POLÍTICA

POL-SG002-2019

Política Pública de Segurança da Informação e Cibernética

Objetivo: Estabelecer diretrizes, objetivos de segurança da informação e segurança cibernética apropriadas ao contexto de negócios, protegendo as informações da Núclea, seus riscos inerentes, e em acordo com a Missão, Visão e Valores da Núclea. Além disso, essa política aborda também os processos gerenciados por segurança da informação, papéis e responsabilidades.

Autor do documento: Segurança da Informação e Resiliência Cibernética (SIRC).

Contato: SIRC.

Público-alvo: A presente Política deve ser observada pela Núclea, pelos membros do seu Conselho de Administração, da sua Diretoria Executiva, dos seus Comitês de Assessoramento, do seu Conselho Fiscal, caso instalado, e por todos os seus funcionários, estagiários e terceiros abrangendo todas as áreas da Companhia.

O responsável deve ser contatado nos casos de:

- Dúvidas sobre as informações tratadas neste documento;
- Falhas ou vulnerabilidades encontradas no processo;
- Necessidade de adequação identificada internamente, ou apresentada por auditoria, por órgão regulador, ou por cliente.

Sumário

1. OBJETIVO

Estabelecer diretrizes e objetivos de segurança da informação e segurança cibernética apropriadas ao contexto de negócios, protegendo as informações da Núclea, seus riscos inerentes, e em acordo com a Missão, Visão e Valores da Núclea. Além disso, essa política aborda também os processos gerenciados por segurança da informação, papéis e responsabilidades.

2. DIVULGAÇÃO

Este documento pode ser encontrado em:

- Portal Corporativo da Núclea (*intranet*); e
- Site da Núclea.

3. VIGÊNCIA

Este normativo deverá ser revisto quando do vencimento de sua vigência, ou quando necessário.

4. PROCESSO DE REFERÊNCIA

- Gerir Segurança da Informação e Continuidade de Negócios.

5. DOCUMENTOS COMPLEMENTARES APLICÁVEIS

- Externos mandatórios:
    - Lei Geral de Proteção de Dados Pessoais - LEI Nº 13.709
    - Resolução BCB nº 304/23

- Boas práticas:
    - Norma ISO/IEC 27001
    - Norma ISO/IEC 27002
    - COBIT *for Information Security*
    - CIS *Critical Security Controls*
    - AWS *Best Practices*
    - *NIST AI RMF, CSF, SP-800-53*
    - OPEN CSIRT SIM3
    - Resolução CMN Nº 4.893, de 26 de fevereiro de 2021
    - Resolução CVM Nº 35 , de 26 de maio de 2021
    - SUSEP Nº 638, de 27 de julho de 2021

- Demais documentos internos restritos (normativos e manuais) também fazem parte dos documentos aplicáveis como referência.

6. DEFINIÇÕES:

Cadeia de Suprimentos: Cadeia de suprimentos tem início no processo de aquisição de serviços ou soluções de fornecedores e se estende a todos os processos de segurança aplicáveis aquele serviço ou solução requerido para o fornecedor.

Gerenciamento de crise: Crise é um período de incerteza ocasionado pelo aparecimento de um problema ou incidente com forte impacto nas operações de negócio. O gerenciamento de crise envolve: resposta à crise, ativação dos planos de Continuidade de Negócios, monitoramento e encerramento, não se limitando a apenas esses processos.

***ISO* 27.001:** Padrão para sistema de gestão da segurança da informação publicado pelo *International Organization for Standardization* e pelo *International Electrotechnical Commission*.

***ISO* 22.301:** Uma norma de sistema de gestão publicada pelo *International Organization for Standardization* que especifica requisitos para planejar, estabelecer, implementar, operar, monitorar, revisar, manter e melhorar continuamente um sistema de gestão documentado para proteger contra a probabilidade de ocorrência, preparar-se para responder a, e a recuperar-se de incidentes disruptivos quando surgirem.

Incidente de Segurança da Informação: Um evento de segurança da informação, incluindo cibernético que foi determinado como tendo um impacto na organização, levando à necessidade de resposta e recuperação.

Plano de Continuidade de Negócios: Baseado nos cenários de riscos de indisponibilidade, o plano de continuidade de negócios considera a preservação e a manutenção do ambiente dos sistemas de negócio em caráter contínuo, bem como do processamento dos sistemas internos da Núclea, determinando a necessidade de redundância de ambiente tecnológico e documentação de procedimentos específicos que assegurem a continuidade destas operações.

Risco de segurança da informação/ cibernético: São eventos que, uma vez materializados, podem afetar o cumprimento dos objetivos de segurança da informação. Os riscos podem ser caracterizados por suas causas, consequências ou uma combinação destes.

Resiliência Cibernética: Capacidade de um sistema em se adaptar ou resistir, recuperar em eventuais falhas mantendo as funções operacionais, adotando uma abordagem proativa para garantir a continuidade dos negócios.

Segurança da Informação/Cibernética: Preserva a confidencialidade, a integridade e a disponibilidade das informações em meios físicos e lógicos, por meio da aplicação de tecnologia, processos e pessoas.

Notebook corporativo (baremetal): Notebook corporativo projetado especificamente para fornecer um ambiente seguro de acesso às aplicações internas da Núclea.

Sistema de Inteligência Artificial (AI): Sistema projetado ou baseado em máquina que pode, para um determinado conjunto de objetivos, gerar resultados como previsões, recomendações ou decisões que influenciam ambientes reais ou virtuais. Os sistemas de IA são projetados para operar com diferentes níveis de autonomia.

7. OBJETIVOS DA SEGURANÇA CIBERNÉTICA E INFORMÁTICA

7.1 A SEGURANÇA CIBERNÉTICA E INFORMÁTICA VISA ATINGIR OS SEGUINTES OBJETIVOS

Os objetivos de SIRC foram definidos para suportar os objetivos estratégicos da Núclea e manter a segurança operacional, a qualidade dos serviços entregues, o atendimento ao mercado com excelência, a disponibilidade dos serviços e a proteção de dados pessoais e dados pessoais sensíveis em seu tratamento.

7.2 APROVAÇÃO E COMUNICAÇÃO DA POLÍTICA

O fluxo de aprovação desta política encontra-se assim configurado: (1) apreciação da Diretoria da Núclea, (2) avaliação, análise e recomendação da 2ª linha representado pela Diretoria de Riscos, Controles Internos e *Compliance*; (3) avaliação, análise e recomendação do Comitê de Riscos, Controles Internos e *Compliance* e por fim (4) deliberação pelo Conselho de Administração.

Devem estar em conformidade com esta política os funcionários, estagiários, clientes, prestadores de serviços e fornecedores[1].

Nota[1]: As partes externas podem ter acesso aos requisitos desta Política sendo de responsabilidade da Núclea exigir os cumprimentos dessas diretrizes através de cláusulas contratuais, acordos e mecanismos técnicos se aplicável.

8. DISPOSIÇÕES GERAIS

Para assegurar que as informações tratadas estejam adequadamente protegidas, a Núclea adota processos baseados em leis, resoluções e diferentes práticas do mercado, conforme apresentado no "item 5 Documentos complementares aplicáveis.

A Núclea estabeleceu as diretrizes e as responsabilidades no gerenciamento de riscos corporativos, considerando a implantação e a manutenção do ambiente de controles necessário para apoiar a tomada de decisão e o cumprimento dos objetivos da Núclea, mantendo o nível dos riscos alinhados ao apetite, à missão, à visão e aos valores da Núclea.

Para adoção segura de Sistemas de Inteligência Artificial, as diretrizes e os requisitos a serem seguidas por toda organização, bem como os papeis e responsabilidades considerando o ciclo de vida de um Sistema de IA, estão estabelecidas na Instrução Normativa de Desenvolvimento e Uso de Inteligência Artificial Generativa.

8.1. PAPEIS E RESPONSABILIDADES

É papel de todos:

- Promover e manter sólida cultura em segurança cibernética e privacidade, apoiando as ações de conscientização; incentivar o contínuo aprimoramento dos processos para mitigação dos riscos de vazamento de informações para que a gestão da segurança cibernética e de privacidade tenha eficácia.
- Ter ciência e cumprir todas as diretrizes descritas nesta política e demais documentos relacionados (termos de responsabilidade, acordo de confidencialidade, contratos etc.).

- Manter a conformidade com as diretrizes da Política de Trabalho Remoto da Núclea ficando permitido a condução de reuniões que tratem de informações internas e confidenciais da empresa somente em ambientes reservados.

Segurança da Informação e Resiliência Cibernética (SIRC):

- A Diretoria de SIRC deve elaborar um Programa de Segurança que contemple a estratégia, o orçamento e recursos humanos, bem como garantir a sua implementação para atendimento aos objetivos propostos, dar suporte, supervisionar, monitorar e comunicar os resultados obtidos.

- Submeter o Programa de Segurança e a Política de Segurança da Informação e Cibernética, quando houver atualização, para aprovação da Diretoria e Conselho de Administração, e referendo da 2ª linha e Comitê de Riscos, Controles Internos e *Compliance*.

- Quando da contratação de serviços relevantes de processamento e armazenamento de dados, verificar a capacidade do prestador de serviços em garantir diversos aspectos. Entre eles, destacam-se: a) assegurar o acesso da instituição aos dados e informações a serem processados ou armazenados pelo prestador de serviço; b) garantir a confidencialidade, integridade, disponibilidade e recuperação dos dados e informações processados ou armazenados; c) verificar a conformidade do prestador de serviço com as certificações exigidas pela instituição para a prestação do serviço contratado; d) realizar a identificação e segregação dos dados dos participantes por meio de controles físicos ou lógicos; e) garantir a qualidade dos controles de acesso direcionados à proteção dos dados e informações dos clientes.

Segunda Linha:

- Revisar a Política de Segurança da Informação e Cibernética, o Programa de Segurança, e emitir o parecer no Comitê de Riscos, Controles Internos e *Compliance*.

Diretoria:

- Aprovar a estratégia de segurança cibernética, definida no Programa de Segurança, zelar e supervisionar pelo seu cumprimento, incluindo a efetividade do ambiente de controles e implementar as recomendações do Conselho de Administração.

Conselho de Administração:

- Estabelecer diretrizes, apetite e tolerância, estabelecer o comprometimento da liderança e a cultura do risco cibernético, e alinhar estratégia com as práticas de segurança da informação.

Auditoria Interna (Terceira Linha):

- Atividade independente e objetiva, desenhada para proteger, adicionar valor e melhorar as operações da Núclea. A Auditoria Interna auxilia a Núclea a atingir seus objetivos por meio da avaliação e aprimoramento da eficácia do gerenciamento de riscos, ambiente de controles e governança corporativa, considerando os riscos cibernéticos e de segurança da informação.

8.2. NORMAS GERAIS

Gestão de Demandas

A área de SIRC está presente no atendimento às *Squads*, Tribos de negócio e Áreas de Apoio da Núclea com participação ativa nas cerimônias de alinhamento ágil para entendimento e captura de novas demandas.

As demandas e novas iniciativas, como projetos e aquisições, são prontamente avaliadas para priorização, análise dos riscos relacionados e definição dos requisitos de segurança para as informações.

Gestão de Requisitos

Os controles mínimos necessários (arquitetura e requisitos) para mitigação dos riscos relacionados à segurança da informação dos sistemas que suportam os negócios da Núclea foram definidos e catalogados, inclusive para suportar o gerenciamento de segurança em tempo de projeto. A Núclea mantém um conjunto de práticas e requisitos (*framework*) para a aquisição de infraestrutura, *software* e processamento de dados, incluindo ambiente computacional em nuvem.

Os requisitos são revisados periodicamente garantindo alinhamento constante com as melhores práticas e necessidades de proteção dos dados e ativos institucionais.

A Inteligência Artificial e *Machine Learning* devem permitir ganhos de eficiência operacional para a organização. Uma vez comprovada sua eficácia, a utilização dessas tecnologias estará restrita, desde que sejam avaliados os potenciais riscos para a segurança das informações e mitigados os eventuais impactos na operação da Núclea.

Aquisição

A Núclea estabeleceu em seu processo de Compras critérios de segurança para avaliação e homologação de fornecedores para gerenciamento dos riscos relacionados na Cadeia de Suprimentos.

Desenvolvimento Seguro

A Núclea estabeleceu um conjunto de princípios para projetar sistemas seguros, incluindo Sistemas de IA, a fim de que a segurança cibernética seja implementada no ciclo de vida de desenvolvimento dos sistemas, considerando a privacidade desde sua concepção por meio do processo de s*ecurity* e *privacy by design*. Controles foram adotados para avaliação automática de segurança em código-fonte e os resultados integrados à gestão de riscos corporativo da Núclea.

Gestão da Qualidade

Antes da efetiva entrada em operação, os controles de segurança que sustentam os sistemas de negócios e corporativos são avaliados adequadamente, inclusive por empresas independentes, para evitar falhas, brechas ou vulnerabilidades conhecidas.

Capacidade e Disponibilidade

As diretrizes para gerenciamento da capacidade e disponibilidade dos sistemas que suportam as operações da Núclea foram estabelecidas para adequada projeção de volumes, dimensionamento e acompanhamento da infraestrutura tecnológica.

Gestão de Mudanças

O processo de Gestão de Mudanças da Núclea mantém controles específicos para avaliação dos aspectos de segurança da informação antes da efetiva autorização de mudanças para ambiente produtivo.

Gestão de Certificados

Sempre que possível, as transmissões de dados sensíveis ou confidenciais da Núclea devem ser criptografadas e autenticadas com o uso de certificados digitais. Controles são adotados para armazenamento, validação e vigência dos certificados digitais.

Prevenção de Vazamento de Dados

A classificação quanto a confidencialidade e privacidade das informações é adotada na Núclea em conjunto com controles automáticos de prevenção de perda de dados, visando minimizar a exposição da organização em decorrência de vazamento de informações internas e confidenciais.

Os controles estão estabelecidos para guarda, retenção e descarte das informações da Núclea, inclusive dados pessoais, conforme exigências legais, internas e externas.

Gestão de Ameaças

O processo de gerenciamento de ameaças (*threat intelligence*) adotado pela Núclea visa assegurar que as ameaças (ex.: vírus, *malware*, conteúdo *web*) de segurança cibernética, incluindo monitoramento da logomarca, sejam prontamente identificadas e compartilhadas com órgãos competentes, e que ações de proteção sejam estabelecidas em tempo hábil.

Segurança de Rede e Conectividade

Os perímetros dos sistemas que sustentam os negócios e operações da Núclea são segregados por redes lógicas compostas por dispositivos de monitoração, filtro de acessos, detecção e prevenção a intrusões.

Segurança *Endpoint*

Os dispositivos (*hardware* e *software*) são homologados e configurados de forma segura antes de sua plena utilização de forma corporativa. O uso correto e autorizado de dispositivos móveis nas atividades de trabalho, no formato de Notebook corporativo (*baremetal*), VDI (*Virtual Desktop Interface*) e *BYOD* (*Bring Your Own Device*), minimiza a exposição da Núclea aos riscos e possíveis danos (perda de informação

confidencial, de propriedade intelectual, danos à imagem e sistemas internos etc.), além de manter a conformidade com os requisitos legais vigentes.

Gestão de Vulnerabilidades

A Núclea estabeleceu um processo para gestão de vulnerabilidades do seu ambiente tecnológico com objetivo de identificar periodicamente, avaliar e corrigir tempestivamente junto aos responsáveis da organização, eventuais brechas, falhas, recursos de segurança desatualizadas (*patches*) e vulnerabilidades conhecidas.

Um programa de divulgação de vulnerabilidades está estabelecido para que qualquer pessoa externa possa reportar uma fragilidade de segurança à Núclea a partir do portal institucional público.

Gestão de Identidades e Acessos Lógicos

A Gestão da Identidade aos sistemas, recursos e serviços tecnológicos da Núclea é conduzida por meio de *logins* únicos e intransferíveis. Os privilégios e funções são atribuídos aos usuários sistêmicos considerando o mínimo necessário para desempenho das atividades.

O processo de Gestão de Acessos contempla controles com alçadas para concessão, autorização, revogação, bloqueio e revisão dos acessos aos sistemas e ambiente de rede da Núclea. O acesso aos sistemas, incluindo acesso remoto às redes corporativas e recursos proprietários da Núclea é gerenciado por camadas e mecanismos para identificação, autenticação e autorização dos usuários.

Gestão de Acessos Físicos

A Núclea mantém um conjunto de boas práticas para zelar pelo acesso físico de seus escritórios e *data-center*s. Controles foram estabelecidos para concessão, revogação, bloqueio e revisão dos acessos físicos, incluindo a monitoração por circuito interno de TV (CFTV) e gravação das imagens na Núclea.

Gestão de Ativos

Os ativos são inventariados e classificados de acordo com a relevância para os negócios e gerenciados durante o ciclo de vida desde a sua aquisição, manutenção e descarte.

Gerenciamento e Correlacionamento de Eventos de Segurança

O processo de gerenciamento e correlacionamento dos eventos de segurança contempla a coleta, centralização e integração de diferentes fontes de dados, normalização e adequado armazenamento seguro das trilhas de auditoria dos sistemas relevantes da Núclea, possibilitando a rastreabilidade e análise tempestiva de ameaças e incidentes, fornecendo inteligência de segurança por meio de alertas, relatórios e *dashboards*.

As trilhas de auditoria contempladas nesse processo tratam especificamente dos eventos referente a segurança das informações e devem ser retidas pelo período mínimo de um ano.

Gestão de Incidentes de Segurança

A Núclea mantém o canal interno ABUSE "**abuse@nuclea.com.br**" para registro e reporte de eventos de segurança. O Centro de Resposta a Incidentes de Segurança Cibernética **"csirt@nuclea.com.br"** é o ponto de referência externo para comunicação de incidentes de segurança.

A gestão de incidentes de segurança conta com controles e procedimentos adequados para identificação, detecção e respostas. Os eventos e incidentes são classificados e priorizados de acordo com critérios estabelecidos e as respostas conduzidas por protocolos específicos de acordo com os cenários identificados.

Cláusulas contratuais são estabelecidas com os fornecedores e terceiros, englobando o processo de prevenção e reporte a incidentes de segurança da informação à Núclea, para registro, tratativa, impacto e controle de resposta a incidentes de forma tempestiva.

Gestão da Continuidade e Crises

A estratégia de continuidade de negócios tem como objetivo avaliar alternativas para assegurar a proteção dos ativos e a continuidade das operações de negócio mediante cenário de indisponibilidade causada por quaisquer tipos de riscos, inclusive físicos (muitos dos quais resultantes de mudanças climáticas). Tais riscos

são cobertos pela alocação de datacenters em áreas geográficas distintas ou contratação de serviços que garantam essa distância, visando segurança em situação de desastre climático em uma localidade não afetar outra, bem como diligência de manutenções em ferramentas que assegurem a infraestrutura crítica desses locais de processamento, além da asseguração de locais de trabalho distintos e avaliação de ameaças e vulnerabilidades do escritório corporativo.

A Continuidade de Negócios na Núclea é pautada na avaliação de impactos os seus negócios, considerando a estratégia e apetite aos riscos corporativos, com construção de estratégias, testes e planos para garantir a recuperação de processos críticos à empresa.

A Análise de Impacto ao Negócio (*BIA*) identifica dependências de recursos e fornecedores (*cloud*, *datacenters*), bem como informações relevantes para recuperação dos negócios e operação, resultando em um mapeamento de criticidade, tolerância para interrupção de negócios e seus tempos de recuperação.

Os planos de continuidade abrangem os processos manuais e sistêmicos da Núclea, além de procedimentos de repostas às crises de acordo com cenários mapeados, como recuperação de desastre, contingência operacional, crise cibernética, pandemia e epidemia, comunicação com mídia, entre outros.

O calendário anual de exercícios é definido a partir de diferentes cenários, desde indisponibilidade sistêmica até procedimentos de gestão de crises, abrangendo simulação de comunicação com mídia, Conselho de Administração, Comitês de assessoramento ao Conselho de Administração, fornecedores e parceiros estratégicos.

O compartilhamento de informações às partes interessadas sobre crises segue os procedimentos e protocolos estabelecidos pela Núclea.

Gestão de *Facilities*

A infraestrutura crítica que sustenta os ambientes computacionais da Núclea é composta por controles ambientais que visam o fornecimento contínuo de energia e refrigeração, como geradores, ar-condicionado, detectores de fumaça, controle de temperatura e umidade, alarme de incêndio e para-raios.

Treinamentos e Capacitações

A Núclea estabeleceu um Programa de Comportamento de Segurança com objetivo de promover uma cultura de segurança positiva a partir de comportamentos seguros em toda organização. Dessa forma, para lidar com os riscos de cyber causados por atividades humanas o programa foi implantado a partir dos comportamentos adequados esperados pelas pessoas que acessam o ambiente tecnológico da Núclea, e definidos uma série de indicadores para monitoração do comportamento humano. Os resultados apurados servem de reflexão para revisão do plano de treinamentos e capacitações, seu conteúdo, formatos e público-alvo que requeiram melhorias e melhor conscientização dos temas escopo. Além disso, se observada violações das normas gerais dessa política, a área de Desenvolvimento Humano é comunicada para condução do processo disciplinar formal.

O plano de treinamentos e capacitações tem como objetivo treinar e capacitar o Conselho de Administração, Comitês de Assessoramento do Conselho de Administração, os funcionários, estagiários, terceiros e parceiros ao longo do ano, conforme calendário pré-estabelecido. O conteúdo elaborado considera temas relevantes, como comportamentos seguros esperados, cuidados com a Inteligência Artificial, técnicas de ataques, proteção de dados sensíveis, fraudes cibernéticas, segurança em nuvem, cenários de *ransomware*, tendências, seguro e ameaças, *hacking tools,* novidades sobre técnicas de defesa, tendências do mercado, riscos emergentes e melhores práticas.

Gestão de Riscos na Cadeia de Suprimentos

As diretrizes estabelecidas nessa política são aplicáveis a fornecedores e parceiros, visando adequada gestão dos riscos cibernéticos na cadeia de suprimentos. Controles de segurança devem estar presentes na prestação de serviços à Núclea e serem periodicamente avaliados por SIRC, considerando também cenários de falhas de fornecedores decorrentes de mudanças climáticas, interrupções operacionais causadas por desastres naturais ou outros riscos de segurança que possam comprometer a confidencialidade, integridade e disponibilidade das informações da Núclea.

Monitoração dos objetivos táticos

O monitoramento do atendimento aos objetivos táticos de segurança é realizado por um Programa de Qualidade que tem por objetivo avaliar e monitorar por meio de indicadores o ambiente de controles internos (inclui opiniões dos órgãos de asseguração como 2ª linha, Auditoria Interna, Auditoria Externa, Órgão Certificador, Clientes e Reguladores), a eficiência dos processos de segurança e conformidade com requerimentos legais, regulatórios e contratuais**.**

Auditoria Interna

Os trabalhos de Auditoria Interna são definidos em um Plano de Auditoria com visibilidade de 3 anos. A definição do plano segue metodologia definida, baseado em riscos, orientados pelos planejamentos estratégico, tático e operacional. Esse é anualmente discutido, revisado e recomendado pelo Comitê de Auditoria para aprovação do Conselho de Administração.

9. CONTROLE DA DOCUMENTAÇÃO

9.1. HISTÓRICO DE ATUALIZAÇÃO

Versão	Rev.	Emissão	Motivo/ Descrição	Responsável	Publicação
1	0	13.02.2020	Elaboração Inicial	QSCI	13.02.2021
2	0	03.08.2020	Atualização da classificação do documento	SIRC	03.08.2021
3	0	19.10.2020	Adequação a nova versão da Política de Segurança da Informação Corporativa	SIRC	19.10.2021

Para efeito de registro, mantivemos o histórico antigo acima.

VERSÃO	REV	DATA DE PUBLICAÇÃO	MOTIVO/DESCRIÇÃO	RESPONSÁVEL	DATA DE VENCIMENTO
4	0	20.05.2021	Revisão GOV (correção erros português, formatação e/ou padronização).	SIRC	20.05.2022
5	0	06.04.2022	Revisão Periódica.	SIRC	06.04.2023
6	0	26.04.2023	Revisão Periódica. Atualização de *template* da Núclea.	SIRC	26.04.2025
7	0	04.09.2023	Revisão Extraordinária. Atualização de *template* da Núclea.	SIRC	04.09.2025
8	0	28.03.2024	Revisão periódica da Política de Segurança da Informação e adequação ao regulamento BCB nº 304/23 / revisão dos membros do Comitê de Riscos	SIRC	28.03.2025

9	0	10.03.2025	Revisão periódica da Política de Segurança da Informação.	SIRC	10.03.2026
10	0	02/04/2026	Revisão periódica da Política de Segurança da Informação.	SIRC	02/04/2027

9.2. CICLO DE REVISÃO

Este documento será revisto e atualizado quando:

- Houver solicitação de atendimento, correção ou adição de informações;
- Existir a necessidade de atender requisitos legais, boas práticas ou recomendações de auditoria;
- Existir mudança na organização que tenha impacto relevante na atividade abordada neste documento;
- No vencimento, conforme HISTÓRICO DE ATUALIZAÇÃO deste documento.

9.3. GUARDA E RETENÇÃO

As versões deste documento deverão ser armazenadas por cinco anos, após o vencimento de seu prazo de validade.

9.4. DISPONIBILIDADE DO DOCUMENTO

A última versão deste documento poderá ser obtida no Portal Corporativo e Sítio Eletrônico da Núclea:

https://www.nuclea.com.br/

9.5. CLASSIFICAÇÃO DA INFORMAÇÃO

Podem ser disseminadas dentro e fora da empresa com acesso liberado para leitura. Sua divulgação não causa qualquer dano à Núclea

NÚCLEA, São Paulo, 02 de abril de 2026.