Campanha de Divulgação e Conscientização sobre Segurança da Informação		Laboratório Nacional de Computação Científica / MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES	
CÓDIGO	**VERSÃO**	**TIPO DE ACESSO**	**NÍVEL DE ACESSO**
20-CDCSI	4.1	Externo	Público
CONTROLES DA ABNT NBR ISO/IEC 27001:2013		**PUBLICADO EM**	**PAGINAÇÃO**
7.3, A.7.2.2 e A.12.2.1		05/07/2024	1/4

SUMÁRIO

1 OBJETIVO

O objetivo deste documento é apresentar a Campanha de Divulgação e Conscientização de Segurança da Informação do Laboratório Nacional de Computação Científica (LNCC). Neste documento serão descritas as ações a serem executadas no período compreendido entre janeiro de 2024 e dezembro de 2024.

O processo de conscientização e divulgação faz parte dos esforços do LNCC em promover a cultura de segurança da informação entre os seus colaboradores e, desta forma, atender aos requisitos da IEC/ISO 27001.

Com esta campanha o LNCC busca reduzir os riscos relacionados à falta de entendimento das regras de segurança, que podem levar a vários tipos de violações e incidentes de segurança tais como: acesso não autorizado às informações e mídias; erros operacionais; vazamento, roubo de informações e mídias.

2 CAMPO DE APLICAÇÃO

Esta campanha se aplica a todos os colaboradores do LNCC, quais sejam: agentes públicos, estagiários, menores aprendiz, prestadores de serviços ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, infraestrutura ou informações deste órgão.

3 RESPONSABILIDADE

O gestor de segurança da informação e a chefia do SECIN são os responsáveis pela elaboração e análise crítica deste procedimento. A responsabilidade pela aprovação e publicação deste procedimento é do gestor de segurança.

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 27001:2013	Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos
ABNT NBR ISO/IEC 27002:2013	Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação
Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020	Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal (https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215)
Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021	Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal (https://www.in.gov.br/en/web/dou/-/instrucao-normativa-gsi/pr-n-3-de-28-de-maio-de-2021-322963172)
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)

Continua...

Portaria MCTI nº 6572, de 22 de novembro de 2022	Regimento Interno do Laboratório Nacional de Computação Científica (https://in.gov.br/en/web/dou/-/portaria-mcti-n-6.572-de-22-de-novembro-de-2022-446088220)
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 Cientifica).
Política de Segurança da Informação do LNCC (02-PSI)	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-1/02-PSI%20LNCC)

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.

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://in.gov.br/en/web/dou/-/portaria-mcti-n-6.572-de-22-de-novembro-de-2022-446088220).

7 TERMOS E DEFINIÇÕES

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 POLÍTICA DE TRANSIÇÃO PARA ADEQUAÇÃO DA NORMA

8.1 O prazo para adequação dos processos e procedimentos aos requisitos deste documento será até julho/2024. Após essa data, os documentos que não tenham sido adequados à presente norma serão considerados não conformes com relação aos requisitos.

9 PAPEIS E RESPONSABILIDADES PELO PROCESSO

9.1 A direção do LNCC deve prover os recursos para a implementação e monitoramento das ações relacionadas a conscientização em segurança da informação.

9.2 O gestor de segurança da informação deve acompanhar o monitoramento das ações relacionadas a conscientização em segurança da informação.

9.3 A equipe do SECIN deve promover a divulgação e apoiar na execução das ações relacionadas a conscientização em segurança da informação.

9.4 Os colaboradores devem acompanhar ações relacionadas a conscientização em segurança da informação.

9.5 Recomenda-se aos colaboradores que encaminhem aos gestores de segurança (gsi@lncc.br) e ao SECIN (secin@lncc.br) sugestões e indicações de temas a serem abordados na campanha e nas ações de conscientização.

10 CAMPANHA DE CONSCIENTIZAÇÃO

10.1 Em 2024 serão realizadas divulgações de materiais sobre segurança da informação, que se utilizarão duas estratégias:

a) **Estratégia física**: cartazes serão fixados no campus;
b) **Estratégia eletrônica**: uso de e-mails, do site oficial e das redes sociais da instituição.

10.2 Dependendo do tema da Semana Nacional de Ciência e Tecnologia (SNCT), havendo aderência com segurança da informação, o Gestor de Segurança da Informação (GSI) e o Serviço de Comunicação Institucional (SECIN) elaborarão atividades a serem realizadas neste evento.

10.3 Mensalmente são definidos um ou mais temas e, baseado neles, serão produzidos os materiais, que serão divulgados utilizando o sistema de e-mail do LNCC, os murais, e as redes sociais da instituição.

11 ATIVIDADES DA CAMPANHA DE CONSCIENTIZAÇÃO

Mês	Tema	Assuntos
Janeiro/2024	Segurança e Políticas de segurança da informação	1. Reconhecendo o papel dos colaboradores na segurança da informação e no SGSI do LNCC 2. A importância e a necessidade da política de Mesa Limpa e Tela Limpa 3. Localizando as políticas e notificando não conformidades (5.2.b; A.5.1.1)
Fevereiro/2024	Privacidade	1. A Lei geral de proteção de dados e a classificação das informações 2. Identificando e mapeamento de dados pessoais 3. Protegendo nossos equipamentos contra acessos não autorizados (equipamentos sem monitoramento e equipamentos que são mantidos “desbloqueados”)
Março/2024	Incidentes de segurança	1. Conhecendo o CTIR.GOV, a ETIR e notificando incidentes de segurança 2. Principais incidentes de segurança identificados pelo CTIR.GOV
Abril/2024	Proteção de Dados	1. Entendo por que a proteção contra malware vai além do uso de antivírus. 2. Ataques de Ransonware e como podemos evitá-los
Maio/2024	Uso consciente	1. Uso consciente do e-mail institucional 2. Uso consciente da área de armazenamento de dados institucional 3. Aplicações utilizadas em reuniões remotas, dicas e boas práticas de segurança
Junho/2024	Proteção de Dados e trabalho remoto	1. Acesso remoto vantagens, desvantagens e cuidados. 2. Acesso remoto e o uso da VPN 3. Protegendo suas credenciais de acesso e verificando possíveis vazamentos
Julho/2024	Segurança da informação	1. Os quatro pilares da segurança da informação – Confidencialidade, Disponibilidade, Integridade e Autenticidade 2. A importância de uma gestão eficaz da segurança da informação e da conformidade com os requisitos do sistema de gestão da segurança da informação; (5.1.d)
Agosto/2024	Segurança da informação	1. Segurança da informação e a conformidade legal na administração pública federal (AFP) 2. A segurança da informação nos acordos com fornecedores (A.15.1.2) e na cadeia de suprimentos.
Setembro/2024	Segurança da informação	1. Risco de segurança da informação 2. Identificando e notificando riscos de segurança da informação e não conformidade do SGSI 3. Riscos de segurança da informação nos processos de contratação
Outubro/2024	Proteção de Dados	1. Alertas de segurança e as vulnerabilidades técnicas 2. Mantendo os sistemas e as aplicações atualizadas
Novembro/2024	Segurança da Informação	1. A importância e a necessidade da política de Mesa Limpa e Tela Limpa 2. Riscos relacionados a dispositivos sem monitoramento e que não são mantidos bloqueados enquanto não estão em uso 3. Uso consciente de dispositivos móveis no ambiente de trabalho e remotamente
Dezembro/2024	Proteção de Dados	1. Phishing, Ransonware e outros males 2. Lidando e notificando phishing 3. Backup como uma forma de minimizar o impacto dos ransonwares

12 ANÁLISE CRÍTICA

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

13 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.

Quadro de Aprovação		
	Nome	**Atribuição**
Elaborado por:	Anmily Paula Martins	Chefe do SECIN
Verificado por:	Rhamine Carin Vieira	Equipe do SESTI
Aprovado por:	Luis Rodrigo de Oliveira Gonçalves	Gestor de Segurança da Informação

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

_____