Uso de Dispositivos Pessoais *(Bring your own device)*			
CÓDIGO	**VERSÃO**	**TIPO DE ACESSO**	**NÍVEL DE ACESSO**
53-BYOD	2.0	Externo	Público
CONTROLES DA ABNT NBR ISO/IEC 27001:2013		**PUBLICADO EM**	**PAGINAÇÃO**
A.6.2.1		12/06/2024	1/4

SUMÁRIO

1 OBJETIVO

Esta norma estabelece os requisitos de segurança a serem atendidos pelos colaboradores quando da utilização de dispositivos móveis pessoais para acessar os ativos de informação do LNCC. Ela visa aumentar a produtividade ao mesmo tempo que flexibiliza o uso de dispositivos pessoais, tais como: smartphones, laptops, notebooks e tablets.

Esta norma utiliza como base os princípios, estrutura e processos apresentados nas normas ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013.

Esta norma visa esclarecer as partes envolvidas sobre as regras de uso de dispositivos pessoais no LNCC. No contexto do ambiente do LNCC, esta política corresponde a política de Uso de Dispositivos Pessoais, doravante denominada BYOD.

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.

A norma aplica-se a todos os colaboradores e seus dispositivos móveis.

3 RESPONSABILIDADE

A responsabilidade pela elaboração, revisão, publicação ou cancelamento desta norma é do Comitê de Segurança da Informação e Comunicação do LNCC. A responsabilidade pela aprovação desta norma é do Diretor do LNCC. Este documento é elaborado com o apoio do Serviço de Suporte de Sistemas e Redes - SERED.

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
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 2022	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)

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.

11- PS	Política de Senhas

6 SIGLAS

SGSI Sistema de Gestão de Segurança da Informação
BYOD *Bring Your Own Device*, do inglês Traga Seu Próprio Dispositivo

Nota: As siglas das UO do LNCC podem ser acessadas no Regimento Interno do Laboratório Nacional de Computação Científica.

7 TERMOS E DEFINIÇÕES

Para os efeitos deste documento, aplicam-se os termos e definições a seguir, baseados nas normas de referência a Portaria GSI/PR nº 93/2021 e a 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.

BRING YOUR OWN DEVICE (BYOD)	trata-se de uma política de segurança de uma organização, que permite que os dispositivos pessoais dos colaboradores sejam usados nas atividades corporativas. Uma política BYOD estabelece limitações e restrições sobre se um dispositivo pessoal (como um notebook, smartphone ou tablet) pode ou não ser conectado pela rede corporativa;
DISPOSITIVOS MÓVEIS	equipamentos portáteis, dotados de capacidade de processamento, ou dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não limitando a estes: e-books, notebooks, netbooks, smartphones, tablets, pendrives, USBdrives, HD externo, e cartões de memória;
EVENTO DE SEGURANÇA	qualquer ocorrência identificada em um sistema, serviço ou rede, que indique uma possível falha da política de segurança, falha das salvaguardas ou mesmo uma situação até então desconhecida, que possa se tornar relevante em termos de segurança;

8 PAPEIS E RESPONSABILIDADES PELO PROCESSO DE BYOD

8.1 O gestor de segurança da informação e o comitê de segurança da informação são os responsáveis pela elaboração da norma de BYOD, por avaliar a eficácia e a eficiência do processo de BYOD.

8.2 Para avaliar eficácia e a eficiência da gestão de BYOD gestor deve acompanhar o monitoramento da ocorrência de eventos de segurança envolvendo dispositivos móveis pessoais utilizados pelos colaboradores.

8.3 Imediatamente após identificarem eventos de segurança, os colaboradores devem realizar a notificação dos mesmos utilizando endereço eletrônico do Service Desk (helpdesk@lncc.br).

8.4 Periodicamente, o SECIN deve realizar a divulgação desta norma para a comunidade de colaboradores do LNCC.

9 DIRETRIZES GERAIS

9.1 A segurança dos ativos do LNCC é uma prioridade desta política.

9.2 Ao usar um dispositivo pessoal, no ambiente do LNCC, o colaborador concorda em cumprir todas as políticas de segurança da instituição.

9.3 Dispositivos pessoais não devem ser conectados à rede cabeada da instituição.

9.4 Dispositivos pessoais somente devem ser conectados as redes Wi-fi da instituição.

9.5 O colaborador deve estar ciente de que as redes da instituição podem ser monitoradas e que um controle de acesso pode ser aplicado.

9.6 O colaborador é responsável pela segurança das informações da instituição que acessa através de seu dispositivo pessoal.

9.7 O colaborador é responsável por garantir a conformidade com todas as políticas de segurança do LNCC, a instalação de atualizações de software e segurança, e a conformidade com todas as leis e regulamentações aplicáveis.

10 DISPOSITIVOS SUPORTADOS

10.1 Dentre os dispositivos pessoais permitidos no ambiente do LNCC destacam-se: e-books, tablets, smartphones, laptops e notebooks.

10.2 Demais tipos de dispositivos não devem ser conectados ao ambiente do LNCC, assim como não devem ser utilizados para acessar ou processar dados da instituição.

10.3 Recomenda-se que os dispositivos estejam com sistemas operacionais atualizados e com as últimas atualizações de segurança.

10.4 Casos específicos deverão ser avaliados pela COTIC, que poderá autorizar o uso do equipamento.

11 RESPONSABILIDADE DOS COLABORADORES

11.1 Os colaboradores devem cumprir todas as políticas de segurança e privacidade do LNCC e do Governo Federal, incluindo a Lei Geral de Proteção de Dados (LGPD) e outras leis de privacidade de dados.

11.2 Os colaboradores devem garantir que seus dispositivos estejam sempre seguros e protegidos.

11.3 Recomenda-se que os colaboradores mantenham os softwares e os aplicativos do dispositivo com as devidas correções de vulnerabilidades.

11.4 Os colaboradores devem realizar o armazenamento dos dados do LNCC apenas em áreas de armazenamento seguras.

11.5 Recomenda-se que colaboradores ativem a criptografia de dados em seus dispositivos. Garantindo que todas as informações armazenadas no dispositivo sejam criptografadas.

11.6 Os colaboradores devem informar imediatamente ao Service Desk (helpdesk@lncc.br) quando houver qualquer suspeita de comprometimento da segurança em seus dispositivos pessoais.

11.7 Recomenda-se que os colaboradores não deixem seus dispositivos desbloqueados enquanto conectados à rede do LNCC.

11.8 Os colaboradores devem ativar as opções de bloqueio automático de tela.

11.9 Recomenda-se aos colaboradores que utilizem uma solução contra malware instalada nos dispositivos. Recomenda-se aos colaboradores que a solução realize análises periódicas dos dispositivos, garantindo que o mesmo não esteja contaminado.

11.10 Recomenda-se que os colaboradores mantenham uma solução de firewall ativa em seus dispositivos.

11.11 Recomenda-se que os colaboradores periodicamente verifiquem seus dispositivos contra vulnerabilidades técnicas e que apliquem as tratativas apropriadas.

11.12 Os colaboradores devem utilizar senhas fortes e únicas para acessar seus dispositivos, sites e aplicativos.

11.13 Recomenda-se que os colaboradores sigam as diretrizes definidas na política de senhas do LNCC.

11.14 Os colaboradores não devem compartilhar senhas ou informações confidenciais com outras pessoas.

11.15 Os colaboradores não devem utilizar os softwares e os sites listados na seguinte URL: https://www.gov.br/lncc/pt-br/acesso-a-informacao/institucional/politica-de-seguranca-1/politica-de-seguranca-da-informacao-supercomputador-santos-dumont/lista-de-softwares-e-sites-nao-autorizados.

11.16 Os colaboradores são responsáveis por manter a integridade dos dados do LNCC e não devem alterar, apagar ou compartilhar dados do LNCC sem autorização.

11.17 Os colaboradores devem estar cientes que uso inadequado de informações da instituição ou violação desta política pode resultar na revisão do acesso aos recursos do LNCC.

11.18 Conforme a legislação em vigor, ações que comprometam a segurança dos dados do LNCC ou custodiados por ele, assim como ações que comprometam a privacidade dos indivíduos, poderão acarretar, aos colaboradores, penalidades de cunho civil e administrativas.

12 ACESSO REMOTO

12.1 Em caso de acesso remoto, os colaboradores devem seguir a Política de Trabalho Remoto, assim como, a de Acesso Remoto.

13 ENCERRAMENTO DAS ATIVIDADES

13.1 Quando do encerramento do vínculo (desligamento) do colaborador com o LNCC, o colaborador deve excluir, de

seus dispositivos pessoais, todos os dados e informações da instituição ou custodiados pela instituição.

13.2 O Colaborador pode solicitar ao LNCC apoio na remoção remota de quaisquer dado ou informação confidencial relacionada a sua atividade na instituição.

14 CASOS OMISSOS

14.1 Caberá ao Gestor de Segurança da Informação e à COTIC deliberar casos omissos a esta política.

15 ANÁLISE CRÍTICA

15.1 Este documento deverá ser analisado criticamente, quanto à sua eficácia e adequação ao SGSI do LNCC, ao menos a cada 12 meses, ou quando ocorrem mudanças.

16 HISTÓRICO DA REVISÃO E QUADRO DE APROVAÇÃO

Revisão	Data	Itens Revisados
1.0	16/06/2023	Versão Original
2.0	12/06/2024	Remoção da seção “Política de Transição”. Atualização das referências para os documentos de referência. Atualização dos controles adotados na norma compatibilizando-a com a norma de trabalho remoto.

Quadro de Aprovação		
	Nome	**Atribuição**
Elaborado por:	Luis Rodrigo de Oliveira Gonçalves	Gestor de segurança da informação
Verificado por:	Comitê de Privacidade e Segurança do LNCC - Portaria LNCC/MCTI nº 420/2024	Membros do Comitê de Privacidade e Segurança da Informação do LNCC
Aprovado por:	Wagner Vieira Léo	Diretor do LNCC - Substituto

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

_____