização e Treinamento em Segurança da Informação do Laboratório Nacional de Computação Científica (LNCC) para o período de janeiro a dezembro de 2026.

Esta iniciativa é parte integrante do Sistema de Gestão de Segurança da Informação (SGSI) e visa:

1. Promover a Cultura de Segurança: Fomentar uma cultura organizacional onde a segurança da informação seja responsabilidade de todos.
2. Atender à Conformidade: Assegurar o cumprimento do controle 5.2.2 (Treinamento e conscientização em segurança da informação) do Anexo A da ABNT NBR ISO/IEC 27001:2022 e o controle 6.3 (Conscientização, educação e treinamento em segurança da informação) da ABNT NBR ISO/IEC 27002:2022.
3. Redução de Risco: Mitigar ativamente os riscos de segurança (tratados no nosso Plano de Tratamento de Riscos) associados ao fator humano, como a falta de conhecimento ou negligência das políticas e procedimentos de segurança.

O sucesso da campanha deve resultar na redução da ocorrência de incidentes críticos, especialmente aqueles causados por erros humanos, como: Acessos e divulgações não autorizados, erros de classificação/manuseio de dados e violações de confidencialidade, integridade e disponibilidade de informações e mídias do LNCC.

2. CAMPO DE APLICAÇÃO

Esta Campanha de Conscientização tem aplicação universal e obrigatória e se estende a todas as pessoas que atuam no LNCC e/ou que trabalham sob o seu controle operacional, incluindo:

- Agentes Públicos (servidores e empregados);
- Estagiários e Menores Aprendizes;
- Prestadores de Serviços (terceirizados) com acesso a sistemas e informações;
- Qualquer Parte Interessada Externa Relevante que, direta ou indiretamente, utilize, acesse, manipule ou suporte os sistemas, infraestrutura ou ativos de informação do LNCC

A aplicação da campanha é crítica e prioritária para todo o pessoal envolvido nos processos e sistemas que fazem parte do escopo certificado pelo SGSI, conforme definido na ABNT NBR ISO/IEC 27001. O conteúdo da campanha é concebido, planejado e monitorado com base nos princípios e nos controles de referência estabelecidos nas normas ABNT NBR ISO/IEC 27001:2022 e ABNT NBR ISO/IEC 27002:2022.

3. RESPONSABILIDADE

O sucesso da Campanha depende do entendimento claro das funções e responsabilidades, alinhadas às diretrizes da ABNT NBR ISO/IEC 27001 (Cláusulas 5 e 7).

Responsável	Atribuições Chave (SGSI)
Gestor de Segurança da Informação (GSI)	**Planejamento e Execução (Cláusula 7.2):** Elaborar, manter, revisar e publicar o conteúdo técnico da Campanha. Coordenar as ações com o SECIN e o Comitê de Privacidade e Segurança da Informação
Comitê de Privacidade e Segurança da Informação	**Monitoramento e Melhoria Contínua (Cláusula 9.1):** Avaliar a eficácia e a eficiência das ações da Campanha.
Serviço de Comunicação Institucional (SECIN)	**Divulgação e Formato:** Promover a divulgação da Campanha, garantindo que o formato (pôster, e-mail, vídeo, etc.) seja didático e atrativo. Apoiar na execução logística das ações (calendário, plataformas).
Colaboradores (Pessoas sob Controle do LNCC)	**Participação e Feedback (Cláusula 7.3):** É responsabilidade individual acompanhar, participar ativamente e aplicar os conhecimentos e as regras divulgadas na Campanha. Os colaboradores são incentivados a encaminhar sugestões de temas ao GSI (**gsi@lncc.br**) para garantir a relevância e adequação contínua da Campanha.

4. DOCUMENTOS DE REFERÊNCIA

Os documentos listados a seguir são mencionados neste documento e fornecem requisitos, diretrizes ou orientações essenciais para sua aplicação. Para referências com datas específicas, aplicam-se apenas as edições citadas. Para referências sem datas específicas, aplicam-se as edições mais recentes, 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

27001:2022	informação — Requisitos
ABNT NBR ISO/IEC 27002:2022	Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação
Glossário de Segurança da Informação	Portaria GSI/PR nº 93, de 18 de outubro de 2021 (https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370)
Política de Segurança da Informação do LNCC	Esta política representa o comprometimento do LNCC em satisfazer os requisitos aplicáveis relacionados à segurança da informação, como: a ABNT NBR ISO/IEC 27001, requisitos definidos em contratos, as leis, os decretos e demais normativas governamentais (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)
Sistema de Gestão de Segurança da Informação (08-ISMS)	Visão geral do Sistema de Gestão de Segurança da Informação (SGSI) do LNCC (Laboratório Nacional de Computação Científica).

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.

Não há documentos complementares.

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

Para este documento, aplicam-se os seguintes termos e definições, baseados nas normas de referência, no Glossário de Segurança da Informação e na ISO/IEC 27000. As descrições devem ser interpretadas em conjunto. Em caso de divergência, prevalecem os termos e definições estabelecidos no Glossário de Segurança da Informação do GSI/PR.

Colaboradores	No contexto deste documento, "colaborador" refere-se a qualquer agente público, estagiário, menor aprendiz, terceirizado ou indivíduo que direta ou indiretamente utiliza ou suporta os sistemas, infraestrutura ou informações da instituição.

8. METODOLOGIA E CANAIS DE DIVULGAÇÃO

8.1 Estratégias de Comunicação Multicanal

8.1.1 Para garantir que as diretrizes de segurança alcancem todos os colaboradores de forma eficaz, o LNCC adotará em 2026 uma abordagem de

comunicação híbrida e multicanal, dividida em duas frentes principais:

a) Estratégia Física: Fixação de materiais impressos (cartazes, infográficos e avisos) em pontos estratégicos de circulação no campus. O objetivo é manter a visibilidade constante de boas práticas no ambiente de trabalho físico (ex: política de mesa limpa e descarte de documentos).

b) Estratégia Digital: Disseminação de conteúdos por meio dos ativos de comunicação eletrônica da instituição, incluindo e-mail corporativo, intranet, site oficial e perfis institucionais em redes sociais. Esta frente permite o compartilhamento de alertas rápidos e conteúdos interativos.

8.1.2 A norma recomenda que o programa de conscientização seja variado para evitar a "fadiga de segurança". Alternar entre cartazes físicos e e-mails ajuda a manter o engajamento.

8.2 Ações Especiais e Eventos Institucionais

8.2.1 O Gestor de Segurança da Informação (GSI), em colaboração com o Serviço de Comunicação Institucional (SECIN), monitorará o tema da Semana Nacional de Ciência e Tecnologia (SNCT). Caso haja correlação com a Segurança da Informação, serão desenvolvidas atividades técnico-educativas específicas (ex: palestras, workshops ou simulações) para integrar a cultura de segurança aos eventos científicos da instituição.

8.3 Cronograma e Periodicidade de Temas

8.3.1 A campanha terá caráter contínuo e progressivo. Mensalmente, o GSI selecionará um ou mais temas prioritários.

a) Produção de Conteúdo: Para cada tema mensal, serão produzidos materiais didáticos adaptados para cada canal de divulgação (e-mail, murais e redes sociais).

b) Objetivo da Periodicidade: Garantir que a conscientização não seja um evento isolado, mas um processo de aprendizado contínuo que mantenha o nível de alerta dos colaboradores elevado durante todo o ano.

8.3.2 Após a última divulgação da campanha de conscientização prevista para Dezembro de 2026, será conduzido um conjunto de atividades de avaliação e planejamento, contemplando a realização de pesquisa de percepção e maturidade em Segurança da Informação junto aos colaboradores, a análise do nível de adesão às ações e aos conteúdos divulgados ao longo do ano, bem como a consolidação e divulgação dos resultados obtidos. Com base nessas análises, será elaborado o planejamento preliminar da campanha de conscientização de 2027, de forma a promover a melhoria contínua do programa, o alinhamento às necessidades institucionais e o fortalecimento da cultura de Segurança da Informação no LNCC.

8.4 Evidência de Auditoria

a) Recomenda-se que o GSI e o SECIN guardem cópias (digitais ou fotos) de todos os materiais divulgados em 2026. Isso servirá como evidência objetiva de que o controle de conscientização está operando de forma eficaz durante a auditoria de certificação.

9. AÇÕES PLANEJADAS

ID	Mês	Tema	Assuntos Sugeridos	Referência ISO/IEC 27002:2022 ou

				PPSI
01	Jan	Fundamentos e cultura PPSI	Mensagem da alta administração sobre importância do PPSI; - Responsabilidade de todos pela segurança; - Visão geral da governança (alta administração, gestor de SI, ETIR).	PPSI Controle 0 (estruturação básica); PPSI Controle 0.11 POSIN; Princípios da PSI.
02	Jan	Governança e Políticas	Políticas de Segurança da Informação - Principais políticas - Onde encontrar, o que mudou e o dever de cumprimento.	ISO Controles 5.1, 5.36
03	Fev	Governança e Políticas	Responsabilidades e Papéis: - Quem é quem na segurança (Gestor, Comitê, Usuário) e o dever de reportar falhas.	ISO Controles 5.2, 5.4
04	Fev	Política de Segurança e canais de denúncia	Difusão da Política de Segurança da Informação; - Responsabilidades dos usuários; - Sanções; - Canais de denúncia de incidentes e violações da política.	ISO Controle 0.11 POSIN; artigos 22, 30–33 do modelo de PSI; ISO Controle 14.
05	Mar	Conceitos básicos de SI e LGPD	- Confidencialidade, integridade, disponibilidade e autenticidade; - Noções iniciais de LGPD no setor público; - Papel do usuário de informação e do encarregado.	ISO Controle 14 (conscientização); ISO Controles 19–21 (registro, prevenção, direitos titulares).
06	Mar	Controle de Acesso e Identidade	Autenticação Segura: - A importância da autenticação multifator (MFA) e a gestão de senhas fortes (não compartilhar, não anotar).	ISO Controles 5.17, 8.5
07	Mar	Controle de Acesso e Identidade	Gestão de Identidade: - O ciclo de vida do acesso (admissão, mudança de cargo e desligamento) e a devolução de ativos.	ISO Controle 5.16, 5.11
08	Abr	Segurança Física e Ambiente	Mesa Limpa e Tela Limpa: - Proteção de documentos impressos e bloqueio de tela automático em estações de trabalho.	ISO Controle 7.7
09	Abr	Segurança Física e Ambiente	Trabalho em Áreas Seguras e Remotas: - Cuidados com informações ao trabalhar fora do escritório (Home Office/Viagens) e "espiar por cima do ombro".	ISO Controles 7.6 e 6.7
10	Abr	Proteção de Dados e Privacidade	Privacidade e LGPD: - Tratamento de Dados Pessoais e Técnicas de Mascaramento de Dados (anonimização/pseudonimização).	ISO Controle 5.34 e 8.11
11	Maio	Proteção de Dados e Privacidade	Exclusão de Informações: - Como e quando descartar dados de forma segura (limpeza digital) para evitar vazamentos.	ISO Controle 8.10 e 7.14

12	Maio	Segurança na Nuvem e Internet	Uso Seguro de Serviços em Nuvem: - Riscos de armazenar dados institucionais em nuvens públicas não homologadas (Shadow IT).	ISO Controle 5.23
13	Maio	Segurança na Nuvem e Internet	Navegação Segura e Filtragem Web: Riscos de acessar sites maliciosos e o papel do filtro de conteúdo.	ISO Controle 8.23
14	Jun	Ameaças Cibernéticas	Engenharia Social e Phishing (Reforço): - Identificação de e-mails, SMS e chamadas fraudulentas. - Novas táticas de ataque.	ISO Controle 8.7
15	Jun	Engenharia social e phishing	Reconhecimento de phishing, vishing e smishing; - Cuidados com links e anexos; - Verificação de remetente; - Reporte de tentativas de fraude Referência: Guia PPSI 2.0-v1	PPSI Controle 9 (proteção de e-mail) PPSI Controle 10 (defesa contra malware) PPSI Controles 14.4–14.7.
16	Jul	Uso aceitável de e-mail, internet e mídias	- Regras de uso aceitável; - Riscos em mídias sociais; - Download e instalação de software; - Vedação a sites inadequados e software não autorizado. Referência: Modelo de Política Segurança Informação - SGD	PPSI Controle 9; PPSI Controle 10; diretrizes de uso aceitável e vedações (arts. 25, 26–29).
17	Jul	Ameaças Cibernéticas	Inteligência de Ameaças: - Entendendo o cenário atual de ataques e como a organização usa informações para se defender.	ISO Controle 5.7
18	Jul	Gestão de Incidentes	Notificação de Eventos: - Como relatar um incidente suspeito ou confirmado (ponto de contato, o que informar).	ISO Controles 6.8 e 5.24
19	Ago	Gestão de Incidentes	Aprendizado com Incidentes: - Estudos de caso (anonimizados) sobre incidentes reais e como foram resolvidos.	ISO Controle 5.27
20	Ago	Teletrabalho e redes inseguras	- Riscos de redes Wi-Fi abertas; - Boas práticas para rede doméstica; - VPN institucional; - Proteção de dados em acesso remoto. Referência: Guia PPSI 2.0-v1	PPSI Medida 14.8 (redes inseguras); PPSI Controle 12 (infraestrutura de rede); NC 18/IN01/GSI/PR.
21	Set	Dispositivos e Mobilidade	Segurança em Dispositivos Móveis: - Uso de dispositivos corporativos e pessoais (BYOD), - Criptografia e bloqueio remoto.	ISO Controle 8.1
22	Set	Dispositivos e Mobilidade	Mídias Removíveis: - Riscos do uso de Pen Drives e HDs externos não criptografados.	ISO Controle 7.10

23	Set	Continuidade e Resiliência	Backup das Informações: - A responsabilidade do usuário em salvar dados nos locais corretos (rede/nuvem) para garantir a recuperação.	ISO Controle 8.13
24	Out	Continuidade e Resiliência	Segurança durante Disrupção: - Como manter a segurança operando mesmo durante falhas ou crises.	ISO Controle 5.29
25	Out	Cibersegurança	Proteção contra Malware e Ransomware: A importância das atualizações de software e antivírus.	ISO Controles 8.7 e 8.19
26	Out	Cibersegurança	Gestão de Vulnerabilidades: - Por que o TI solicita a realização de atualizações e reinicializações (Correção de falhas).	ISO Controle 8.8
27	Nov	Terceiros e provedores de serviço	- Riscos com fornecedores; - Cláusulas contratuais de privacidade e segurança; - Responsabilização por incidentes; - Fluxo de desligamento seguro de provedores. Referência: Guia PPSI 2.0-v1	PPSI Controle 15 (provedores de serviço); PPSI Controle 22 (contratos, acordos).
28	Nov	Segurança nas Relações	Segurança com Fornecedores: - Cuidados ao compartilhar dados com terceiros e contratos de manutenção.	ISO Controle 5.19 e 5.20
29	Dez	Conformidade e Ética	Propriedade Intelectual e Licenciamento: - Uso correto de software licenciado e respeito aos direitos autorais.	ISO Controle 5.32
30	Dez	Conformidade e Ética	Retrospectiva e Riscos: - Revisão dos principais riscos do ano e preparação para o próximo ciclo.	ISO Controle 5.36

10. ANÁLISE CRÍTICA

Este documento deve ser analisado criticamente quanto à sua pertinência e eficácia ao SGSI ao menos a cada 12 meses, ou quando ocorrem mudanças.

11. HISTÓRICO DA REVISÃO E QUADRO DE APROVAÇÃO

Revisão	Data	Itens Revisados
1.0	11/10/2019	Documento Inicial.
1.1	17/05/2020	Aplicação dos rótulos de classificação e atualização dos dados da equipe
1.2	10/03/2021	Atualização das atividades para 2021 e 2020
1.3	21/04/2021	Adequação do documento ao novo formato.
2.0	06/06/2022	Atualização das informações e atividades para 2022

3.0	15/06/2024	Atualização das informações e atividades para 2023 e 2024; Conversão do documento para o novo template utilizando no SGSI
4.0	09/01/2024	Atualização das informações sobre as atividades, com o replanejamento da execução das mesmas para iniciarem em janeiro de 2024.
4.1	05/07/2024	Atualização na formatação.
5.0	27/12/2024	Adequação do documento aos controles da versão de 2022 da norma ABNT NBR ISO/IEC 27001; Planejamento dos temas da campanha de 2025.
6.0	18/12/2025	Planejamento dos temas da campanha de 2026

Quadro de Aprovação		
	Nome	**Atribuição**
Elaborado por:	Luís Rodrigo de Oliveira Gonçalves	Gestor de Segurança da Informação
Verificado por:	Rhamine Carin Vieira	Colaboradora da Coordenação de Tecnologia da Informação e Comunicação
Validado por:	Fernanda Fernandes Beirão Sperling	Chefe Substituta do SECIN

Documento assinado eletronicamente por **Luis Rodrigo De Oliveira Gonçalves**, **Gestor de Segurança da Informação**, em 18/12/2025, às 12:11 (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 **Rhamine carin vieira (E)**, **Usuário Externo**, em 18/12/2025, às 13:57 (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 **Fernanda Fernandes Beirao Sperling**, **Analista em Ciência e Tecnologia**, em 05/01/2026, às 12:58 (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 **13387993** e o código CRC **6B2E2E9D**.