## 1.OBJETIVO

Definir as diretrizes de Segurança da Informação, visando preservar os princípios da integridade, confidencialidade, disponibilidade e autenticidade das informações, através de um programa efetivo de prevenção, detecção e redução de impactos gerados pelos incidentes de segurança da informação.

Declarar formalmente o comprometimento da M. Dias Branco na promoção de diretrizes estratégicas, responsabilidades, competências e apoio ao Sistema de Gestão de Segurança da Informação (SGSI), a fim de garantir a proteção dos seus ativos de informação.

Estabelecer as responsabilidades e os limites de atuação dos colaboradores da M. Dias Branco em relação à segurança da informação, reforçando a cultura interna e priorizando as ações necessárias conforme o negócio.

## 2.APLICAÇÃO

A todo indivíduo ou organização que possui, possuiu ou possuirá vínculo com esta instituição, compreendendo todos os colaboradores, ex-colaboradores, prestadores de serviço, ex-prestadores de serviço, fornecedores que possuem, possuíram ou virão a possuir acesso às informações da M. Dias Branco e/ou fazem ou farão uso de recursos computacionais compreendidos na infraestrutura da M. Dias Branco.

## 3.GESTORES RESPONSÁVEIS

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

## 4.DESCRIÇÃO

### 4.1 Introdução

**4.1.1** A estrutura da Política de Segurança da Informação (PSI) será composta por um conjunto de documentos denominados de Política, Procedimentos Operacionais, Manuais e Documentos de Instruções Operacionais, que possuem os seguintes objetivos:

**4.1.1.1** Política: Contém as diretrizes estratégicas 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 normas que 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 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 que os ativos corporativos, com potencial para armazenar ou processar dados, sejam inventariados, classificados e protegidos.

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

**4.2.1.3** Assegurar a implementação de controles adequados para proteção das informações e sistemas contra acesso indevido, leitura, cópia, modificação, destruição e divulgação não autorizada.

**4.2.1.4** 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.

**4.2.1.5** Assegurar a implementação de controles robustos para proteger o acesso físico e lógico aos ambientes, aos dados e aos dispositivos.

**4.2.1.6** Assegurar que o acesso às informações pelos usuários é restrito às necessidades inerentes ao desempenho de suas funções e atribuições.

**4.2.1.7** Assegurar mecanismos para disseminação da cultura de segurança da informação e cibernética 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 através da implementação de controles para detecção, resposta e recuperação em casos 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** Proteger as informações através de controles nos data centers e nas instalações corporativas contra acesso físico não autorizado, bem como contra outros danos.

**4.2.1.12** Assegurar procedimentos e controles de segurança para aquisição e desenvolvimento de sistemas de informação, assim como a adoção de novas tecnologias empregadas nas atividades da companhia.

**4.2.1.13** Compreender os riscos da segurança cibernética associados à condução do negócio e administrar esses riscos de forma eficaz em consonância com a Política de Gerenciamento de Riscos da Companhia.

**4.2.1.14** Assegurar o comprometimento da alta gestão no processo de melhoria contínua do programa de segurança da informação.

**4.2.1.15** Zelar por relações transparentes e éticas e coibir toda forma de corrupção, fraude, suborno, favorecimento e extorsão praticados por colaboradores em consonância com o Código de ética da Companhia.

**4.2.1.16** Cumprir a legislação brasileira e os demais instrumentos regulamentares relacionados ao negócio no que diz respeito à segurança da informação.

**4.2.1.17** Assegurar que os relacionamentos e contratações com fornecedores, clientes, 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.

**4.2.1.18** 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.

## 4.3 Responsabilidades

**4.3.1** Cabem àqueles definidos no item 2 deste documento as seguintes responsabilidades:

**4.3.1.1** Estar ciente e manter-se atualizado (a) com esta política bem com o de quaisquer normas e procedimentos de Segurança da Informação que sejam aplicáveis as suas atividades laborais;

**4.3.1.2** Esclarecer quaisquer dúvidas relativas à Segurança da Informação junto a Coordenação de Segurança da Informação, assim como solicitar orientações, sempre que necessário, através do e-mail si@mdiasbranco.com.br;

**4.3.1.3** Responder legalmente pelos prejuízos advindos da inobservância das medidas relatadas 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;

**4.3.1.7** Zelar e manter em segurança suas credenciais e senhas de acesso aos sistemas de informação, incluindo redes, infraestrutura tecnológica e/ou às instalações da M. Dias Branco, bem como os respectivos recursos autorizados que necessite para o desenvolvimento de suas atividades profissionais;

**4.3.1.8** Comunicar à Coordenação de Segurança da Informação qualquer evento que coloque em risco a segurança das informações ou dos recursos computacionais da M. Dias Branco ou que viole esta política através do e-mail si@mdiasbranco.com.br;

**4.3.1.9** A omissão daquele que tiver ciência de incidente relacionado à Segurança da Informação, implica em responsabilização na medida de sua omissão;

**4.3.1.10** Responder por toda e qualquer atividade realizada através da sua credencial digital;

**4.3.1.11** Assinar os termos de responsabilidade cabíveis a contratação e dar aceite a política de segurança da informação.

**4.3.2** Cabe aos Gestores da Informação:

**4.3.2.1** Gerenciar as informações geradas ou confiadas à sua área de negócio e atuação durante sua criação, manuseio e descarte conforme as normas estabelecidas pela M. Dias Branco;

**4.3.2.2** Transmitir aos usuários ou partes interessadas sob sua responsabilidade as diretrizes desta política;

**4.3.2.3** Identificar e classificar as informações conforme critérios e procedimentos adotados;

**4.3.2.4** Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;

**4.3.2.5** Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pela organização.

**4.3.3** Cabe a Coordenação de Segurança da Informação

**4.3.3.1** Coordenar e conduzir a Gestão da Segurança da Informação;

**4.3.3.2** Auxiliar no cumprimento desta política;

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

**4.3.3.4** Homologar e especificar os programas de computador autorizados a serem utilizados pelos usuários da M. Dias Branco, suas subordinadas e coligadas;

**4.3.3.5** Revogar todos direitos e credenciais de acesso e certificados digitais de usuários desligados ou alterações de atribuições entre áreas negócio distintas conforme solicitação da Gerência de RH;

**4.3.3.6** Gerenciar os incidentes de Segurança da Informação;

**4.3.3.7** Analisar pareceres sobre incidentes de Segurança da Informação sob o enfoque técnico com a finalidade de recomendar atualizações e/ou alterações que entender cabíveis a esta política;

**4.3.3.8** Esclarecer, em última instância, dúvidas e fornecer orientações aos usuários;

**4.3.3.9** Realizar e acompanhar estudos de tecnologias, quanto a possíveis impactos na segurança da informação;

**4.3.3.10** Manter o contato com grupos especiais, associações profissionais ou outros fóruns especializados em Segurança da Informação;

**4.3.3.11** Garantir que as configurações dos sistemas estejam de acordo com a Política de Segurança da Informação e seus documentos complementares;

**4.3.3.12** Desenvolver processos, procedimentos e configurações tecnológicas para facilitar a implementação das políticas de segurança cibernética do ICS e padrões associados.

**4.3.4** Cabe ao Encarregado pelo Tratamento de Dados Pessoais e Dados Pessoais Sensíveis

**4.3.4.1** 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;

**4.3.4.2** 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;

**4.3.4.3** Avaliar e auxiliar na elaboração de Relatórios de Impacto à Proteção de Dados Pessoais e Dados Pessoais Sensíveis;

**4.3.4.4** Apoiar no desenvolvimento do Plano de Análise e Resposta a Incidente de Segurança de Dados Pessoais e Dados Pessoais Sensíveis que identifique o tipo de violação, o número de registros afetados, quais registros foram afetados e as categorias de dados pessoais e dados pessoais sensíveis envolvidas, as notificações apropriadas e plano de mitigação dos efeitos da violação; e

**4.3.4.5** Auxiliar no que couber, para que o tratamento de Dados Pessoais e Dados Pessoais Sensíveis tenha o mesmo nível de tratamento que informações consideradas confidenciais.

**4.3.5** Cabe a Gerência Jurídica

**4.3.5.1** 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;

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

**4.3.6** Cabe a Gerência de Recursos Humanos

**4.3.6.1** Colher as assinaturas dos usuários, arquivar e guardar de forma segura todos os Termos de Uso dos Sistemas de Informação;

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

**4.3.6.3** Apoiar a divulgação e orientação da Política de Segurança da Informação para todos os usuários;

**4.3.6.4** Estipular controles de segurança especificamente relacionados aos processos de contratação, encerramento e modificação das atividades dos colaboradores;

**4.3.6.5** Disponibilizar os normativos da M. Dias Branco, além de custodiar e colher assinatura do "Termo de Ciência e Responsabilidade" na admissão de novos colaboradores.

**4.3.7** Cabe ao Comitê de Segurança da Informação

**4.3.7.1** Atualizar a Política de Segurança da Informação, de acordo com a legislação vigente, os avanços da tecnologia e as melhores práticas em Segurança da Informação, fornecendo todas as justificativas necessárias para aprovação de novas versões da política;

**4.3.7.2** Revisar a Política de Segurança da Informação e seus documentos complementares de forma anual ou sempre que se fizer necessário;

**4.3.7.3** Criar, revisar e validar os procedimentos de Segurança da Informação;

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

**4.3.7.5** Patrocinar a implantação local do Sistema de Gestão da Segurança da Informação (SGSI);

**4.3.7.6** Quando solicitado, analisar as infrações cometidas pelos usuários a presente política e deliberar sobre a aplicação das ações disciplinares que entender cabíveis, considerando a gravidade das infrações sob o enfoque técnico e legal, assim como os riscos relacionados.

## 4.4 Sanções e Punições

**4.4.1** O descumprimento desta Política sujeitará o infrator a sanções disciplinares, de acordo com as normas internas da Companhia (e.g. Código de Ética da Companhia e Política de Consequências da M. Dias Branco S/A Indústria e Comércio de Alimentos), sem prejuízo das sanções administrativas, civis e penais cabíveis, imputáveis pelas autoridades competentes.

**4.4.2** No caso de terceiros contratados ou prestadores de serviço, a M. Dias Branco deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato.

# 5. 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.

**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.

**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.

**Usuários:** colaboradores com vínculo empregatício de qualquer área da M. Dias Branco 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.

## 6. HISTÓRICO DE ALTERAÇÕES

| Revisão | Últimas Alterações |
|---|---|
| 0 | Emissão inicial |

| ELABORADO POR: | APROVADO POR: |
|---|---|
| MARIA DAS GRACAS DA SILVA VASCONCELOS | MAURO CESAR BRANCO ALARCON |