Política de Segurança da Informação

MSB TECNOLOGIA

HISTÓRICO DE REVISÃO E SUBSTITUIÇÃO

Código:	PO SGPI 01
Versão:	1.2
Data da versão:	19/03/2025
Criado por:	Frederico Coelho
Aprovado por:	Comitê de Compliance
Nível de confidencialidade:	Pública

Histórico de alterações

Data	**Versão**	**Criado por**	**Descrição da alteração**
12/11/2024	1.0	Frederico Coelho	Criação da primeira versão da política de segurança da informação.
12/03/2025	1.1	Lucien Rocha	Ajuste da primeira versão do procedimento Revisão Final
19/03/2025	1.1	Comitê de Compliance	Aprovação do documento.

SUMÁRIO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. INTRODUÇÃO

O primeiro passo para a implementação do Sistema de Gestão de Segurança da Informação e Privacidade (SGPI) é a adoção de uma Política de Segurança da Informação, definida e aprovada pela Alta Direção. Este documento depende da combinação de requisitos do negócio, de estrutura de processos, do uso de tecnologias e mecanismos de proteção e, o mais relevante, depende do comportamento de seus usuários, independentemente do nível hierárquico ou da atividade desenvolvida para a MSB Tecnologia (MSB).

Para ampliar a cultura de segurança da informação e privacidade, a MSB, alinhada às boas práticas e normas internacionalmente aceitas, criou sua Política de Segurança da Informação (PSI), a fim de adequá-la à legislação nacional vigente e garantir a proteção de todos os seus ativos tangíveis e intangíveis.

2. OBJETIVO

O objetivo desta política é estabelecer as diretrizes necessárias para assegurar a confidencialidade, integridade e a disponibilidade da informação utilizada pela MSB.

Minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de clientes ou de qualquer outro impacto negativo no negócio da organização como resultado de falhas de segurança ou violação de dados pessoais.

3. ABRANGÊNCIA

Esta política abrange todas as informações, os sistemas e recursos de Tecnologia da Informação da MSB, incluindo todos os usuários em quaisquer das dependências da MSB e

operações, seja em ambientes corporativos ou em locais externos, incluindo o uso de dispositivos móveis e plataformas de trabalho remoto.

4. DIRETRIZES GERAIS

A MSB por meio dessa Política, busca:

a) Assegurar o cumprimento de todas as suas obrigações legais, para atender aos requisitos regulamentares e contratuais pertinentes às suas atividades, a exemplo da Lei Geral de Proteção de Dados Pessoais (LGPD), 13.709 de agosto de 2018;

b) Empregar medidas técnicas e organizacionais adequadas no tratamento de dados pessoais, e envidar esforços para proteção dos dados pessoais dos titulares de dados pessoais contra acessos não autorizados, perda, destruição, compartilhamento não autorizado, entre outras hipóteses;

c) Garantir a confidencialidade, integridade e disponibilidade das informações de seus titulares de dados pessoais e da própria organização, protegendo os sistemas de informação contra acessos indevidos e modificações não autorizadas;

d) Assegurar que somente pessoas autorizadas tenham acesso às instalações da MSB, às informações e aos sistemas de informação;

e) Conscientizar os usuários sobre as possíveis consequências para a organização, se ocorrer incidentes de segurança da informação ou violação às políticas de segurança e privacidade;

f) Garantir a continuidade de seus negócios, protegendo os processos críticos contra falhas ou desastres significativos;

g) Assegurar o treinamento contínuo e atualizado nas políticas e nos procedimentos de segurança da informação e privacidade, enfatizando as obrigações das pessoas pela proteção de dados;

h) Garantir que todas as responsabilidades pela segurança da informação e privacidade

estão claramente definidas e que os usuários indicados são competentes e capazes de cumprir com as atribuições;

i) Melhorar continuamente o Programa de Segurança e Privacidade.

4.1. CONFORMIDADE

A conformidade com requisitos legais, regulatórios e contratuais é responsabilidade de todos os colaboradores da MSB. Os líderes imediatos devem identificar e observar a legislação aplicável à MSB, garantindo a adequação contratual e observância das diretrizes de Segurança da Informação desta Política.

Os requisitos da Lei Geral de Proteção de Dados (LGPD) e a Política de Proteção de Dados devem ser observados por todos os colaboradores visando preservar a privacidade do titular dos dados pessoais. Em nenhum caso, o colaborador poderá vender ou transferir informações da MSB ou de responsabilidade desta a terceiros, ou fornecer acesso a elas sem a autorização formal e prévia. A confidencialidade e sigilo de dados pessoais devem ser observados, preservados e garantidos por todos os usuários da MSB.

4.2. USO DE E-MAIL

O correio eletrônico é um recurso de comunicação institucional da MSB e as regras de acesso e utilização do e-mail devem atender a todas as orientações desta PSI, além das demais diretrizes da Política de Proteção de Dados. Portanto, fica proibido o uso do e-mail corporativo para fins pessoais. O compartilhamento de informações da MSB por meio de e-mails pessoais também é proibido.

O não cumprimento dessas diretrizes poderá resultar em sanções disciplinares, que poderão incluir advertências, suspensões ou até mesmo desligamento, conforme a gravidade da infração, sem prejuízo de outras medidas legais cabíveis.

4.3. USO DE INTERNET

A Internet é uma ferramenta de trabalho para o desenvolvimento de atividades, processos, pesquisas, tecnologias e competências. A MSB mantém regras de utilização e bloqueio de acesso a determinados sites, caixas de e-mail, conteúdos, anexos, emitentes, destinatários, assinaturas, notas, limites de tráfego e armazenamentos. A MSB não autoriza a utilização dos meios de comunicação da organização para divulgar mensagens com conteúdo ilegal, pornográfico, com qualquer sentido discriminatório, de cunho religioso, político-partidário, ideológico ou em desacordo com os princípios éticos e morais da MSB.

4.4. USO DAS REDES SOCIAIS E WHATSAPP

A publicação de informações relacionadas à MSB Tecnologia em mídias, aplicativos de mensagens instantâneas (como WhatsApp, Discord, Telegram, Skype, entre outros) e redes sociais deve ser realizada exclusivamente por setores ou usuários formalmente designados para essa função. Qualquer outra pessoa ou área não autorizada está terminantemente proibida de publicar, compartilhar ou comentar, em nome da organização, qualquer tipo de conteúdo que envolva dados, decisões, produtos ou opiniões institucionais.

Quando no uso de suas mídias e redes sociais particulares, os usuários devem observar as seguintes restrições:

- Não é permitido o uso da logomarca, bem como de qualquer parte da identidade visual da MSB sem autorização prévia e expressa;
- Não é permitida a criação, participação ou interação de/com quaisquer perfis, comunidades, grupos, tópicos de discussão e afins que empreguem o nome, marca ou outros sinais distintivos da MSB, excetuando-se os canais oficiais da empresa ou designacao especifica para este fim por parte da Diretoria;
- Não é permitida a publicação de conteúdo ou comentários diretamente relacionados à MSB, seus empregados, terceiros contratados e prestadores de serviço;
- Não é permitida a publicação de qualquer tipo de imagem, foto, vídeo, áudio

relacionado ao ambiente corporativo da MSB sem a expressa autorização da organização, excetuando-se material divulgado em canais oficiais.

4.5. USO DE COMPUTAÇÃO EM NUVEM

A computação em nuvem é uma ferramenta essencial para o armazenamento, transferência de documentos, processamento de dados, execução de aplicações e suporte a sistemas corporativos. A MSB disponibiliza aos colaboradores uma infraestrutura de nuvem corporativa dedicada exclusivamente a atividades relacionadas à organização, garantindo segurança, conformidade com a legislação vigente e eficiência operacional.

É terminantemente proibido o armazenamento ou compartilhamento de informações corporativas em serviços de nuvem pessoais ou não autorizados. O uso de driver pessoais (ex.: Google Drive, OneDrive, Dropbox) para arquivos relacionados às atividades da MSB não é permitido.

Todos os arquivos devem ser armazenados no ambiente corporativo fornecido pela MSB, que é monitorado para assegurar conformidade e proteção contra acessos indevidos. A infraestrutura em nuvem corporativa oferece recursos como controle de acesso, auditoria de logs e backups automatizados, sendo a responsabilidade de cada colaborador garantir que as informações estejam corretamente alocadas nesse ambiente.

Em caso de necessidade específica de acesso a serviços externos de nuvem, uma solicitação formal deve ser feita à Área Compliance, que avaliará a viabilidade e os riscos envolvidos, garantindo o cumprimento das diretrizes de segurança da informação.

A MSB realiza revisões periódicas na política de uso da nuvem, considerando as melhores práticas de mercado e novas tecnologias, com o objetivo de proteger os ativos de informação da organização e reduzir os riscos associados ao uso inadequado de recursos de nuvem.

4.6. USO DE DISPOSITIVOS MÓVEIS

As diretrizes gerais de uso de dispositivos móveis para acesso às informações, sistemas, aplicações e e-mail da MSB devem considerar, prioritariamente, os requisitos legais e a estrutura da organização, atendendo a esta Política de Segurança da Informação e a Política de Proteção de Dados, e devem ser regidas por normas específicas, a qual contempla as recomendações sobre o uso desses dispositivos.

4.7. USO DE ANTIVÍRUS

Toda estação de trabalho e servidor deve possuir antivírus (software) instalado e atualizado automaticamente.

É responsabilidade da área Técnica assegurar o processo de controle de malware na MSB.

É responsabilidade do colaborador comunicar à área Técnica comportamentos associados a malwares em suas estações de trabalho. O uso de mídias removíveis (pen drives, discos externos, smartphones, etc.) em equipamentos da MSB Tecnologia é monitorado e, por padrão, proibido, exceto em casos previamente autorizados pela área Técnica, com registro formal e controle rigoroso. Somente dispositivos escaneados e criptografados poderão ser usados, quando necessário, para atividades essenciais.

A Área Técnica deve realizar auditorias regulares nos logs gerados pelos softwares antivírus, analisando eventos suspeitos, falhas e incidentes de segurança. Os resultados dessas auditorias devem ser documentados e utilizados para reforçar as estratégias de proteção contra códigos maliciosos e garantir a conformidade com as diretrizes de segurança da MSB.

A organização incentiva o uso de alternativas seguras, como drives na nuvem corporativos, pastas compartilhadas e redes VPN.

4.8. DRIVE DE REDE

Informações relacionadas ao negócio da MSB Tecnologia não devem ser armazenadas localmente em estações de trabalho ou dispositivos móveis, como laptops, pen drives, HDs externos, celulares e tablets. Todos os dados corporativos devem ser armazenados exclusivamente nos diretórios de rede disponibilizados pela organização, como o Google Drive corporativo, para garantir a segurança e a realização adequada das cópias de segurança. É responsabilidade de cada colaborador assegurar que todas as informações relevantes estejam devidamente alocadas nesses diretórios, seguindo as diretrizes de segurança e conformidade da MSB.

4.9. MONITORAMENTO

A MSB reserva o direito para si de monitorar e manter registros de todos os tipos de acesso aos seus sistemas, redes e informações. Incluindo-se o uso particular (pessoal) através destes recursos, quando da existência de informações e/ou evidências de atos ilícitos ou conduta inadequada. Estes registros também podem ser utilizados para análises estatísticas visando a boa prestação de serviços e para verificação em casos relacionados a incidentes de segurança.

5. RISCOS

A não observância dos princípios e diretrizes constantes nesta Política e seus documentos complementares, pode impactar seriamente a MSB, pois pode possibilitar a violação de leis e regulamentos, além de afetar negativamente a reputação e a estabilidade financeira da MSB.

Desvios e exceções devem ser tratados pelo Comitê de Privacidade.

Suspeitas de violação de dados pessoais devem ser comunicadas ao superior imediato, Encarregado de Dados e/ou através de envio de e-mail para grc@msbtec.com.br.

6. RESPONSABILIDADES

6.1. USUÁRIOS

Para fins desta política, considera-se como **usuários** todas as pessoas físicas que desempenham atividades relacionadas à MSB, independentemente do vínculo empregatício. Isso inclui colaboradores contratados sob o regime CLT, prestadores de serviços, estagiários, menores aprendizes e jovens aprendizes, seja por meio de pessoa jurídica ou não, e atuando dentro ou fora das dependências da organização.

É dever dos usuários:

a) Ler, respeitar e cumprir esta Política de Segurança da Informação e seus documentos complementares;

b) Responder pela guarda e proteção dos recursos computacionais colocados à sua disposição durante seu horário de trabalho;

c) Responder pelo uso exclusivo e intransferível de suas senhas de acesso;

d) Buscar conhecimento necessário para a correta utilização dos recursos de hardware e software;

e) Relatar prontamente à área responsável, qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, violação de dados pessoais, fragilidade, mau funcionamento, presença de vírus etc.;

f) Assegurar que as informações e dados de propriedade da MSB não sejam disponibilizados a terceiros, ou sem a devida autorização por escrito do responsável hierárquico;

g) Comprometer-se em não auxiliar terceiro e ou provocar invasão dos computadores ou da rede de dados, conforme artigo 154-A do Código Penal Brasileiro.

6.2. ADMINISTRATIVO E RH

a) Ter postura exemplar em relação à segurança da informação e privacidade, servindo como modelo de conduta para os colaboradores e prestadores de serviço sob a sua gestão;

b) Assegurar que todos os candidatos a emprego sejam adequadamente analisados, especialmente em cargos ou serviços com acesso a informações, dados pessoais e dados pessoais sensíveis. São obrigatórias as verificações de referência profissional;

c) Garantir que todos os novos colaboradores recebam instruções sobre sua responsabilidade pela segurança da informação e privacidade.

d) Garantir a solicitação de criação de perfis de acesso ao ambiente de tecnologia da informação e as dependências da MSB para as áreas responsáveis;

e) Estabelecer Plano de Treinamento e Conscientização em segurança da informação e privacidade, garantindo a ciência e aderência dos colaboradores e terceiros aos princípios e diretrizes da segurança da informação e proteção de dados;

f) Aplicar as medidas disciplinares formais vigentes para os colaboradores e terceiros que tenham cometido incidentes de segurança ou violação de dados pessoais, garantindo inclusive, dissuasão para que novas violações não ocorram.

6.3. ÁREA TÉCNICA

a) Garantir a devolução dos ativos de TI da MSB e a solicitação de retirada de acesso de todos os colaboradores e terceiros no encerramento de suas atividades, contratos ou acordos;

b) Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes e violação de dados pessoais;

c) Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI;

d) Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente;

e) Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações;

f) Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes;

g) Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências;

h) Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a organização;

i) Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela;

j) Proteger continuamente todos os novos ativos, antes de serem introduzidos no ambiente de produção, sejam devidamente verificados e comprovadamente livres de quaisquer códigos maliciosos ou indesejados. Os ativos de informação já existentes no ambiente de produção sejam constantemente monitorados e protegidos contra a introdução de códigos maliciosos. Mecanismos eficazes de detecção, prevenção e resposta a incidentes envolvendo códigos maliciosos sejam implementados e mantidos, visando preservar a integridade e disponibilidade dos ativos de informação. Todos os usuários estejam cientes de suas responsabilidades e adotem as melhores práticas de segurança da informação para mitigar os riscos relacionados a códigos maliciosos. O descumprimento destas determinações estará sujeito às sanções previstas nesta Política de Segurança da Informação.

6.4. FÁBRICA DE SOFTWARE

a) Ler, respeitar e cumprir esta Política de Segurança da Informação e seus documentos complementares;

b) Atuar conforme determina os Guias de Processos de desenvolvimento de Software e a Política de Desenvolvimento Seguro.

6.5. ALTA DIREÇÃO

a) Aprovar esta Política;

b) Atualizar esta política em decorrência de alterações legais, normativas ou estatutárias, tendo-se por derrogada qualquer disposição nela descrita que resultar incompatível com alterações futuras do Estatuto Social da organização ou de norma legal, sendo no mínimo obrigatório a revisão a cada Dois (02) anos;

c) Zelar pela aplicação efetiva das melhores práticas em Segurança da Informação e Privacidade;

d) Garantir que medidas corretivas sejam tomadas quando desconformidades forem identificadas.

6.6. POLÍTICAS COMPLEMENTARES

Serão criadas, aprovadas e implementadas as seguintes políticas complementares, para apoiar no Programa de Privacidade da MSB:

1. Política de Segurança da Informação;
2. Política de Uso dos Ativos de Tecnologia da Informação;
3. Política de Acesso Remoto;
4. Política de Controle de Acesso;
5. Política de Uso de Dispositivos Móveis;
6. Política de Gestão de Vulnerabilidades;
7. Política de Plano de Respostas a Incidentes;
8. Política de Proteção de dados;
9. Política de Privacidade;
10. Política de Privacidade Interna;
11. Política de Atendimento aos Titulares;
12. Procedimento de Compartilhamento de Dados Pessoais com Terceiros;
13. Política de Adequação de Contratos com Terceiros;
14. Política de Backup e Restauração;
15. Política de Desenvolvimento Seguro;
16. Política Retenção e Descarte de Dados Pessoais.

7. PENALIDADES - PROCESSO DISCIPLINAR

Em caso de transgressão desta Política, das normas de segurança da informação ou da legislação brasileira, poderão ser aplicadas sanções administrativas e/ou legais, as quais poderão incluir desde medidas disciplinares internas até o desligamento do infrator, sem prejuízo de outras medidas judiciais cabíveis nas esferas administrativa, cível e criminal.

7.1. VIOLAÇÕES

Constituem violações à presente Política, Normas e Procedimentos de Segurança da Informação:

- Qualquer ação ou situação que possa expor a MSB ou seus clientes a riscos financeiros e de imagem, sejam eles potenciais ou reais, comprometendo seus ativos de informação;
- Utilização indevida de dados corporativos e divulgação não autorizada de informações, segredos comerciais ou quaisquer outros dados confidenciais, sem a permissão expressa do responsável legal pela informação;
- Utilização de dados, informações, equipamentos, softwares, sistemas ou outros recursos tecnológicos para fins ilícitos, incluindo a violação de leis, regulamentos internos e externos, princípios éticos ou exigências de órgãos reguladores da área de atuação do MSB ou de seus clientes;
- A não comunicação imediata à Diretoria da MSB de quaisquer descumprimentos desta Política, Normas ou Procedimentos de Segurança da Informação, que porventura um colaborador, empregado, estagiário, aprendiz ou prestador de serviços venha a ter conhecimento ou presenciar.

7.2. SANÇÕES

O descumprimento da política, normas e procedimentos de segurança da informação, incluindo a não adesão à Política de Segurança da Informação da MSB, será considerado falta

grave. Nesses casos, poderão ser aplicadas penalidades disciplinares, conforme as normas internas de recursos humanos e a legislação vigente.

8. DOCUMENTOS DE REFERÊNCIA

LEI Nº 13.709/18: Lei Geral de Proteção de Dados Pessoais (LGPD);

ABNT NBR ISO/IEC 27001:2013: Tecnologia da Informação — Técnicas de Segurança — Sistemas de Gestão da Segurança da Informação — Requisitos;

ABNT NBR ISO/IEC 27002:2013: Tecnologia da Informação — Técnicas de Segurança — Código de Prática para Controles de Segurança da Informação;

ABNT NBR ISO/IEC 27032:2015: Tecnologia da Informação — Técnicas de Segurança — Diretrizes para Segurança Cibernética;

ABNT NBR ISO/IEC 27701:2019: Tecnologia da Informação — Técnicas de Segurança — Extensão à ABNT NBR ISO/IEC 27002 para Gestão da Privacidade da Informação – Requisitos e Diretrizes;

9. SIGLAS E DEFINIÇÕES

- **Comitê de Privacidade:** Comitê estabelecido pela MSB e tem como principal função ajudar na elaboração e na revisão contínua da Política de Segurança da Informação, assim como na avaliação dos controles utilizados e na resposta aos incidentes gerados a partir dos eventos de segurança da informação e privacidade.

- **Confidencialidade:** Garantia de que a informação, quando necessária, esteja acessível apenas aos colaboradores e/ou processos autorizados, e seja devidamente protegida do conhecimento ou acesso alheio indevido.

- **Integridade:** Garantia que uma informação esteja correta, verdadeira e não seja corrompida ou perda suas características originais.

- **Disponibilidade:** Garantia que a informação e seus ativos de tecnologia da informação sejam preservados e estejam disponíveis sempre que necessário, mediante a devida autorização para seu acesso e/ou uso.

- **Informação:** É o resultado do processamento, manipulação e organização de dados;

- **Usuários:** Todas as pessoas que acessam as informações ou recursos de Tecnologia da Informação da MSB são usuários, sejam clientes, membros dos comitês, diretores, colaboradores CLT, estagiários, jovens aprendizes, terceiros, parceiros, prestadores de serviços e fornecedores.

- **Vírus:** Um vírus de computador é um programa que, quando executado, se autorreplica inserindo cópias de si mesmo em outros programas, arquivos de dados ou no setor de boot do disco rígido. Quando a replicação é bem sucedida diz-se que estas áreas estão infectadas. Estas ameaças frequentemente trazem algum tipo de dano para as atividades dos sistemas infectados tais como: diminuição do espaço de armazenamento dos discos rígidos, aumento da carga de processamento dos processadores, acesso à informação

privada, corrupção de dados, exibição de mensagens políticas ou humorísticas na tela do usuário, roubo dos contatos do usuário ou captura do conteúdo digitado.