Política de classificação e tratamento da informação		Laboratório Nacional de Computação Científica / MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES	
CÓDIGO	**VERSÃO**	**TIPO DE ACESSO**	**NÍVEL DE ACESSO**
61-CTI	1.1	Externo	Público
CONTROLES DA ABNT NBR ISO/IEC 27001:2022		**PUBLICADO EM**	**PAGINAÇÃO**
A.5.1 - Políticas de segurança da informação; A.5.12 - Classificação das informações; A.5.13 - Rotulagem de informações; A.5.14 - Transferência de informações; A.8.3 - Restrição de acesso à informação;		13/08/2025	1/9

SUMÁRIO

1 Objetivo

A política estabelece os requisitos de proteção das informações acessadas, tratadas ou armazenadas pelo Laboratório Nacional de Computação Científica (LNCC). Ela atua nas quatro propriedades básicas de segurança da informação (confidencialidade, integridade, disponibilidade e autenticidade), assim como na privacidade e proteção de dados pessoais.

A política visa promover a identificação e o entendimento das necessidades de proteção das informações de acordo com a sua importância para o LNCC.

Promover a segurança das informações transferidas dentro do LNCC e com qualquer parte interessada externa.

Esta política tem como objetivo estabelecer diretrizes para a classificação e tratamento das informações com base nos princípios de confidencialidade, autenticidade, disponibilidade, integridade e privacidade, conforme as normas ISO/IEC 27000, a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI).

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.

Esta norma se aplica a todos os tipos de informações geradas, recebidas, armazenadas, processadas ou transmitidas no Laboratório Nacional de Computação Científica (LNCC), independentemente de seu formato (físico, digital, verbal, etc.), e aos colaboradores, estagiários, consultores, fornecedores e demais partes interessadas que tenham acesso a tais informações.

Esta norma abrange todas as áreas funcionais do LNCC, bem como os processos, sistemas, equipamentos e recursos que envolvem o manuseio de informações. Estão incluídas, mas não limitadas a:

a) Documentos físicos e digitais;

b) Dados em trânsito ou armazenados em dispositivos;

c) Sistemas de informação e redes do LNCC;

d) Equipamentos eletrônicos e dispositivos de armazenamento;

e) Informações verbais em reuniões, discussões ou interações internas e externas;

f) Serviços de terceiros que tenham acesso às informações do LNCC.

3 Responsabilidade

A responsabilidade pela elaboração, revisão e publicação desta norma é do Gestor de Segurança da Informação.

A responsabilidade pela aprovação e cancelamento desta norma é do Diretor do LNCC.

O gestor de segurança da informação e o comitê de segurança da informação são os responsáveis por avaliar a eficácia e a eficiência dos controles da política.

O gestor de segurança periodicamente deve conscientizar os colaboradores e outras partes interessadas sobre os controles contidos nesta política.

Para avaliar eficácia e a eficiência dos controles de segurança relacionados a classificação e tratamento das informações, o gestor deve acompanhar o monitoramento da ocorrência de eventos de segurança envolvendo a rotulagem e a classificação das informações no contexto do LNCC.

Os proprietários de informações e dos respectivos ativos são os responsáveis pela sua classificação e por garantir a aplicação desta política.

Os gestores devem garantir que as informações de suas áreas sejam corretamente classificadas e rotuladas. Assim como, devem monitorar o cumprimento da política em suas respectivas equipes.

Os colaboradores devem seguir as diretrizes de classificação e proteção da informação, garantindo o tratamento adequado conforme os níveis de classificação. Assim como, devem reportar quaisquer não conformidades com a política.

A Equipe de Segurança da Informação é a responsável por monitorar e auditar a conformidade com esta política.

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	Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos
ABNT NBR ISO/IEC 27002	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	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
Lei Geral de Proteção de Dados (LGPD)	Lei nº 13.709/2018
Lei de Acesso à Informação (LAI)	Lei nº 12.527/2011

Devem ser utilizadas, ainda, as instruções normativas e normas complementares relacionadas à segurança da informação, publicadas pelo Gabinete de Segurança Institucional da Presidência da República.

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

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, 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.

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.
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 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 de 2025. Após essa data os processos, procedimentos e os documentos que não tenham sido adequados à presente norma serão considerados não conformes com relação aos requisitos.

9 Diretrizes gerais de classificação

9.1 As informações no LNCC serão classificadas de acordo com o nível de sensibilidade e o impacto potencial no LNCC em caso de divulgação não autorizada, modificação ou destruição.

9.2 Ao classificar as informações deve-se levar em consideração as seguintes características:

a) **Confidencialidade**: indica o grau de severidade caso a informação seja revelada à pessoa, sistema, órgão ou entidade não autorizados nem credenciados. Relacionada a proteção contra acesso não autorizado.

b) **Integridade**: indica o grau de severidade caso a informação seja modificada ou destruída de maneira não autorizada ou acidental. Proteção contra alterações não autorizadas.

c) **Disponibilidade**: indica o grau de severidade caso a informação não esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados. Garantia de que a informação está acessível e utilizável sob demanda.

d) **Autenticidade**: indica o grau de severidade caso a informação não tenha sido produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade. Garantia de que a informação é genuína e provém de uma fonte confiável.

e) **Privacidade**: indica o nível de severidade à privacidade no caso de vazamento de dados de pessoas naturais. Proteção dos dados pessoais conforme a LGPD.

9.3 As classificações e os controles de proteção associados às informações devem levar em consideração as necessidades de negócios para compartilhá-las ou restringi-las, assim como para proteger a integridade das informações e para assegurar a disponibilidade, bem como os requisitos legais relativos as características apontadas no controle 9.1.

9.4 Os demais ativos também poderão ser classificados em conformidade com a classificação das informações que são armazenadas, processadas, manuseadas ou protegidas por ele.

9.5 As informações e os respectivos ativos devem ser classificadas pelos seus proprietários.

9.6 Recomenda-se que o processo inicial de classificação ocorra quando do mapeamento da informação e do respectivo ativo associado.

9.7 As informações devem ser revisadas periodicamente para garantir que a classificação permaneça adequada. Alterações no nível de sensibilidade devem ser refletidas nas classificações.

9.8 Recomenda-se o processo de análise crítica da classificação das informações e os respectivos ativos atendam aos seguintes critérios:

a) a cada 12 meses;

b) quando ocorre da mudança nos critérios de classificação apontados nesta norma;

c) quando do processo de avaliação de riscos;

d) quando das lições apreendidas;

e) quando de eventos ou incidentes de segurança;

f) quando de mudanças na legislação;

g) quando de mudanças nas necessidades de negócio;

h) de acordo com as alterações do valor, sensibilidade e criticidade das informações ao longo de seu ciclo de vida.

9.9 Os controles de acessos, incluindo qualquer política ou procedimento, implementados pelo LNCC devem estar alinhados com o esquema de classificação desta política.

9.10 Recomenda-se que os acordos de compartilhamento de informações com outras organizações incluam um procedimento para identificar e classificação destas informações e para realizar a intepretação dos níveis de classificação adotados fora do LNCC.

9.11 Convém que a correspondência entre diferentes esquemas de classificação seja buscada com base na equivalência dos métodos de manuseio e proteção associados.

9.12 Sempre que possível as informações com necessidades de proteção semelhantes devem ser associadas a "grupos" específicos. A estes grupos pode-se especificar procedimentos de segurança específicos, reduzindo a necessidade da avaliação de risco caso a caso.

9.13 A sensibilidade, ou criticidade, de algumas informações podem mudar com o passar do tempo, em decorrência ou não do seu ciclo de vida. Convém que a mudança na sensibilidade em uma de suas características seja levada em consideração para evitar uma superclassificação ou uma subclassificação.

10 Categorias de classificação

10.1 As informações devem ser classificadas com base nas características abaixo, cada uma dividida em cinco níveis de criticidade.

10.2 Quanto à Confidencialidade

Escala	Rotulo	Impacto	Parâmetros para avaliação do nível de impacto
[1]	Publica – Externa	Muito Baixo	Informações destinadas a serem amplamente divulgadas, sem necessidade de controle de acesso.
			Acesso irrestrito, pode ser divulgado sem prejuízo.
			Exemplo: Relatórios anuais, políticas públicas.
[2]	Pública – Interna	Baixo	Informações destinadas a serem divulgadas interna, sem necessidade de controle de acesso. Comunicados de imprensa, informações de marketing.
			Exemplo: políticas internas cujos conteúdo seja de interesse de grupos específicos. Procedimentos operacionais. Políticas internas, manuais de funcionários.
[3]	Restrita ou Reservada	Moderado	Informações que devem ser acessadas apenas por grupos específicos.
			Informações destinadas ao uso interno da organização, com acesso restrito a alguns colaboradores
			Prazo de sigilo: 5 anos, sem possibilidade de prorrogação.
			Motivos: • Prejudicar investigações em andamento. • Comprometer atividades administrativas sensíveis.
			Exemplo: Documentos internos da organização utilizados para tomada de decisão. Relatórios financeiros internos, planos de negócios.
[4]	Secreta	Alto	Informações sensíveis cujo acesso é limitado a pessoas autorizadas.
			Prazo de sigilo: 15 anos, sem possibilidade de prorrogação.
			Motivos: • Prejudicar a condução de negociações diplomáticas. • Comprometer atividades de inteligência ou segurança nacional.
			Exemplo: Dados financeiros, estratégias corporativas.
[5]	Ultrasecreta	Muito Alto	Informações altamente sensíveis, com acesso rigorosamente controlado.
			Prazo de sigilo: 25 anos, prorrogável uma vez por igual período.
			Motivos: • Ameaçar a soberania nacional. • Prejudicar as relações internacionais. • Pôr em risco a segurança do Estado ou de seus cidadãos em situações críticas.
			Exemplo: Dados de segurança nacional ou protótipos confidenciais. Segredos comerciais, informações de propriedade intelectual.

10.2.1. O processo de classificação deve ser formal, com a devida justificativa, indicando os critérios utilizados para atribuir o grau de sigilo.

10.2.2. Após o vencimento do prazo de sigilo, a informação deve ser automaticamente tornada pública, salvo exceções previstas na legislação.

10.2.3. O acesso a informações classificadas como sigilosas pode ser restrito às pessoas autorizadas, de acordo com o nível de classificação.

10.2.4. A autoridade que classificar a informação deve assegurar a revisão da necessidade do sigilo, em conformidade com os prazos e legislações aplicáveis.

10.3 Quanto à Integridade

Escala	Rotulo	Impacto	Parâmetros para avaliação do nível de impacto
[1]	Não Crítico	Muito Baixo	Informação que pode sofrer alterações sem impacto significativo.
			Alterações não comprometem o uso.
			Exemplos: Rascunhos de documentos, notas de reuniões. Modelos de apresentações padrão; listas de eventos antigos.
[2]	Baixo	Baixo	Alterações podem causar erros ou retrabalho.
			Informação que deve ser protegida contra alterações não autorizadas.
			Exemplos: Relatórios de status, planilhas de trabalho.
[3]	Moderado	Moderado	Alterações afetam a precisão operacional
			Informação que deve ser rigorosamente protegida contra alterações
			Exemplos: Registros financeiros, dados de inventário.
[4]	Alto	Alto	Qualquer alteração compromete a processos específicos.
			Informação que não pode sofrer nenhuma alteração
			Exemplos: Registros de auditoria, logs de segurança.
[5]	Muito Alto	Muito Alto	Qualquer alteração compromete a organização.
			Informação que deve ser protegida contra qualquer tipo de alteração, com múltiplos níveis de verificação.
			Exemplos: Dados de pesquisa científica, registros de transações bancárias.

10.4 Quanto a Disponibilidade

Escala	Rotulo	Impacto	Parâmetros para avaliação do nível de impacto
[1]	Não Crítico	Muito Baixo	Informação que pode sofrer interrupções prolongadas.
			Informação que pode ter interrupções sem impacto significativo.
			Exemplos: Informações de eventos passados, arquivos de backup. Informações históricas de vendas; dados de antigos fornecedores não mais utilizados.
[2]	Baixo	Baixo	Deve estar disponível em até 48 horas.
			Informação que deve estar disponível durante o horário comercial.
			Exemplos: documentos de projeto. Relatórios gerenciais trimestrais; cronogramas de reuniões recorrentes.
[3]	Moderado	Moderado	Disponibilidade necessária em até 24 horas
			Informação que deve estar disponível 24/7 com tolerância mínima a interrupções.
			Exemplos: Sistemas de CRM, bases de dados de clientes.
[4]	Alto	Alto	Indisponibilidade impacta significativamente a operação.
			Informação que deve estar disponível 24/7 sem tolerância a interrupções.
			Exemplos: Sistemas de pagamento online, plataformas de e-commerce. Informações de inventário em tempo real; sistema de ERP para controle de produção.
[5]	Muito Alto	Muito Alto	Necessidade de disponibilidade imediata e contínua.
			Informação que deve estar disponível 24/7 com redundância total e sem tolerância a interrupções.
			Exemplos: Redes de telecomunicações. Sistemas de pagamento online; bases de dados de clientes em e-commerces.

10.5 Quanto a Autenticidade

Escala	Rotulo	Impacto	Parâmetros para avaliação do nível de impacto
[1]	Não verificada	Muito Baixo	Informação de origem ou autoria incerta.
			Informação com baixa necessidade de verificação de autenticidade.
			Exemplos: Boatos recebidos de fontes externas; comentários em redes sociais. Informações de contato público, horários de funcionamento.
[2]	Verificada	Baixo	Informação com evidência mínima de autenticidade.

			Informação que requer verificação básica de autenticidade.
			Exemplos: Notícias públicas confirmadas por sites confiáveis; e-mails internos com remetentes conhecidos. E-mails internos, documentos de trabalho.
[3]	Garantida	Moderado	Verificada por fontes confiáveis internas.
			Informação que requer verificação rigorosa de autenticidade.
			Exemplos: Relatórios assinados por gestores; documentos gerados automaticamente por sistemas internos. Relatórios de auditoria, registros de transações.
[4]	Certificada	Alto	Validada por mecanismos externos ou padrões.
			Informação que requer verificação contínua e rigorosa de autenticidade.
			Exemplos: Contratos assinados digitalmente; relatórios fiscais auditados. Documentos legais, registros médicos.
[5]	Auditorada	Muito Alto	Revisada e garantida por auditoria independente.
			Informação que requer verificação contínua, rigorosa e múltipla de autenticidade.
			Exemplos: Documentos financeiros revisados por auditorias externas; relatórios submetidos à Receita Federal. Documentos legais, registros médicos.

10.6 Quanto a Privacidade

Escala	Rotulo	Impacto	Parâmetros para avaliação do nível de impacto
[1]	Dados não pessoais	Muito Baixo	Informações não associadas a pessoa natural
			Informação que não identifica indivíduos.
			Informações anonimizadas
			Exemplos: lista de itens adquiridos em uma contratação, identificação do órgão
[2]	Pseudonimizado	Baixo	Identificação indireta é possível com esforço
			Exemplos: 123.xxx.xxx.89
[3]	Dados Pessoais	Moderado	Dados que identificam diretamente pessoas
			Exemplos: Nome, endereço, e-mail, número de telefone, CPF, dados de localização
[4]	Sensíveis	Alto	Dados protegidos por lei, como saúde e biometria
			Exemplos: Dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.
[5]	Desconhecido	Muito Alto	Quando não é possivel identificar claramente a existência de dados pessoais, ou quando o mapeamento ainda não foi realizado
			Exemplos: quando não há informações sobre o mapeamento.

11 Diretrizes de tratamento das informações

11.1 Convém aos proprietários criar, gerir e avaliar critérios de tratamento da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

11.2 É vedado comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pelo LNCC.

11.3 Quando documentos relacionados à segurança da informação, como as políticas, as normas e os procedimentos, forem disponibilizados para acesso externo, deve-se assegurar a proteção de informações confidenciais ou restritas.

12 Diretrizes de rotulagem

12.1 Os procedimentos de rotulagem devem estar de acordo com o esquema de classificação da informação e dos ativos associados.

12.2 Os procedimentos de rotulagem devem facilitar a comunicação da informação e apoiar a gestão e tratamento das informações.

12.3 Os procedimentos de rotulagem devem abranger todos os formatos que as informações possam assumir.

12.4 Os procedimentos devem orientar como e onde as etiquetas devem ser anexadas. Deve-se levar em consideração o tipo de mídia, assim como as informações são acessadas e como os ativos são tratados.

12.5 Recomenda-se que os procedimentos definam:

a) Casos em que a rotulagem é omitida;

b) Como rotular informações enviadas ou armazenadas em meios físicos, eletrônico e qualquer outro formato;

c) Como lidar com casos em que a rotulagem não é possível (restrições técnicas).

12.6 Recomenda-se que sejam adotados ao menos as seguintes técnicas de rotulagem:

a) Rótulos físicos;

b) Cabeçalhos e rodapés;

c) Metadados;

d) Marca d´água;

e) Carimbos de borracha.

12.7 Recomenda-se o uso de metadados para identificar, gerenciar e controlar as informações digitais, especialmente quanto a confidencialidade.

12.8 Quanto ao uso de metadados, recomenda-se:

a) que permitam a realiza de buscas eficiente e correta das informações;

b) que facilitem aos sistemas a interação e a tomada de decisões;

c) que os procedimentos descrevam como os metadados devem ser anexados e quais rótulos devem ser utilizados.

12.9 Os colaboradores e demais partes interessadas devem receber treinamento para assegurar que as informações estão sendo rotuladas e tratadas corretamente.

13 Diretrizes Gerais de transferência de Informações

13.1 Devem ser definidas regras, procedimentos e acordos de transferência de informações para todos os tipos de recursos de transferência dentro do LNCC e com outras partes. Os controles devem levar em consideração que as transferências podem ocorrer de forma eletrônica, através de uma mídia de armazenamento físico e de forma verbal.

13.2 As regras, procedimentos e acordos de transferência devem estar alinhados com a classificação das informações envolvidas.

13.3 Quando da transferência de informações entre o LNCC e terceiros, acordos devem ser estabelecidos.

13.4 Convém que para todos os tipos de transferência sejam definidos controles:

a) para proteger as informações contra interceptação, acesso não autorizado, cópia, modificação, desvio, destruição e negação de serviço, incluindo níveis de controle de acesso proporcionais à classificação das informações envolvidas;

b) para assegurar a rastreabilidade e não repúdio, incluindo a manutenção de uma cadeia de custódia de informações durante o trânsito;

c) para identificação de contatos apropriados relacionados à transferência, incluindo proprietários de informações, proprietários de riscos, agentes de segurança e custodiantes de informações, conforme aplicável;

d) para definição de responsabilidades, incluindo responsabilidade em caso de incidentes de segurança da informação;

e) para o uso de um sistema de rotulagem;

f) para promover a confiabilidade e disponibilidade do serviço de transferência;

g) para a política sobre o uso aceitável de recursos de transferência de informações;

h) com as diretrizes de retenção e descarte para todos os registros;

i) consideração de quaisquer outros requisitos legais, estatutários, regulamentares e contratuais relevantes.

14 Diretrizes para transferência eletrônica

14.1 Quando da transferência eletrônica devem ser considerados controles para:

a) detecção e proteção contra malware;

b) proteção de informações eletrônicas sensíveis comunicadas que estão na forma de um anexo;

c) prevenção contra o envio de documentos e mensagens para destinos incorretos;

d) obtenção de aprovação antes do uso de serviços públicos externos;

e) autenticação ao transferir informações através de redes de acesso público;

f) aconselhamento de pessoal e outras partes interessadas a não enviar SMS ou mensagens instantâneas com informações críticas;

g) aconselhamento de pessoal e outras partes interessadas sobre os problemas de uso de máquinas de fax.

15 Diretrizes para transferência de mídias

15.1 Quando da transferência de mídia de armazenamento físico, incluindo papel, devem ser considerados controles para:

a) definir responsabilidades pelo controle e notificação da transmissão, expedição e recebimento das informações;

b) assegurar o endereçamento e o transporte corretos das informações;

c) proteção do conteúdo de qualquer dano físico que possa ocorrer durante o trânsito. Deve-se levar em consideração: as especificações de qualquer fabricante, a proteção contra fatores ambientais, como exposição ao calor, umidade ou campo eletromagnéticos;

d) determinar a lista de serviços postais confiáveis autorizados;

e) verificar a identificação dos entregadores;

f) determinar a lista aprovada de terceiros que fornecem serviços de transporte ou postal, dependendo da classificação das informações.

15.2 Deve-se prover a manutenção de registros para:

a) identificação do conteúdo dos meios de armazenamento;

b) proteção aplicada;

c) lista de destinatários autorizados;

d) os horários de transferência para os custodiantes de trânsito e o recebimento no destino.

16 Diretrizes para transferência verbal

16.1 Quando da transferência verbal de informações, os colaboradores e outras partes interessadas devem observar os seguintes controles:

a) não ter conversas verbais envolvendo dados confidenciais em locais públicos ou por canais de comunicação inseguros;

b) não deixar mensagens contendo informações confidenciais em secretárias eletrônicas ou mensagens de voz;

c) assegurar que os controles apropriados de sala sejam implementados, por exemplo manter a porta fechada;

d) iniciar quaisquer conversas sensíveis com um aviso para que os presentes saibam o nível de classificação e quaisquer requisitos de tratamento do que estão prestes a ouvir.

17 Casos omissos

17.1 Casos específicos, como exigências legais, podem demandar exceções, que devem ser documentadas.

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

18 Análise crítica

18.1 Este documento deve ser analisado criticamente, quanto à sua eficácia e adequação ao SGSI do LNCC, sempre que necessário, ao menos, uma vez ao ano.

18.2 O processo de análise crítica deve incluir a avaliação de oportunidade de melhoria.

18.3 O processo de análise crítica deve estar apto a responder às mudanças no seguinte:

a) estratégia de negócios do LNCC;

b) ambiente técnico do LNCC;

c) regulamentos, estatutos, legislação e contratos;

d) riscos à segurança da informação;

e) ambiente atual e projetado de ameaça à segurança da informação;

f) lições aprendidas com eventos e incidentes de segurança da informação.

19 Histórico da revisão e quadro de aprovação

Revisão	Data	Itens Revisados
1.0	30/01/2025	Versão Original
1.1	13/08/2025	Atualização do cabeçalho

Quadro de Aprovação		
	Nome	**Atribuição**
Elaborado por:	Luís 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:	Fábio Borges de Oliveira	Diretor do LNCC

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