## 1.OBJETIVO

Estabelecer as diretrizes necessárias para a proteção dos ativos de informação da M. Dias Branco, assegurando os princípios de **confidencialidade**, **integridade**, **disponibilidade** e **autenticidade.**

Formalizar o comprometimento da Alta Direção da M. Dias Branco com o Sistema de Gestão de Segurança da Informação (SGSI), promovendo diretrizes estratégicas, definindo competências e fornecendo apoio para a implementação de medidas que assegurem a proteção das informações, conforme as legislações e normas aplicáveis.

Fortalecer a cultura de segurança da informação dentro da organização, estabelecendo funções claras para todos os colaboradores, com foco na mitigação de riscos cibernéticos e outros riscos que impactem a segurança das informações, alinhando as práticas de segurança às necessidades e objetivos do negócio.

## 2.APLICAÇÃO

A todas as partes interessadas que possuam, possuíram ou venham a possuir vínculo com esta instituição, incluindo colaboradores, ex-colaboradores, prestadores de serviços, ex-prestadores de serviços e fornecedores que tenham ou venham a ter acesso às informações da M. Dias Branco, ou que utilizem recursos computacionais integrados à infraestrutura da M. Dias Branco.

## 3.GESTORES RESPONSÁVEIS

Vice-presidência de Administração, Desenvolvimento e Sustentabilidade;
Diretoria de Tecnologia da Informação;
Gerência de Segurança da Informação.

## 4.DESCRIÇÃO

### 4.1.Introdução

4.1.1.A estrutura da Política de Segurança da Informação (PSI) é composta por esta política, além de um conjunto de documentos adicionais, que possuem os seguintes objetivos:

4.1.1.1.**Política**: Contém as diretrizes de alto nível, que a M. Dias Branco incorporou à sua gestão para atendimento aos requisitos de Segurança da Informação.

4.1.1.2.**Procedimentos Operacionais**: São documentos que tem caráter normativo e especificam as tecnologias, os controles e as regras que deverão ser adotados para alcançar a estratégia definida pelas diretrizes da PSI.

4.1.1.3.**Manuais e Documentos de Instruções Operacionais**: Os Manuais detalham um determinado produto ou funcionalidade necessários para implementar os controles e tecnologias estabelecidas nos Procedimentos Operacionais. Os Documentos de Instruções Operacionais detalham as atividades, passo a passo que normalmente envolvem interações entre pessoas, processos e tecnologias.

### 4.2.Diretrizes

4.2.1.As diretrizes são a base para compor normas específicas (conforme item 4.4) e visam orientar as atividades dos usuários de acordo com princípios éticos, legais e das boas práticas de segurança da informação, são elas:

4.2.1.1.Assegurar o comprometimento da Alta Direção no processo de melhoria contínua do programa de Segurança da Informação.

4.2.1.2.Assegurar que os ativos corporativos, com potencial para armazenar ou processar dados, sejam inventariados, classificados e protegidos.

4.2.1.3.Assegurar que as informações relevantes para companhia sejam classificadas e possuam os controles de segurança de informação adequados para sua proteção.

4.2.1.4.Assegurar a implementação de controles eficazes para a segurança e o gerenciamento de identidades, acompanhando todo o ciclo de vida dos colaboradores dentro da M. Dias Branco.

4.2.1.5.Assegurar a proteção dos dados pessoais e dados pessoais sensíveis dos colaboradores, consumidores e fornecedores em todo o seu ciclo de vida, em qualquer formato de armazenamento ou suporte, tendo o mesmo nível de tratamento de informações confidenciais, preservando os princípios da Segurança da Informação e conforme as legislações vigentes.

4.2.1.6.Assegurar a implementação de controles robustos para proteger o acesso físico aos dados, dispositivos e ambientes, incluindo data centers.

4.2.1.7.Disseminar a cultura de segurança da informação na Companhia.

4.2.1.8.Assegurar estratégias com o objetivo de prevenir, detectar e reduzir vulnerabilidades relacionadas ao ambiente tecnológico.

4.2.1.9.Assegurar a gestão de incidentes de segurança por meio da implementação de controles para monitoramento contínuo de ameaças cibernéticas, detecção de eventos suspeitos, resposta estruturada e recuperação eficaz, com o objetivo de mitigar os impactos de ataques cibernéticos.

4.2.1.10.Assegurar estratégias de Continuidade de Negócios de acordo com os riscos de segurança da informação identificados, avaliados e classificados em consonância com a Política de Gestão de Continuidade de Negócios da Companhia.

4.2.1.11.Assegurar procedimentos e controles de segurança em todo ciclo de vida para aquisição e desenvolvimento de sistemas de informação, assim como a adoção de novas tecnologias empregadas nas atividades da companhia.

4.2.1.12.Compreender os riscos da Segurança da Informação associados à condução do negócio e administrar esses riscos de forma eficaz em consonância com a Política de Gerenciamento de Riscos da Companhia.

4.2.1.13.Zelar pela manutenção de relações transparentes e éticas, coibindo corrupção, fraude, suborno, favorecimento e extorsão, em conformidade com o Código de Ética da Companhia, a legislação brasileira e os regulamentos aplicáveis, de modo a alinhar-se aos princípios de segurança da informação.

4.2.1.14.Assegurar que os relacionamentos com clientes e contratações de fornecedores, prestadores de serviços e terceiros, em que ocorra o acesso ou compartilhamento de informações, sejam precedidos por termos de confidencialidade e cláusulas relacionadas à Segurança da Informação.

4.2.1.15. Detectar e avaliar riscos de segurança nos serviços e produtos adquiridos, a fim de garantir que estejam em conformidade com os requisitos de segurança da informação, assegurando a proteção dos ativos e a integridade dos dados durante todo o ciclo de vida da relação com o fornecedor.

4.2.1.16. Assegurar a realização de auditorias periódicas para garantir a eficácia do Sistema de Gestão de Segurança da Informação (SGSI) e conformidade dos seus controles, além de garantir a sua efetiva implementação e manutenção;

4.2.1.17. Garantir a segurança cibernética em todo o espaço de controle industrial da M. Dias Branco, ao implementar controles e processos de ICS resilientes e protegidos.

4.2.1.18. Assegurar que a utilização, aquisição, desenvolvimento e integração de soluções baseadas em Inteligência Artificial ocorram de forma segura, ética e alinhada aos objetivos do negócio, mediante a implementação de controles para proteção das informações, avaliação de riscos, conformidade regulatória, supervisão humana, prevenção de uso indevido e monitoramento contínuo dos impactos decorrentes do uso dessas tecnologias.

## 4.3.Responsabilidades

4.3.1. **Compete a Todos os Colaboradores e Demais Partes Interessadas**

4.3.1.1.Estar ciente e manter-se informado sobre esta política, bem como as demais normas e procedimentos relacionados à Segurança da Informação que se apliquem às suas funções e responsabilidades;

4.3.1.2. Zelar pela segurança da informação na M. Dias Branco, informando quaisquer anormalidades a Gerência de Segurança da Informação através do e-mail: si@mdiasbranco.com.br

4.3.1.3.Responder legalmente pelos prejuízos advindos da inobservância das diretrizes elencadas nesta política;

4.3.1.4.Utilizar as informações da M. Dias Branco exclusivamente para atividades laborais e relacionadas aos objetivos de negócio, jamais para fins pessoais;

4.3.1.5.Preservar a integridade, a disponibilidade, a confidencialidade, autenticidade das informações corporativas acessadas ou manipuladas, não as utilizando, enviando, transmitindo ou compartilhando indevidamente, em qualquer local ou mídia, inclusive na Internet;

4.3.1.6.Manter sigilo sobre todas as informações que venha a tomar conhecimento em virtude das suas atividades profissionais, inclusive após o término da relação contratual existente, a qualquer título, por qualquer das partes, resguardando o direito da M. Dias Branco de pleitear o ressarcimento pelas eventuais perdas e danos decorrentes da má conduta e/ou de qualquer violação do sigilo por parte do usuário, inclusive mediante a tomada das medidas legais cabíveis.

4.3.2.**Compete à Gerência de Segurança da Informação**:

4.3.2.1.Gerenciar e Coordenar Gestão da Segurança da Informação;

4.3.2.2.Auxiliar no cumprimento desta política;

4.3.2.3.Definir, selecionar, garantir a implantação e revisar os controles e/ou soluções técnicas aderentes aos requisitos de Segurança da Informação;

4.3.2.4.Gerenciar os incidentes de Segurança da Informação.

4.3.3.**Compete ao Encarregado pelo Tratamento de Dados Pessoais**:

4.3.3.1.Dar suporte e acompanhar aprovação, bem como análise de contratos que envolvam tratamento de dados pessoais e dados pessoais sensíveis, seguindo a legislação vigente e aplicável a cada situação em suas particularidades;

4.3.3.2.Apoiar em sindicâncias para apuração de responsabilidade dos envolvidos em incidentes de dados pessoais e auxiliar na definição de aplicação das penalidades internas, em consonância com a Política de Consequências, quando necessário.

4.3.4.**Compete à Gerência Jurídica**:

4.3.4.1.Analisar pareceres sobre incidentes de Segurança da Informação sob o enfoque legal, com a finalidade de recomendar atualizações e/ou alterações que entender cabíveis a esta política;

4.3.4.2.Dar suporte jurídico na aplicação das penalidades decorrentes do não cumprimento da Política de Segurança da Informação em consonância com a Política de Consequências.

4.3.5.**Compete à Gerência de Recursos Humanos**:

4.3.5.1.Dar suporte operacional na aplicação das penalidades decorrentes do não cumprimento da Política de Segurança da Informação em consonância com a Política de Consequências;

4.3.5.2.Apoiar a divulgação e orientação da Política de Segurança da Informação para todos os usuários.

4.3.6.**Compete ao Comitê de Segurança da Informação**:

4.3.6.1.Revisar a Política de Segurança da Informação e seus documentos complementares de forma bienal ou sempre que se fizer necessário;

4.3.6.2.Propor melhorias à estratégia de conscientização dos colaboradores da M. Dias Branco em Segurança da Informação;

4.3.6.3.Apoiar a implantação do Sistema de Gestão da Segurança da Informação (SGSI);

4.3.6.4.Deliberar sobre os temas encaminhados ao Comitê.

## 4.4.Documentos complementares de SI e áreas de apoio

| ID | Nome do Documento | Assunto | Aplicabilidade |
|---|---|---|---|
| MDB.GSI.TAB.0001 | Matriz de Responsabilidades de Segurança da Informação. | Informar as responsabilidades de todas as áreas em relação ao tema Segurança da Informação | Todos os colaboradores, terceiros e demais partes interessadas aplicáveis. |
| MDB.GSI.PO.0001 | Acesso à Internet | Orientar quanto ao acesso à internet visando preservar a integridade, a confidencialidade, a disponibilidade e a autenticidade das informações | Todos os colaboradores, terceiros e demais partes interessadas aplicáveis. |

| | | | |
|---|---|---|---|
| MDB.GSI.PO.0002 | Uso de Mídia Social | Orientar quanto ao uso de mídias sociais | Todos os colaboradores, terceiros e demais partes interessadas aplicáveis. |
| MDB.DTI.PO.0013 | Gerenciamento de Backup | Definir regras para execução de procedimentos de backup dentro do ambiente tecnológico da M. Dias Branco | Diretoria de Tecnologia da Informação |
| MDB.GSI.PO.0009 | Gestão de acessos | Orientar quanto às atividades relacionadas à gestão de acessos e direitos de uso aos sistemas de informação. | Todos os colaboradores, terceiros e demais partes interessadas aplicáveis. |
| MDB.GSI.PO.0017 | Acesso Remoto | Estabelecer as regras e restrições relativas ao uso e concessão de acesso remoto ao ambiente lógico da M Dias Branco | Todos os colaboradores, terceiros e demais partes interessadas aplicáveis. |
| MDB.GSI.PO.0016 | Gestão de Ativos | Estabelecer limites, regras, orientações e restrições sobre a utilização corporativa dos recursos computacionais da M. Dias Branco | Todos os colaboradores, terceiros e demais partes interessadas aplicáveis. |
| MDB.GSI.PO.0013 | Controles Criptográficos | Estabelecer critérios para utilização de ferramentas de criptografia | Diretoria de Tecnologia da Informação |
| MDB.GSI.PO.0029 | Segurança Cibernética do ICS | Definir regras e padrões conforme as boas práticas e normas de Segurança Cibernética para os Sistemas de Controle e Automação Industrial (ICS) com o objetivo de proteger o ambiente industrial de incidentes cibernéticos | Gerência de Riscos / Gerência de Manutenção Industrial / Diretoria Técnica e de Operações / Diretoria Industrial / Diretoria de TI / Comitê de Segurança Cibernética Industrial / Colaboradores que atuem no ICS |
| MDB.GSI.PO.0003 | Proteção de Dados | Estabelecer as regras e restrições quanto a classificação e tratamento da informação de propriedade ou sob responsabilidade da M. Dias Branco | Todos os colaboradores, terceiros e demais partes interessadas aplicáveis. |
| MDB.GSI.PO.0014 | Configuração Segura de Ativos | Instruir as equipes a configurar os recursos computacionais da M. Dias Branco de maneira segura | Diretoria de Tecnologia da Informação |
| MDB.GSI.PO.0010 | Contratação de Serviços em Nuvem | Estabelece requisitos para contratação de serviços de processamento e armazenamento de dados na Internet | Diretoria de Tecnologia da Informação |
| MDB.GSI.PO.0022 | Desenvolvimento Seguro | Garantir que a segurança da informação esteja projetada e implementada no ciclo de vida de desenvolvimento dos sistemas de informação. | Diretoria de Tecnologia da Informação |
| MDB.GSI.PO.0006 | Gestão de Patches | Estabelecer as responsabilidades no gerenciamento dos serviços e sistemas da M. Dias Branco referente à aplicação e monitoramento de patches, visando minimizar riscos e falhas de vulnerabilidades técnicas em recursos computacionais. | Diretoria de Tecnologia da Informação |

| | | | |
|---|---|---|---|
| MDB.GSI.PO.0023 | Gestão de Logs e Trilhas de Auditoria | Estabelecer as regras relativas ao registro, coleta e a preservação de logs, trilhas de auditoria e o monitoramento do ambiente lógico da M. Dias Branco. | Diretoria de Tecnologia da Informação |
| MDB.GSI.PO.0007 | Gestão de Vulnerabilidades | Garantir que os ativos estejam com as vulnerabilidades identificadas e corrigidas de acordo com as prioridades definidas pela M. Dias Branco. | Diretoria de Tecnologia da Informação |
| MDB.GSI.PO.0008 | Monitoramento do Ambiente Tecnológico | Apresentar e estabelecer as responsabilidades dos profissionais que atuam no monitoramento sistemático dos serviços e sistemas da M. Dias Branco | Diretoria de Tecnologia da Informação |
| MDB.GSI.PO.0021 | Plano de Resposta a Incidentes | Instruir as equipes a tratar um incidente detectado ou informado. | Comitê de Resposta a Incidentes / Diretoria de Tecnologia da Informação / Gerência de Riscos / Gerência Jurídica |
| MDB.GSI.PO.0015 | Programa de Conscientização em Segurança da Informação | Estabelecer as responsabilidades e os limites de atuação dos colaboradores da M. Dias Branco em relação ao Programa de Conscientização em Segurança da Informação (PCSI) | Comunicação Interna / Gerência de Segurança da Informação |
| MDB.GSI.PO.0011 | Regimento Interno do Comitê de Segurança da Informação | Dispõe sobre as funções, responsabilidades, prerrogativas, composição e funcionamento do Comitê de Segurança da Informação (CSI) da M. Dias Branco. | Membros do Comitê de Segurança da Informação |
| MDB.GSI.PO.0018 | Resposta a Incidentes Cibernéticos | Instruir as equipes a tratar um incidente de segurança detectado ou informado. | Comitê de Resposta a Incidentes / Diretoria de Tecnologia da Informação / Gerência de Riscos / Gerência Jurídica |
| MDB.GSI.PO.0024 | Retenção e Descarte Seguro de Informações | Estabelecer os conceitos relativos à retenção e ao descarte de informações, registradas em meio físico ou digital, de propriedade ou que estão sob a responsabilidade da M. Dias Branco. | Colaboradores / Terceiros/ Gestores da Informação / Gerência Jurídica / Diretoria de Tecnologia da Informação |
| MDB.GSI.PO.0020 | Segurança em Computação em Nuvens | Estabelecer requisitos para segurança da computação em nuvem quanto ao processamento e/ou armazenamento de dados. | Diretoria de Tecnologia da Informação |
| MDB.GSI.PO.0025 | Segurança Física | Estabelecer as regras e restrições para garantir o controle de acesso e a segurança física adequada aos ambientes da M. Dias Branco. | Todos os colaboradores, terceiros e demais partes interessadas aplicáveis. |
| MDB.GSI.PO.0004 | Uso de E-mail Corporativo | Orientar quanto ao uso do e-mail corporativo visando preservar a integridade, a confidencialidade, a disponibilidade e autenticidade das informações. | Todos os colaboradores, terceiros e demais partes interessadas aplicáveis. |
| MDB.GSI.PO.0032 | Gerenciamento de Softwares | Estabelecer diretrizes para identificar, registrar, controlar e manter atualizadas as informações sobre os softwares | Diretoria de Tecnologia da Informação |

| | | | |
|---|---|---|---|
| | | gerenciados internamente na organização. | |
| MDB.GSI.PO.0033 | Segurança da Informação para Uso de Dispositivos Móveis Particulares (BYOD) | Estabelecer as regras e restrições relativas ao uso de dispositivo móvel particular pelo Usuário para realização das atividades profissionais, garantindo a segurança das informações e a conformidade com os padrões da M. Dias Branco. | Todos os colaboradores, terceiros e demais partes interessadas aplicáveis. |
| MDB.GSI.PO.0034 | Segurança da Informação para Uso de Inteligência Artificial Generativa | Estabelecer regras para o uso seguro de ferramentas de Inteligência Artificial Generativa (IAG), visando preservar a integridade, a confidencialidade, a disponibilidade e a autenticidade das informações. | Todos os colaboradores, terceiros e demais partes interessadas aplicáveis. |
| MDB.GSI.PO.0035 | Gerenciamento de Riscos Cibernéticos de Fornecedores de Tecnologia da Informação (TI) | Estabelecer diretrizes e responsabilidades para a gestão de fornecedores de Tecnologia da Informação com foco na avaliação de riscos de Segurança da Informação associados a fornecedores de Aplicações e Sistemas, bem como na definição de mecanismos alternativos de tratamento de riscos para os demais tipos de fornecedores. | Área de Negócios / Diretoria de Tecnologia da Informação / Suprimentos / Gerência Jurídica / Fornecedores / Gerência de Riscos |

Observação: Outros normativos e procedimentos operacionais poderão entrar em vigor sem estar citados neste documento e serão devidamente comunicados no canal oficial de comunicação da companhia.

## 4.5.Sanções e Punições

4.5.1.O descumprimento desta Política poderá resultar em sanções disciplinares, conforme as normas internas da Companhia (por exemplo, o Código de Ética e a Política de Consequências da M. Dias Branco S/A Indústria e Comércio de Alimentos), sem prejuízo das sanções administrativas, civis e penais aplicáveis, conforme determinação das autoridades competentes.

4.5.2.No caso de terceiros contratados ou prestadores de serviços, a M. Dias Branco realizará a análise da ocorrência e deliberará sobre a aplicação das sanções, conforme os termos estabelecidos em contrato.

# 5.REFERÊNCIAS

## 5.1.Documentos Explicitamente Citados

5.1.1.Não se aplica.

## 5.2.Outros Documentos Relacionados ao Assunto

5.2.1.A matéria tratada neste documento é regulamentada, mas não se limita, pelo Código Civil, Código Penal, Consolidação das Leis do Trabalho, Lei n.º 9.279/96 relativa à propriedade industrial, Lei n.º 9.610/98 relativa a direitos autorais, Lei n.º 9.609/98 relativa a programas de computador (*software*), Norma ABNT NBR ISO/IEC 27001:2022, demais políticas e procedimentos da companhia e demais legislação aplicável.

## 6.GLOSSÁRIO

**Ativos:** tudo aquilo que tenha valor para a M. Dias Branco.

**Ativos de Informação:** patrimônio intangível da M. Dias Branco constituído por suas informações, que podem ser de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, legal ou qualquer outra natureza, assim como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas à M. Dias Branco por parceiros, clientes, colaboradores e terceiros, não importando se protegidas ou não, de confidencialidade, em formato escrito ou verbal, físicas ou digitalizadas, armazenadas, trafegadas ou transitando pela infraestrutura computacional da M. Dias Branco, além dos documentos em suporte físico ou mídia eletrônica transitada dentro e fora de sua estrutura física.

**Autenticidade:** garantia de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade, assegurando o não repúdio, ou seja, a impossibilidade de esquiva de autoria pelo emissor (irretratabilidade).

**Confidencialidade:** é a garantia de que o acesso à informação seja obtido somente por pessoas autorizadas e vedado às demais.

**Continuidade de Negócios:** a organização deve estabelecer, documentar, implementar e manter processos, procedimentos e controles para assegurar o nível requerido de continuidade para a segurança da informação, durante uma situação adversa, conforme a ISO 27001:2013.

**Controles de Segurança de Informação:** são métodos para monitoramento, medição, análise e avaliação, aplicável, para assegurar resultados válidos, mitigar riscos para garantir os processos de segurança da informação.

**Credencial de Acesso (Conta de Acesso):** conjunto de caracteres alfanuméricos que identifica um usuário que tem acesso a um sistema de informação.

**Disponibilidade:** é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

**Incidente de Segurança de Informação:** são eventos de segurança da informação que são usados para reduzir a probabilidade e o impacto de riscos futuros, classificados como incidentes de segurança da informação.

**Integridade:** garantia de que a informação seja mantida em seu estado original e seja a mais atualizada, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais, e durante todo o seu ciclo de vida: criação, manutenção e descarte.

**Gestor da Informação:** usuário que exerça função gerencial, que ocupe cargo permanente na estrutura organizacional da M. Dias branco e que tenha criado adquirido ou recebido em confiança determinada informação.

**Princípio da Segurança de Informação:** os princípios básicos da segurança da informação. são definidos como: confidencialidade, integridade, disponibilidade, autenticidade e irretratabilidade ou não repúdio. (vide definições no glossário).

**Recursos Computacionais:** são os equipamentos, softwares, as instalações e demais ativos que constituem a infraestrutura computacional física e lógica da M. Dias Branco, tais como, mas, não se limitando a:

- Os computadores servidores, os computadores para uso individual ou coletivo, de qualquer porte, incluindo os dispositivos móveis, os equipamentos de armazenamento e distribuição de dados, as impressoras, as

copiadoras e os equipamentos multifuncionais, assim como os respectivos suprimentos, periféricos e acessórios.

- Os sistemas computacionais adquiridos ou desenvolvidos pelo da M. Dias Branco, bem como suas respectivas licenças.

**ICS:** sigla para Sistemas de Controle Industrial, o termo geral que abrange vários tipos de sistemas de controle, incluindo sistemas de controle de supervisão e aquisição de dados (SCADA), sistema digital de controle distribuído (SDCD) e outras configurações de sistema de controle, como controladores lógicos programáveis (PLC) frequentemente encontrados nos setores industriais e infraestruturas críticas. Um ICS consiste em combinações de componentes de controle (por exemplo, elétricos, mecânicos, hidráulicos, pneumáticos) que atuam juntos para alcançar um objetivo industrial.

**Usuários:** colaboradores com vínculo empregatício de qualquer área da M. Dias Branco, estagiários ou terceiros alocados na prestação de serviços a M. Dias Branco, independente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a utilizar os recursos computacionais ou obter acesso às informações da M. Dias Branco para o desempenho de suas atividades profissionais.

## 7.LISTA DE REGISTROS

| Código | Identificação do Registro | Tipo de Armazenamento | Proteção | Local da Recuperação | Tempo de Retenção | Disposição do Registro |
|---|---|---|---|---|---|---|
| - | - | - | - | - | - | - |

## 8.CONTROLE DE DIVULGAÇÃO

Todos os usuários da M. Dias Branco e empresas coligadas.

## 9.HISTÓRICO DE ALTERAÇÕES

| Revisão | Data | Alterações |
|---|---|---|
| 00 | XX/XX/XXXX | Liberação inicial |
| 01 | 25/01/2023 | Padronização da estrutura do documento e adição dos itens 4.2.1.17., 4.2.1.18., 4.3.3.10., 4.3.3.11., 4.3.3.12., 4.3.7.4., 4.3.7.5., 4.5.2. |
| 02 | 17/04/2026 | Inclusão do item 4.2.1.18 sobre Inteligência Artificial;<br>Atualização do item 4.3 Responsabilidades;<br>Inclusão do item 4.4 Documentos complementares de SI e áreas de apoio. |