| POLÍTICA DE SEGURANÇA PARA TRABALHO REMOTO | | | LNCC Laboratório Nacional de Computação Científica — MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO |
|---|---|---|---|
| **CÓDIGO** | **VERSÃO** | **TIPO DE ACESSO** | **NÍVEL DE ACESSO** |
| 55-PSTR | 1.0 | Interno | Público |
| **CONTROLES DA ABNT NBR ISO/IEC 27001:2013** | | **PUBLICADO EM** | **PAGINAÇÃO** |
| A.6.2.2 | | 19 de abril de 2024 | 1/6 |

**SUMÁRIO**



## 1 OBJETIVO

Esta política estabelece os requisitos de proteção das informações acessadas, tratadas ou armazenadas fora das instalações do Laboratório Nacional de Computação Científica (LNCC), quando as pessoas estiverem trabalhando remotamente.

Esta política atua do domínio de segurança de proteção, ela envolve a definição de controles do tipo preventivo e corretivo, atua nas três propriedades básicas de segurança da informação (confidencialidade, integridade e disponibilidade) e está focada nas capacidades operacionais de: gestão de ativos, proteção da informação, segurança física e segurança de sistemas de redes.

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

## 2 CAMPO DE APLICAÇÃO

Esta norma se aplica a todas as unidades organizacionais do LNCC, especialmente naquelas que atuam nos processos integrantes do escopo certificado em conformidade à ABNT NBR ISO/IEC 27001.

## 3 RESPONSABILIDADE

A responsabilidade pela elaboração e revisão desta norma é do Comitê de Privacidade e Segurança da Informação e Comunicação do LNCC e do Gestor de Segurança da Informação. A responsabilidade pela aprovação e cancelamento desta norma é do Diretor do LNCC.

Este documento é elaborado com o apoio do Serviço de Suporte de Sistemas e Redes – SERED e publicado com o apoio do SESTI.

O gestor de segurança da informação e o Comitê de Privacidade e Segurança da Informação e Comunicação do LNCC são os responsáveis por avaliar a eficácia e a eficiência dos controles da política.

Para avaliar eficácia e a eficiência dos controles de segurança relacionados ao trabalho remoto, gestor deve acompanhar o monitoramento da ocorrência de eventos de segurança envolvendo dispositivos utilizados pelos colaboradores fora das instalações do LNCC.

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

## 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.

| | |
|---|---|
| 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) |
| 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 |
| Política de senhas | Estabelece as diretrizes para definição e manutenção de senhas fortes em todo ambiente computacional LNCC. |

## 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://www.gov.br/lncc/pt-br/acesso-a-informacao/institucional/regimento-interno).

## 7 TERMOS E DEFINIÇÕES

| | |
|---|---|
| Colaboradores | No contexto deste documento, entende-se como colaborador quaisquer agente público, estagiário, menor aprendiz, terceirizados ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, infraestrutura ou informações da instituição. |
| 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; |
| Trabalho remoto | Conforme definido na ABNT NBR ISO/IEC 27002:2013, refere-se a todas as formas de trabalho fora do escritório, incluindo ambientes de trabalho não tradicionais, como aqueles referidos como: “ambientes de telecommuting”, “local de trabalho flexível”, “trabalho remoto” e “trabalho virtual”. |

Para os efeitos deste documento, aplicam-se os termos e definições a seguir, baseados nas normas de referência, Portaria GSI/PR nº 93/2021, 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 de gestão de trabalho remoto aos requisitos desta norma será até dezembro/2024. Após essa data, os processos, os procedimentos e os documentos que não tenham sido adequados à presente norma serão considerados não conformes com relação aos requisitos.

## 9 DIRETRIZES GERAIS

**9.1.** O trabalho remoto ocorre quando os colaboradores realizam suas atividades laborais em um local fora das instalações do LNCC, acessando informações seja em cópias impressas ou eletronicamente via equipamento de TIC.

**9.2.** Os ambientes de trabalho remoto incluem aqueles chamados de “teletrabalho”, “local de trabalho flexível”, “ambientes de trabalho virtuais” e “manutenção remota”.

**9.3.** O espaço de trabalho remoto deve ser adequado para a realização das tarefas diárias e deve ser capaz de garantir a Confidencialidade, a Integridade e a Disponibilidade das informações.

**9.4.** Visando garantir eficiência e eficácia das atividades, as ações executadas remotamente poderão ser monitoradas.

**9.5.** Os colaboradores são os principais responsáveis por garantir a segurança dos dados e informações do LNCC durante o trabalho remoto.

## 10 RESPONSABILIDADE DO LNCC

**10.1** O LNCC deve garantir que haja treinamento e conscientização sobre segurança da informação aos colaboradores que trabalham remotamente.

**10.2** Os colaboradores devem receber informações sobre as políticas e práticas de segurança do LNCC, bem como serem orientados a reportar quaisquer incidentes de segurança.

**10.3** Os colaboradores devem ser informados sobre quaisquer alterações na política de segurança e serem orientados a seguir as práticas descritas.

**10.4** O acesso remoto à rede do LNCC deve ser concedido somente a colaboradores que necessitem do mesmo para desempenhar suas funções de forma remota. Qualquer tentativa de acesso não autorizado ou atividade maliciosa será investigada imediatamente pela equipe de segurança do LNCC.

**10.5** Os colaboradores devem compreender a importância do acesso remoto seguro e a responsabilidade que têm em manter a segurança dos dados da instituição. O LNCC se compromete a proteger a privacidade dos colaboradores dentro dos limites estabelecidos pelas leis e regulamentos aplicáveis.

## 11 RESPONSABILIDADE DOS COLABORADORES

**11.1** O LNCC valoriza a privacidade e a segurança dos dados dos seus clientes, colaboradores e parceiros de negócios. Ao trabalhar remotamente, os colaboradores devem prezar pela garantia da proteção dos dados.

**11.2** Os colaboradores devem seguir todas as políticas e procedimentos de privacidade e segurança do Governo Federal, incluindo a Lei Geral de Proteção de Dados (LGPD) e outras leis de privacidade de dados.

**11.3** Os colaboradores devem seguir todas as políticas do LNCC, incluindo: a política de senhas, a política de uso aceitável dos ativos de informação e a comunicação segura de dados sensíveis.

**11.4** Os colaboradores devem participar dos treinamentos e das ações de conscientização sobre privacidade e segurança da informação.

**11.5** Os colaboradores devem manter a privacidade do proprietário das informações a que tiver acesso. Os colaboradores são responsáveis por manter a integridade e a autenticidade dos dados manipulados.

**11.6** Os colaboradores que trabalham remotamente devem ter acesso a um computador confiável e conexão de Internet compatíveis com suas atividades laborais.

**11.7** Os colaboradores devem trabalhar de acordo com os horários estabelecidos pelo LNCC, sendo responsáveis pelo cumprimento de suas tarefas e prazos.

**11.8** Os colaboradores são responsáveis por criar e manter um ambiente de trabalho seguro e protegido de possíveis riscos, como roubo ou acesso não autorizado.

**11.9** É vedado o uso de aplicativos não licenciados durante as atividades de teletrabalho.

**11.10** Os colaboradores devem reportar ao Service Desk (helpdesk@lncc.br) ou à ETIR (etir@lncc.br) quaisquer violações de segurança ou comportamentos suspeitos que possam colocar em risco a segurança dos dados e informações do LNCC.

## 12 ACESSO REMOTO E CONEXÕES SEGURAS

**12.1** A comunicação segura é fundamental para proteger o LNCC e seus colaboradores contra ameaças cibernéticas.

**12.2** Todos os colaboradores remotos devem utilizar uma conexão VPN para se conectar à rede do LNCC, para troca de informações e dados sensíveis do LNCC.

**12.3** O acesso remoto só será permitido aos colaboradores previamente autorizados pelo LNCC. O acesso remoto à rede da LNCC deve ser concedido somente a colaboradores que precisam dele para desempenhar suas funções. Qualquer tentativa de acesso não autorizado ou atividade maliciosa poderá ser investigada pela equipe de segurança da instituição.

**12.4** O acesso remoto deve ser usado em conformidade com esta política e quaisquer outras políticas e diretrizes de segurança estabelecidas pelo LNCC.

**12.5** Os usuários devem desconectar completamente do sistema e fechar todas as conexões remotas ao final do uso, garantindo que não haja acesso não autorizado.

## 13 COMUNICAÇÃO SEGURA

**13.1** Os colaboradores devem usar apenas endereços de e-mail corporativos para se comunicar com a instituição, demais órgãos públicos e fornecedores.

**13.2** Os colaboradores não devem realizar o uso de contas de e-mail pessoais em comunicações institucionais, salvo quando da indisponibilidade do serviço oferecido pela instituição.

**13.3** Ao enviar e-mails, os colaboradores devem verificar cuidadosamente o endereço de e-mail do destinatário antes de enviar qualquer informação confidencial. Isso ajudará a evitar o envio acidental de informações para o destinatário errado;

**13.4** Sempre que possível, as informações sensíveis devem ser compartilhadas usando sistemas de compartilhamento de arquivos seguros preferencialmente criptografados.

**13.5** Ao participar de reuniões virtuais, os colaboradores devem usar apenas soluções indicadas pelo LNCC e que ofereçam recursos de segurança, como autenticação de usuário, criptografia e salas de espera para os participantes entrarem nas reuniões;

**13.6** Os colaboradores devem garantir que as conversas sejam conduzidas em um ambiente privado;

**13.7** Quando os colaboradores trabalharem em locais públicos, devem ter cuidado com quem está ao redor e com o que está em suas telas e teclados;

**13.8** Se os colaboradores tiverem suspeitas de phishing, ataques de malware ou outras ameaças de segurança, eles devem reportar imediatamente ao Service Desk (helpdesk@lncc.br) e ao ETIR (etir@lncc.br)

**13.9** É importante que os colaboradores compreendam a importância da comunicação segura e a responsabilidade que têm em manter a segurança do LNCC. Em contrapartida a instituição se compromete a proteger a privacidade dos colaboradores dentro dos limites estabelecidos pelas leis e regulamentos aplicáveis.

## 14 PROTEÇÃO DE DADOS

**14.1** É importante que os colaboradores compreendam a importância da proteção de dados e a responsabilidade que têm em manter a segurança dos dados do LNCC. Em contrapartida, a instituição se compromete em proteger a privacidade dos colaboradores dentro dos limites estabelecidos pelas leis e regulamentos aplicáveis.

**14.2** Os colaboradores devem manter as informações do LNCC confidenciais e protegidas contra acesso não autorizado, incluindo informações sobre parceiros, fornecedores, finanças, propriedade intelectual e outros dados confidenciais;

**14.3** Todos os dados e informações confidenciais devem ser devidamente protegidos e armazenados de acordo com a política de classificação de informações adotado pelo LNCC;

**14.4** Os colaboradores devem informar imediatamente ao Service Desk (helpdesk@lncc.br) em caso de suspeita de violação de dados ou qualquer outro incidente de segurança.

**14.5** Os colaboradores devem relatar imediatamente quaisquer incidentes de segurança, e-mails suspeitos ou atividades suspeitas ao Service Desk (helpdesk@lncc.br)

**14.6** Os colaboradores devem relatar imediatamente quaisquer perda ou roubo de dispositivos da instituição ao SELEP (selep@lncc.br)

**14.7** Os colaboradores devem cumprir todas as leis e regulamentos aplicáveis de proteção de dados e a privacidade, incluindo a Lei Geral de Proteção de Dados (LGPD).

## 15 PROTEÇÃO DOS DISPOSITIVOS

**15.1** Os dispositivos utilizados pelos colaboradores remotos para acessar a rede do LNCC são um ponto crítico de segurança. Eles podem ser alvos de ataques cibernéticos que podem comprometer a segurança da rede do LNCC e a privacidade dos titulares dos dados. Os colaboradores remotos devem tomar medidas para proteger seus dispositivos contra ameaças cibernéticas e manter seus dispositivos atualizados com as últimas atualizações de segurança.

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

**15.3** Os colaboradores devem aplicar as atualizações de segurança dos softwares e dos aplicativos do dispositivo regularmente.

**15.4** Os colaboradores remotos devem garantir que os sistemas e softwares usados estejam atualizados e protegidos com soluções de segurança apropriadas, como antivírus e firewall;

**15.5** Os colaboradores são responsáveis por proteger seus dispositivos, incluindo computadores, smartphones e tablets,

contra vírus e outros softwares maliciosos.

**15.6** Os colaboradores devem utilizar uma solução contra malware instalada nos dispositivos. A solução deve ser mantida ativa. Os colaboradores devem manter a solução atualizada. Os colaboradores devem utilizar a solução para realizar análises periódicas dos dispositivos utilizados no trabalho remoto, garantindo que ele não esteja contaminado.

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

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

**15.9** Os colaboradores podem solicitar apoio do Service Desk (helpdesk@lncc.br) para a realização de análises de vulnerabilidades de seus dispositivos

**15.10** Os colaboradores nunca devem deixar seus dispositivos sem supervisão enquanto conectados à rede da instituição.

**15.11** Os colaboradores devem ativar as opções de bloqueio automático de tela.

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

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

**15.14** Os dispositivos devem ser protegidos com senhas fortes e softwares de segurança atualizados.

**15.15** Os dispositivos devem ser fisicamente seguros em todos os momentos e nunca devem ser deixados desacompanhados em locais públicos ou em veículos;

**15.16** Os colaboradores devem proteger os dispositivos usados para acessar os dados do LNCC contra roubos, danos e acesso não autorizado;

**15.17** Os colaboradores devem relatar imediatamente ao Service Desk (helpdesk@lncc.br) se o dispositivo for perdido ou roubado.

**15.18** Os colaboradores devem proteger dispositivos de armazenamento, como USBs, CDs, DVDs, entre outros, mantendo-os em local seguro e protegido.

**15.19** Os colaboradores não devem fazer download de softwares não licenciados ou de origem desconhecida nos dispositivos do LNCC.

## 16 MONITORAMENTO

**16.1** O LNCC se reserva o direito de monitorar os recursos de rede da instituição utilizados por parte dos colaboradores durante o trabalho remoto.

**16.2** O LNCC pode monitorar o uso de dispositivos móveis fornecidos pela instituição para verificar o uso adequado, segurança, e conformidade com a política de segurança da instituição;

**16.3** É importante ressaltar que o monitoramento será realizado de forma razoável, justa e legal, e em conformidade com as leis e regulamentações aplicáveis.

**16.4** O LNCC se reserva o direito de realizar auditorias de segurança e conformidade periodicamente para garantir a conformidade com essa e demais política da instituição.

**16.5** Qualquer suspeita de atividade inadequada ou não autorizada será investigada pela equipe de segurança da instituição.

**16.6** É importante que os colaboradores compreendam a importância do monitoramento e a responsabilidade que têm em manter a segurança dos dados da instituição.

## 17 USO ACEITÁVEL

**17.1** A Política de Uso Aceitável (PUA) é um conjunto de regras que regula o uso de recursos de tecnologia da informação e comunicação do LNCC. O objetivo da PUA é promover um ambiente de trabalho seguro, ético e legal, prevenir danos à reputação do LNCC e minimizar o risco de perda ou roubo de informações confidenciais. Os colaboradores remotos devem aderir à PUA e usá-la como referência para suas atividades diárias.

**17.2** Os recursos de tecnologia da informação e comunicação do LNCC, incluindo hardware, software, rede e dados, só podem ser usados para fins institucionais legítimos e autorizados;

**17.3** Os colaboradores não devem usar recursos de tecnologia da informação e comunicação do LNCC para fins ilegais;

**17.4** Os colaboradores não devem acessar sites ou conteúdos impróprios ou ofensivos e redes sociais não relacionadas ao trabalho;

**17.5** Os colaboradores remotos devem relatar imediatamente quaisquer violações desta e das demais políticas à equipe de segurança da informação do LNCC (gsi@lncc.br).

## 18 ENCERRAMENTO DAS ATIVIDADES

**18.1** Quando um colaborador encerra o vínculo com o LNCC, ele deve excluir, de seus dispositivos pessoais, todos os dados e informações relacionados a sua atividade na instituição.

**18.2** O LNCC pode solicitar que o colaborador permita a remoção remota de quaisquer dados ou informações confidenciais relacionadas a sua atividade na instituição.

## 19 CASOS OMISSOS

**19.1** Caberá ao gestor de segurança e ao comitê de privacidade e segurança avaliar casos omissos a esta política.

## 20 ANÁLISE CRÍTICA

**20.1** Esta norma deve ser analisada criticamente ao menos a cada 12 meses, ou quando ocorrem mudanças.

## 21 HISTÓRICO DA REVISÃO E QUADRO DE APROVAÇÃO

| Revisão | Data | Itens Revisados |
|---|---|---|
| 01 | 19/04/2024 | Versão Original |

| 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 do LNCC | Comitê de Privacidade e Segurança da Informação |
| **Aprovado por** | Fábio Borges de Oliveira | Diretor do LNCC |

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

_____