POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE	
Código	POL-SIP
Versão vigente	1
Data da versão vigente	08/10/2025
Tipo de documento	Política
Autores/Revisores	Rodrigo Lopes Demétrius Fernandes Leandro Correa Monique Campos
Aprovador(es)	Renato Bello Sergio Resende
Classificação	Uso Interno

SUMÁRIO

1. INTRODUÇÃO

O **Motor Group Brasil** (“MGB”) está entre os maiores grupos de concessionárias do Brasil, representando 9 marcas em 5 estados, com uma postura onde a inovação, a qualidade, a excelência e o compromisso com a satisfação máxima de clientes, colaboradores/prestadores e parceiros são pilares fundamentais. O MGB compreende ser de suma importância proteger suas estratégias, metodologias, processos internos, ferramentas tecnológicas e conhecimentos específicos, bem como os dados pessoais de todos os sócios, colaboradores/prestadores, parceiros, fornecedores e demais partes interessadas.

O MGB compreende que informação é um ativo estratégico de inestimável e que sua correta gestão, assegurando que ela esteja sempre disponível para as pessoas certas no momento adequado, é fundamental para o cumprimento do propósito, objetivos de negócio e para a reputação da organização.

Desta forma, o MGB estabelece esta **Política Geral de Segurança da Informação e Privacidade (“Política”)** para direcionar seus esforços de segurança da informação e privacidade, alinhado às melhores práticas de mercado e às normas internacionalmente aceitas, com o objetivo de determinar e manter níveis adequados de segurança capazes de assegurar a confidencialidade, integridade e disponibilidade de suas informações e daquelas tratadas sob sua responsabilidade.

2. TERMOS E DEFINIÇÕES

Consulte o Documento **MGB – Termos e Definições de Segurança da Informação e Privacidade.**

3. OBJETIVOS

3.1. Esta Política estabelece as diretrizes e responsabilidades para o planejamento, implementação, operação, monitoramento e melhoria contínua dos esforços de segurança da informação e privacidade do MGB. Define também objetivos estratégicos alinhados aos objetivos de negócio, propósito, cultura e estratégia de mercado da organização.

3.2. O MGB deve implementar controles aptos a assegurar a confidencialidade, integridade e disponibilidade de informações e demais ativos associados pertencentes

ou tratados sob sua responsabilidade. Estes controles devem ser planejados e implementados com base em um processo de gestão de riscos em segurança da informação e privacidade, através do qual decisões informadas sobre eliminar, transferir, mitigar ou aceitar riscos identificados, analisados e avaliados devem ser tomadas.

3.3. O MGB deve determinar e disponibilizar recursos humanos e financeiros adequados para implementação, operação, monitoramento e melhoria contínua de seus esforços de segurança da informação e privacidade em conformidade com esta Política.

3.4. Os controles de segurança da informação e privacidade devem estar integrados por padrão (by default) e no desenho (by design) de todos os processos, sistemas, ferramentas tecnológicas, documentos e relações do MGB, e questões pertinentes devem ser tratadas como prioridade.

4. APLICAÇÃO

4.1. Esta Política deve ser aplicada a todos os sócios, empregados, parceiros, estagiários e prestadores de serviços contratados direta ou indiretamente (terceirizados) pelo MGB. Isso inclui pessoas que trabalhem em período integral, meio período ou em regime temporário, seja em atuação presencial ou remota. Todos são referidos nesta Política simplesmente como "colaboradores/prestadores".

4.2. Esta Política deve ser aplicada ao tratamento de informações pertencentes ou sob a responsabilidade do MGB, abrangendo comunicações verbais, uso de qualquer plataforma tecnológica ou mídia física.

4.3. Diretrizes de segurança da informação e privacidade estabelecidas por esta Política devem ser aplicadas a instalações físicas, sistemas, *softwares*, ferramentas tecnológicas e recursos de tecnologia da informação e comunicação (TIC) contratados ou pertencentes ao MGB.

5. OBRIGAÇÕES, REQUISITOS E EXPECTATIVAS

5.1. O MGB deve identificar e manter conformidade com obrigações e requisitos de segurança da informação e privacidade, conforme previstos em legislações e

regulamentos aplicáveis. Isso inclui também as obrigações estabelecidas em contratos firmados pela organização.

5.2. O MGB deve identificar os requisitos e expectativas quanto à segurança da informação e privacidade de partes interessadas internas e externas e como eles serão endereçados internamente, incluindo as obrigações estabelecidas em contratos firmados.

6. RESPONSABILIDADES

6.1. O MGB deve assegurar que conte com pessoas com competência comprovada para planejar, implementar, gerenciar, medir e melhorar continuamente seus esforços de segurança da informação e privacidade e todos os controles definidos para aplicação.

6.2. Com objetivo de governar estes esforços, o MGB estabelece o Comitê Gestor de Segurança da Informação e Privacidade (CGSIP), com participação da gerência de TI, membros da liderança, e consultores externos especializados em segurança da informação e privacidade, conforme necessário.

6.3. São atribuições e responsabilidades do **CGSIP**:

- **a.** promover o alinhamento dos esforços de segurança da informação e privacidade aos objetivos de negócios, propósito, cultura, e estratégia de mercado do MGB;
- **b.** promover reuniões periódicas no máximo a cada 3 meses para deliberar sobre questões de segurança da informação e privacidade, revisar e executar atribuições relacionadas;
- **c.** coordenar a gestão de riscos de segurança da informação e privacidade do MGB, responsabilizando-se pela definição dos critérios e metodologia para identificação, análise, avaliação, tratamento e aceitação de riscos;
- **d.** revisar e aprovar a atribuição de papéis e responsabilidades relacionados à segurança da informação e privacidade no MGB;
- **e.** solicitar, revisar e aprovar orçamentos compatíveis com as necessidades do MGB em questões de segurança da informação e privacidade;
- **f.** zelar para que o MGB conte com medidas técnicas e administrativas, compostas por controles organizacionais, de pessoas, físicos e tecnológicos apropriados para a organização, capazes de assegurar sua capacidade de

governar, identificar, proteger, detectar, responder e recuperar em segurança da informação e privacidade;

g. coordenar a elaboração, revisão e aprovação de toda a documentação relativa à segurança da informação e privacidade, inclusive desta Política, envolvendo equipes e colaboradores/prestadores e aconselhamento externo especializado, sempre que considerar necessário;

h. analisar criticamente as medidas estabelecidas para que estas atendam aos requisitos legais, regulatórios e contratuais impostos ao MGB;

i. medir a eficácia, monitorar e revisar controles, avaliações e planos implementados, com objetivo de corrigir não-conformidades e continuamente melhorar a pertinência, adequação, eficácia e eficiência dos esforços de segurança da informação e privacidade do MGB.

6.4. **Todos os colaboradores/prestadores** do MGB devem:

a. considerar segurança da informação e privacidade como sua responsabilidade em conjunto com todos na organização;

b. conhecer integralmente e compreender o conteúdo, regras e diretrizes desta Política e outros documentos de segurança da informação e privacidade relevantes para sua função, atividades de trabalho e ativos aos quais possuem acesso;

c. conhecer e cumprir legislações que regulamentam aspectos como privacidade e proteção de dados pessoais, inteligência artificial e propriedade intelectual, sem prejuízo de outras questões aplicáveis às suas atividades profissionais;

d. cumprir com os treinamentos de segurança da informação e privacidade promovidos pela organização;

e. conhecer e aplicar em sua rotina de trabalho as regras para criação, coleta, inventário, classificação, rotulagem, manuseio, compartilhamento e descarte de informações e outros ativos associados, conforme diretrizes desta Política e outros documentos aplicáveis;

f. adotar senhas fortes em suas contas de acesso para e-mails, sistemas, serviços de TIC e estações de trabalho;

g. nunca compartilhar suas senhas em nenhuma hipótese;

h. habilitar a autenticação multifatorial (MFA) sempre que este recurso estiver disponível;

i. ter ciência de que todas as contas de e-mail, sistemas, serviços de TIC, dispositivos, diretórios em nuvem etc. (“recursos de TIC”) pertencentes ao MGB estão sujeitas ao monitoramento contínuo e auditoria sem aviso prévio. Sendo, portanto, desaconselhada a utilização destes recursos para

o armazenamento, compartilhamento ou comunicação de informações pessoais do próprio colaborador;

j. nunca utilizar contas de e-mail, sistemas, serviços de TIC, dispositivos, diretórios em nuvem ou qualquer outro recurso do MGB para propósito impróprio ou ilegal.

k. ser cauteloso quanto a "*phishing*" e outras práticas similares e, por isso, não abrir e-mails, SMS ou outro tipo de mensagem de procedência duvidosa e/ou com assuntos duvidosos;

l. tratar informações pertencentes ao MGB exclusivamente através de recursos de TIC fornecidos ou homologados pela organização, em conformidade com esta Política e demais normas internas estabelecidas;

m. tratar dados pessoais de clientes, fornecedores e outras partes interessadas em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), sem prejuízo de outras legislações e regulamentos aplicáveis;

n. consultar o DPO sempre que houver dúvidas sobre um determinado tratamento de dados pessoais;

o. não utilizar sistemas, serviços de TIC, *softwares*, aplicativos ou qualquer outra solução "*as a service*" sem que tenham sido previamente homologados pelo Departamento de TI;

p. armazenar arquivos, documentos, códigos fonte etc. pertencentes ao MGB em sistemas, diretórios e dispositivos pré-determinados, conforme regras estabelecidas para governança de informações;

q. zelar pelo uso apropriado de recursos de TIC fornecidos pelo MGB em conformidade com normas internas e procedimentos estabelecidos;

r. quando autorizado a utilizar recursos próprios de TIC, prática conhecida como "*bring your own device*" (BYOD), fazê-lo exclusivamente dentro das regras e diretrizes previstas pelas normas internas e procedimentos estabelecidos;

s. adotar práticas de mesa limpa e tela limpa, guardar documentos e mídias contendo informações confidenciais em gavetas e armários com chave, evitando que informações confidenciais sejam expostas no ambiente de trabalho;

t. adotar medidas cabíveis para proteger as informações do MGB – em formato digital ou físico – contra acesso, modificação, destruição ou divulgação não autorizados, mesmo quando fora da organização, por exemplo em home office ou viagem;

u. reportar de imediato, através dos canais previamente aprovados e comunicados pelo MGB, qualquer suspeita de incidentes relacionados à segurança da informação e privacidade;

v. relatar o descumprimento de políticas e regras por parte de outros colaboradores/prestadores; e denunciar qualquer comportamento suspeito que possa comprometer os esforços de segurança da informação e privacidade do MGB;

w. considerar que as diretrizes estabelecidas nesta Política e demais documentos adotados pelo MGB não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, os exemplos de medidas, procedimentos e protocolos de segurança da informação utilizados não representam um rol taxativo, cabendo a cada colaborador adotar, além daquelas aqui previstas, outras medidas que considerar necessárias para proteger as informações do MGB, mediante comunicação proativa sobre tais medidas.

6.5. A **Diretoria**, sem prejuízo dos deveres de todos os colaboradores/prestadores, deve**:**

a. liderar o tratamento da temática e comunicação sobre a importância de segurança da informação e privacidade para o MGB;

b. indicar ou aprovar os membros do CGSIP.

6.6. **Colaboradores/prestadores com função de liderança** no MGB, sem prejuízo dos deveres de todos os colaboradores/prestadores, devem:

a. promover a comunicação sobre a importância de segurança da informação e privacidade para o MGB aos seus liderados;

b. Quando indicados ao CGSIP, participar das reuniões e atividades do Comitê;

c. tomar ciência e informar ao CGSIP sobre questões, sobretudo legais e regulatórias, relativas à segurança da informação e privacidade que impactem processos e atividades de sua área de especialidade ou responsabilidade;

d. promover a seleção, contratação, mudança de contratação e desligamento de colaboradores/prestadores do MGB conforme diretrizes desta Política;

e. assegurar que nenhum colaborador sob sua liderança exerça suas funções e atividades sem o conhecimento desta Política e outros documentos de segurança da informação e privacidade aplicáveis;

f. formalizar a solicitação de acessos para seus liderados, observando que estes tenham sempre apenas o acesso necessário, pelo tempo necessário para o exercício de sua função;

g. salvo nos casos de dispensa não planejada e com efeito imediato, tomar medidas para que os acessos aos recursos de TIC utilizados pelo colaborador desligado do MGB sejam revogados e as contas bloqueadas;

h. responder, quando for de seu conhecimento, às dúvidas apresentadas por seus liderados, e encaminhá-las ao CGSIP sempre que não puder responder;

i. respeitar as bases legais e princípios estabelecidos pela LGPD para o tratamento de dados pessoais de seus liderados e demais colaboradores/prestadores do MGB.

6.7. O **Gerente de TI** do MGB, sem prejuízo dos deveres de todos os colaboradores/prestadores e da liderança, deve:

a. assegurar que o MGB cumpra com os objetivos de segurança da informação e privacidade estabelecidos pela organização, e informar à Diretoria caso, por qualquer motivo, acredite que algum objetivo não está sendo ou será cumprido;

b. assegurar que o MGB, através de colaboradores/prestadores ou empresas prestadoras de serviços especializados, conte com todas as competências para implementar e manter recursos tecnológicos dentro dos critérios previstos para mitigação de riscos, conforme plano de tratamento de riscos aprovado, no cumprimento de seus objetivos de segurança da informação e privacidade;

c. coordenar a elaboração, revisão e aprovação de procedimentos operacionais de TIC e desenvolvimento seguro;

d. coordenar os esforços para que o MGB possua medidas de segurança cibernética aptas a proteger informações confidenciais, dados pessoais e outros ativos associados de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação indevida ou qualquer outro tratamento inadequado ou ilícito;

e. coordenar a implementação, revisão e testes de *backups* para todos os sistemas, serviços de TIC e dispositivos que armazenem informações do MGB;

f. coordenar os esforços de resposta a incidentes e continuidade de negócios do MGB, com objetivo de assegurar a detecção, contenção, comunicação, resposta e recuperação de incidentes, além do cumprimento dos objetivos do ponto de recuperação (RPO) e de tempo de recuperação (RTO) estabelecidos;

g. elaborar e manter um plano para gestão de configurações e mudanças nos sistemas, serviços de TIC, dispositivos e outros ativos que tratem

informações do MGB, com o objetivo de evitar que mudanças de tecnologia possam impactar a operação ou o negócio, além de prevenir falhas advindas de softwares desatualizados ou equipamentos obsoletos;

h. supervisionar para que sejam utilizados apenas softwares licenciados e suportados por seus fabricantes;

i. atender colaboradores/prestadores, clientes e outras partes interessadas relacionadas ao MGB quanto às solicitações e questionamentos sobre segurança da informação e privacidade e informar ao CGSIP sobre a necessidade de buscar aconselhamento externo sempre que considerar necessário.

6.8. O **DPO** do MGB, sem prejuízo dos deveres de todos os colaboradores/prestadores e da liderança, deve:

a. manter conhecimento relevante e atualizado sobre: (i) a LGPD; (ii) outras legislações e regulamentos sobre privacidade e proteção de dados aplicáveis ao MGB; (iii) melhores práticas para proteção à privacidade; (iv) aspectos nas operações do MGB que possam impactar direitos e liberdades dos titulares de dados;

b. assegurar que seja elaborada e atualizada a documentação relevante para privacidade e proteção de dados, sobretudo aquela obrigatória para o cumprimento da LGPD e outros regulamentos aplicáveis ao MGB;

c. coordenar a revisão, quando aplicável, de documentos de segurança da informação e segurança cibernética quanto à privacidade e à proteção de dados pessoais;

d. agir com autonomia quanto à proteção dos interesses dos titulares de dados tratados pelo MGB, e comunicar ao CGSIP caso perceba cerceada tal autonomia;

e. mensurar a eficácia e a efetividade das medidas para proteção à privacidade implementadas pelo MGB;

f. monitorar as regras internas de privacidade e proteção de dados, obrigações previstas na LGPD e outros regulamentos aplicáveis quanto à sua observância por colaboradores/prestadores e fornecedores do MGB;

g. atuar como ponto de contato com a Autoridade Nacional de Proteção de Dados (ANPD), comprometendo-se em assegurar que o MGB responda às requisições ou medidas necessárias, também buscando orientações proativamente quando considerar apropriado;

h. atuar como ponto de contato entre o MGB e os titulares de dados, garantindo que requisições destes sejam atendidas dentro do prazo legal estabelecido e da melhor forma possível;

i. comunicar, dentro das determinações da LGPD, à ANPD e aos titulares de dados nos caso de um incidente ou violação que comprometa dados pessoais;

j. atuar como disseminador da cultura de privacidade e proteção de dados no MGB, prestando aconselhamento sobre melhores práticas e avaliando a consequência de decisões e operações cotidianas quanto ao tratamento de dados pessoais;

k. prover aconselhamento aos membros da liderança sobre questões relacionadas à privacidade e proteção de dados;

l. informar ao CGSIP sobre a necessidade de buscar aconselhamento externo sempre que considerar necessário.

7. GESTÃO DE RISCOS

7.1. Os esforços de segurança da informação e privacidade do MGB devem ser governados por um processo de gestão de riscos conforme metodologia estabelecida pelo **Plano para Gestão de Riscos de Segurança da Informação e Privacidade**, através da qual riscos são identificados, analisados quanto a sua probabilidade e consequência, avaliados quanto aos critérios estabelecidos e determinado um plano de tratamento, que deve ser executado conforme apropriado.

7.2. Convém que avaliações de riscos de segurança da informação e privacidade sejam repetidas a cada 12 meses, sempre que houver uma mudança significativa no ambiente de negócios, ou quando for deliberada como relevante pelo CGSIP.

7.3. O plano de tratamento de riscos do MGB deve prever a implementação de controles de segurança da informação e privacidade aplicáveis à organização, levando em conta *frameworks* e melhores práticas reconhecidos de mercado.

7.4. Convém que o MGB implemente e mantenha ferramentas tecnológicas aptas a mitigar os riscos avaliados a um nível aceitável.

8. GESTÃO DE MUDANÇAS

8.1. Convém que todas as mudanças que possam causar impacto para estratégias, objetivos ou operação do MGB, incluindo mudanças de processos, infraestrutura, ferramentas, softwares, sistemas e serviços de TIC, sejam planejadas, avaliadas,

testadas, autorizadas pelo CGSIP, implementadas e monitoradas de forma controlada, minimizando consequências negativas para a organização.

8.2. Sempre que possível, as mudanças devem ser planejadas para mitigar potenciais riscos de interrupção ou degradação de serviços e operações da organização, considerando elementos como redundância de recursos e implementação em horários alternativos, como finais de semana, ou períodos de menor atividade, como feriados prolongados.

8.3. Mudanças de sistemas operacionais e softwares devem ser planejadas observando o encerramento do suporte do fabricante (*end of life* ou EOL) ao respectivo software, mitigando brechas provocadas por vulnerabilidades conhecidas sem correção disponível.

8.4. Convém que todas as mudanças estejam previstas por procedimentos, planos ou projetos documentados e aprovados internamente pela liderança responsável.

8.5. Convém que mudanças não controladas sejam mapeadas periodicamente e gerenciadas por meio de procedimentos específicos para cada cenário, sempre considerando os potenciais riscos para a organização.

8.6. Mudanças emergenciais, nas quais não seja possível seguir as regras e procedimentos existentes, devem ser documentadas e, posteriormente, avaliadas pelo CGSIP.

9. INFORMAÇÃO DOCUMENTADA

9.1. O MGB deve determinar, elaborar, revisar, aprovar e controlar políticas, normas internas, planos, procedimentos, inventários, modelos, imagens, fluxogramas, termos, regras, instruções, relatórios e outros documentos que, em conjunto com esta Política, sejam considerados necessários para atender aos objetivos de segurança da informação e privacidade e seu suporte ao cumprimento dos objetivos de negócio.

9.2. Convém que todas as informações tratadas pelo MGB sejam inventariadas, identificando seu proprietário, ativos associados, usuários ou departamentos autorizados para acesso, regras para classificação, armazenamento, compartilhamento, arquivamento, descarte e controles de segurança no documento **Inventário de Informações e Processos de Negócio**.

9.3. O proprietário da informação é o responsável direto por aquela informação. Por exemplo: o gestor de um determinado departamento é o proprietário das informações daquele departamento.

9.4. Todos os dados pessoais tratados pelo MGB em suas atividades de negócio, assim como o processo para coleta, responsabilidade pelo tratamento das informações, regras para armazenamento, compartilhamento, arquivamento e descarte, e bases legais mapeadas para cada atividade, devem constar no documento **Registro de Operações de Tratamento de Dados Pessoais.**

9.5. Todos os sistemas e serviços de TIC pertencentes, controlados ou utilizados pelo MGB devem constar no **Inventário de Sistemas, Serviços de TIC e Softwares**.

9.6. Convém que outros inventários sejam considerados para os demais ativos de TIC do MGB conforme apropriado.

9.7. Convém que todos os inventários sejam atualizados no máximo a cada 12 meses e mantidos relevantes para os objetivos de segurança da informação e privacidade alinhados ao negócio do MGB.

10. ACESSO À INFORMAÇÃO

10.1. O MGB deve adotar medidas adequadas para proteger e controlar o acesso às informações de sua propriedade, de seus clientes e outras partes interessadas, sobretudo quando classificadas como informações confidenciais.

10.2. O acesso às informações pertencentes ao MGB, ou tratadas sob sua responsabilidade, deve ocorrer exclusivamente através de identidades homologadas pela organização.

10.3. A criação, gestão, proteção, monitoramento, revogação, desativação e exclusão de identidades e acessos às informações, infraestrutura, sistemas e serviços de TIC mantidos pelo MGB devem ocorrer conforme autorizado pelo proprietário da informação, respeitando princípios e regras desta Política.

10.4. Convém que acessos atribuídos sejam baseados nos seguintes princípios de segurança:

a. necessidade de conhecer (*need-to-know*): uma entidade só tem acesso às informações que requer para executar suas tarefas;

b. menor privilégio ou necessidade de uso (*least privilege)*: todo acesso para uso de um recurso deve ser atribuído com o menor privilégio possível para execução da tarefa pretendida;

c. acesso sob demanda (*just-in-time*): acessos devem ser liberado apenas pelo tempo necessário para execução das tarefas pretendidas.

10.5. Todos os acessos privilegiados devem ser devidamente justificados, autorizados pelo proprietário da informação, atribuídos, sempre que possível, seguindo os princípios de segurança anteriormente mencionados e documentados no **Inventário de Sistemas, Serviços de TIC e Softwares,** incluindo a descrição dos privilégios concedidos.

10.6. Convém que sejam mantidas um mínimo de duas e um máximo de quatro contas de usuário com privilégios administrativos máximos (geralmente referenciados como “system admin”, “global admin”, “superusuário” ou “root user”) para todos os sistemas e serviços de TIC em uso pelo MGB.

10.7. Recursos de complexidade de senhas e autenticação multifatorial (MFA) devem ser habilitados para todas as identidades e acessos do MGB, sempre que estiverem disponíveis.

10.8. Convém que sistemas e serviços de TIC que não suportam MFA não sejam contratados ou sejam substituídos por soluções que suportem este recurso.

10.9. Registros (“*logs*”) de acessos bem-sucedidos e de tentativas malsucedidas devem ser mantidos por um período mínimo de 30 dias, conforme recursos disponíveis de cada sistema.

10.10. Convém que identidades e acessos sejam revisados regularmente pelo Departamento de TI para assegurar que usuários inativos e acessos não mais necessários sejam desabilitados.

11. CICLO DE VIDA, CLASSIFICAÇÃO E ROTULAGEM DA INFORMAÇÃO

11.1. Convém que toda informação criada, coletada, armazenada, acessada, utilizada, modificada, compartilhada, arquivada ou descartada, por qualquer colaborador ou recurso de TIC em nome do MGB seja inventariada, classificada, criptografada, protegida

e disponibilizada corretamente e com segurança, conforme diretrizes e regras desta Política e de outros documentos internos aplicáveis.

11.2. Conforme a ISO/IEC 27005:2022, informações, assim como os processos de negócio ligados diretamente a elas, devem ser considerados ativos primários para o MGB, enquanto ativos como colaboradores/prestadores, fornecedores, infraestrutura, dispositivos, sistemas e serviços de TIC são considerados ativos de suporte, referenciados nesta política também como ativos associados.

11.3. O proprietário da informação é o responsável direto por aquela informação. Por exemplo: o gestor de um determinado departamento é o proprietário das informações daquele departamento.

11.4. Convém que a classificação ocorra o quanto antes no ciclo de vida da informação, de forma que seja possível a aplicação de controles apropriados para sua proteção e de seus ativos associados.

11.5. Toda informação que não for explicitamente classificada como pública, ou que não esteja publicamente disponível em sites ou redes sociais, deve, por padrão, ser tratada como informação confidencial.

11.6. O tratamento como informação confidencial deve ser mantido até que haja uma reclassificação formal, ou autorização expressa para divulgação em outro nível de confidencialidade.

11.7. Toda informação pertencente ao MGB e seus ativos associados deve ser armazenada, acessada, utilizada, modificada, arquivada, descartada e destruída conforme regras previstas nesta Política.

11.8. O esquema de classificação de confidencialidade de informações foi determinado levando-se em conta o valor estratégico da informação para o MGB, requisitos legais, regulatórios, contratuais e de partes interessadas ligadas à organização, e o dano potencial financeiro, operacional e reputacional caso a informação seja divulgada.

11.9. Os rótulos para classificação de ativos de informação pertencentes ao MGB são:

Rótulo	Definição / Exemplo
Pública	Informação cuja revelação causa danos aos negócios da organização, desde que observada sua integridade. Dados

	de domínio público e que podem ser divulgados livremente. **Exemplo:** informações disponíveis no site.
Interna / Uso Interno	Informação que pode ser divulgada para todos os colaboradores/prestadores e prestadores de serviços. Entende-se que divulgar estas informações publicamente pode causar dano de menor potencial aos interesses e objetivos de negócio da organização. **Exemplo:** políticas e procedimentos internos.
Confidencial	Informação de caráter sigiloso, que deve ser conhecida apenas por determinados indivíduos ou departamentos dentro da organização, que necessitem do acesso a esta informação para o exercício de suas atividades ("*need-to-know*"). Entende-se que a divulgação indevida destas informações causará danos significativos de curto ou médio prazo aos objetivos de negócio, interesses ou operações da organização. **Exemplos:** informações específicas de um determinado departamento como folha de pagamento, procedimentos de TI etc.
Secreta	Informação de caráter altamente sigiloso, que deve ter seu acesso controlado, podendo ser acessada apenas por indivíduos especificamente relacionados. Sempre deve ser avaliado criticamente quem pode ter acesso, através de quais meios ela será acessada e quais controles existem para proteger sua confidencialidade e integridade. Entende-se que a divulgação indevida de informações classificadas como secretas tem uma séria consequência negativa para os objetivos e interesses de longo prazo da organização, podendo colocar a existência do negócio em risco. **Exemplo:** planejamento estratégico de longo prazo.

11.10. Informações classificadas como confidenciais e secretas podem ser referenciadas coletivamente como informações confidenciais. Quando algo for aplicável apenas a informações secretas ou requerer este nível de confidencialidade, este deve ser referenciado especificamente.

11.11. Convém que a classificação de informações ocorra através da aplicação dos rótulos relacionados:

a. aos cabeçalhos ou rodapés de todos os documentos pertencentes ao MGB;

b. conforme *template* aprovado para elaboração do documento;
c. através de marcas d'água aplicada a informações classificadas como secretas;
d. rótulos de confidencialidade do Microsoft 365.

11.12. A classificação da informação deve ser realizada pelo proprietário da informação. Esta atividade pode ser delegada, mas o proprietário da informação continua sendo o responsável pela classificação e rotulagem.

11.13. Todo documento que contenha dados pessoais sensíveis deve ser classificado por padrão como confidencial.

12. ARMAZENAMENTO, UTILIZAÇÃO E MODIFICAÇÃO DE INFORMAÇÕES

12.1. Informações confidenciais devem ser armazenadas exclusivamente em infraestrutura, diretórios, sistemas, serviços de TIC, dispositivos e mídias previamente homologados pelo MGB.

12.2. Convém que toda informação mantida em qualquer meio digital de armazenamento controlado pelo MGB receba criptografia em repouso e em trânsito.

12.3. Toda informação tratada sob a reponsabilidade ou de propriedade do MGB deve estar sujeita a uma rotina de backup compatível com sua relevância para a organização, conforme determinado pelo **Plano de Resposta a Incidentes e Continuidade de Negócios**.

12.4. Convém que sempre que houver modificação em uma informação ou ativo associado, seja avaliado se a classificação atribuída permanece adequada.

13. COMPARTILHAMENTO, ARQUIVAMENTO E DESCARTE DE INFORMAÇÕES

13.1. Convém que o compartilhamento, sobretudo externo, de informações seja gerenciado e controlado conforme rótulos de classificação aplicados.

13.2. Informações classificadas como públicas podem ser compartilhadas livremente.

13.3. Informações classificadas como internas/uso interno podem ser compartilhadas com qualquer colaborador do MGB.

13.4. O compartilhamento interno de informações confidenciais deve ser realizado baseado na função do colaborador conforme sua necessidade de acesso ("*need-to-know*") a esta informação.

13.5. O compartilhamento interno ou externo de qualquer informação classificada como secreta deve ser explicitamente autorizado pela Diretoria do MGB.

13.6. Convém que seja evitado o compartilhamento de informações confidenciais como anexo de e-mails, e seja priorizado o compartilhamento via um link seguro para acesso ao documento ou a sua pasta.

13.7. Convém que nenhuma informação confidencial seja compartilhada com partes externas, como prestadores de serviços e parceiros comerciais, sem a assinatura de um Termo de Confidencialidade.

13.8. Convém que o arquivamento de informações esteja sujeito à análise prévia quanto a sua necessidade e conformidade com os objetivos de negócio do MGB e requisitos legais, regulatórios e/ou contratuais aos quais a organização esteja sujeita.

13.9. Convém que o arquivo morto seja mantido através de um diretório previamente homologado, com acesso controlado, prazo para retenção e recuperação conforme regras internas do MGB.

13.10. Convém que o arquivamento físico de informações impressas seja evitado e, caso necessário, ocorra em local seguro, trancado, com acesso controlado, monitorado por câmeras de segurança e respeitando o mesmo prazo para retenção de informações em formato digital.

13.11. Toda informação que não for mais necessária para as atividades operacionais, para os objetivos do negócio ou para o cumprimento de obrigações legais, regulatórias ou contratuais do MGB deve ser descartada e destruída de forma irrecuperável sob supervisão de seu proprietário ou líder do departamento ao qual a informação pertence através dos métodos descritos a seguir:

MÉTODO	DESCRIÇÃO	APLICABILIDADE

Excluir documentos ou pastas do diretório	Excluir documentos ou pastas que não sejam mais necessários.	Qualquer documento ou pasta em qualquer formato.
Excluir informações do sistema	Excluir informações do sistema.	Informações dos sistemas mantidos pela organização, listados nos inventários correspondentes.
Excluir e-mails ou mensagens do Microsoft Teams	Excluir e-mail/mensagem.	E-mails e mensagens do Microsoft 365 acessadas por contas corporativas.
Triturar de papel	Triturar documentos utilizando os trituradores de papel disponibilizados pela organização.	Documentos impressos classificados como internos, confidenciais ou restritos.
Remover disco	Remover e guardar ou destruir disco de computadores no caso de reaproveitamento do dispositivo.	Laptops, Computadores, Servidores etc.
Expurgar informações	Expurgar dados utilizando software específico homologado previamente.	HDs, SSDs, pen drives, CDs e DVDs que serão reaproveitados.
Aplicar criptografia de caminho único.	Uso de criptografia tipo "*one-way*" com algoritmo homologado previamente.	HDs, SSDs, pen drivers, CDs e DVDs que serão descartados.
Acionar remoção por organização especializada	Remoção do ativo por organização especializada em descarte seguro homologada.	Computadores, smartphones, servidores etc.
Destruir ativo fisicamente	Destruição física do ativo de forma irrecuperável, como através do uso de incineradores, ácido ou pulverizadores previamente homologados.	Qualquer ativo que não seja reaproveitado.

13.12. O descarte efetivo das informações, documentos e mensagens apenas será considerado após o prazo de retenção, conforme regras de backup previstas.

13.13. A necessidade de exclusão imediata de informações, documentos e mensagens de arquivos de backup está sujeita a análise de viabilidade técnica pelo Departamento de TI.

13.14. Convém que todos os documentos contendo informações confidenciais sejam triturados de forma irrecuperável antes do descarte.

13.15. Convém que quando reutilizados, dispositivos como computadores, laptops, smartphones, tablets, mídias removíveis etc. passem por procedimentos conforme métodos homologados para assegurar que os dados do MGB não possam ser recuperados por terceiros não autorizados.

13.16. Convém que dispositivos como computadores, laptops, smartphones, tablets, mídias removíveis etc. contendo informações do MGB sejam descartados de forma segura conforme regras desta Política.

13.17. Convém que o descarte e destruição física de computadores, dispositivos móveis ou mídias de armazenamento respeite as melhores práticas de sustentabilidade e responsabilidade ambiental.

14. CONFIDENCIALIDADE E NÃO DIVULGAÇÃO

14.1. Todos os colaboradores/prestadores e fornecedores devem estar cientes de seu compromisso com a confidencialidade das informações conforme esquema de classificação estabelecido pelo MGB.

14.2. O MGB deve assegurar que todos os colaboradores/prestadores e fornecedores assinem um acordo de confidencialidade e não-divulgação (por exemplo, através de cláusulas em contratos de trabalho, contratos de prestação de serviços ou termos específicos) que especifiquem como confidenciais todas as informações que:

- **a.** não sejam explicitamente classificadas como públicas ou estejam disponíveis em canais públicos (por exemplo, sites ou redes sociais);
- **b.** estejam disponíveis em quaisquer meios digitais (por exemplo, plataformas tecnológicas, sistemas, mídias e documentos digitais) ou físicos (por exemplo, documentos impressos, manuscritos, quadros e murais);
- **c.** sejam expressas oralmente em reuniões, conversas ou negociações presenciais, através de plataformas online ou telefone.

14.3. Deve ficar estabelecido que informações confidenciais incluem não apenas as do MGB, mas também aquelas de terceiros tratadas sob a responsabilidade da organização, como informações de colaboradores/prestadores, clientes, fornecedores e outras partes interessadas.

14.4. Deve ficar estabelecido que o compromisso com a confidencialidade não se extingue com o encerramento do contrato celebrado. O colaborador ou fornecedor permanece obrigado a manter esse compromisso de confidencialidade e sigilo conforme prazos determinados no acordo, abstendo-se, inclusive, de utilizar informações reveladas pelo MGB para benefício próprio ou de terceiros.

14.5. Para colaboradores/prestadores, os acordos de confidencialidade devem estabelecer que a não observância, inclusive por omissão, das disposições de confidencialidade será tratada como uma violação sujeita às punições previstas pelo processo disciplinar interno da organização.

14.6. Além disso, deve ficar estabelecido, tanto para colaboradores/prestadores quanto para fornecedores, que a violação do acordo de confidencialidade pode resultar em processos judiciais e ações indenizatórias por perdas e danos, sejam eles materiais, morais ou lucros cessantes. As responsabilidades civis, trabalhistas e criminais cabíveis serão consideradas, incluindo, mas não se limitando, às despesas advocatícias e custas judiciais decorrentes das violações mencionadas.

15. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

15.1. O MGB compreende privacidade e proteção de dados como uma extensão de seus esforços de segurança da informação, por isso promove a integração de toda a temática relacionada.

15.2. Todo tratamento de dados pessoais, incluindo a identificação, avaliação e mitigação de riscos para os titulares de dados, deve respeitar as bases legais e princípios previstos pela LGPD e ocorrer conforme regras desta Política e da Política de Privacidade estabelecida pelo MGB.

15.3. O tratamento de dados pessoais pelo MGB deve ser mapeado, para que possam ser identificados riscos para os titulares de dados e adotadas medidas apropriadas para mitigar estes riscos.

16. PROPRIEDADE INTELECTUAL

16.1. Todo ativo de propriedade intelectual do MGB, incluindo a propriedade industrial, marcas, patentes, segredos comerciais e direitos autorais, deve ser gerenciado, protegido e utilizado de forma responsável conforme diretrizes e regras determinadas e documentadas internamente.

16.2. Fica proibida a instalação, utilização ou distribuição de softwares que não possuam a devida licença ou autorização para uso, respeitando os contratos firmados, legislações e normas de propriedade intelectual aplicáveis.

17. USO SEGURO DE INTELIGÊNCIA ARTIFICIAL (IA)

17.1. O desenvolvimento, implementação, utilização e monitoramento de sistemas, serviços, ferramentas e recursos de Inteligência Artificial (“recursos de IA”) deve ser ocorrer conforme regras desta Política e outros documentos complementares do MGB, observando os objetivos da organização, a gestão de riscos e oportunidades, a criticidade das operações e a classificação das informações manipuladas.

17.2. Recursos de IA devem ser homologados pela Diretoria do MGB antes de serem implementados e/ou utilizados por qualquer colaborador da organização.

17.3. A utilização de recursos de IA para tomada de decisão automática deve ser previamente autorizada pela Diretoria do MGB.

17.4. Os colaboradores/prestadores devem revisar os conteúdos de textos, insights, imagens, entre outros elementos que sejam gerados por recursos de IA antes de utilizá-los em operações, sistemas, serviços, documentos e apresentações do MGB.

17.5. Todos os conteúdos gerados por recursos de IA incluindo, mas não se limitando a textos, insights e imagens, que sejam utilizados em operações, sistemas, serviços, documentos ou apresentações do MGB, devem conter um aviso claro e visível informando que tal conteúdo foi gerado, total ou parcialmente, por Inteligência Artificial.

17.6. A utilização de recursos de IA para o tratamento de dados pessoais deve ocorrem em conformidade com a Política de Privacidade e autorizada pela Encarregado(a) do MGB.

17.7. Convém a elaboração e documentação de procedimentos que prevejam orientações práticas, alinhadas a esta Política, para a gestão de recursos de IA, sempre que isso for considerado necessário.

17.8. Os colaboradores/prestadores devem ter ciência de que as diretrizes para o desenvolvimento, implementação, utilização e monitoramento de recursos de IA estabelecidas nesta Política e demais documentos complementares do MGB não se esgotam, dada a contínua e acelerada evolução das tecnologias de IA, suas aplicações, bem como o constante surgimento de novos riscos, vulnerabilidades, e considerações éticas específicas a este campo. Desta forma, os exemplos de medidas, procedimentos, protocolos de segurança, e balizas éticas para IA aqui mencionados não representam um rol taxativo, cabendo a cada colaborador que interaja com, desenvolva ou implemente soluções de IA, adotar, além daquelas aqui previstas, outras salvaguardas e práticas prudentes que considerar necessárias para proteger as informações do MGB, assegurar o uso responsável e ético da IA, e mitigar riscos emergentes, mediante comunicação proativa sobre tais medidas e percepções à Diretoria.

18. SEGURANÇA DE RECURSOS DE TIC

18.1. Compreende-se que informações confidenciais são tratadas e operações críticas são mantidas, predominantemente, através de recursos de TIC, como dispositivos *endpoint* (por exemplo, servidores, computadores, laptops, smartphones, tablets e óculos de realidade aumentada); componentes de redes e comunicação (por exemplo, firewalls, roteadores, switches e cabeamentos); softwares, sistemas, aplicações, plataformas digitais e soluções como serviço (*as a service*), que podem possuir provisionamento tanto local (*on-premises*), quanto off-site ou em nuvem.

18.2. Recursos de TIC devem ser adquiridos, contratados ou homologados conforme políticas e procedimentos internos alinhados aos riscos identificados, recursos de segurança disponíveis, melhores práticas reconhecidas e controles estabelecidos para cada cenário; sem prejuízo de fatores como eficácia e eficiência, conformidade legal e regulatória, aderência do mercado, facilidade de uso e economicidade.

18.3. Recursos de TIC devem ser inventariados, classificados, protegidos e controlados conforme a confidencialidade das informações por eles tratadas ou a criticidade das operações por eles mantidas.

18.4. Convém que o MGB implemente, sem prejuízo de outros controles referenciados nesta Política ou apontados por avaliações de riscos internas, os seguintes

controles de segurança cibernética para proteger seus recursos de TIC e informações por ela tratada, conforme aplicável para cada cenário:

a. recursos para gestão de identidades e acessos (IAM);
b. ferramentas para segurança de e-mails, mensageria e outros recursos do ambiente de trabalho digital;
c. recursos para criptografia em repouso e em trânsito de informações confidenciais;
d. recursos ou serviços para gerenciamento de vulnerabilidades;
e. firewalls, segmentação, VPNs e outros recursos aplicáveis para proteção de redes;
f. controles de acesso físico, câmeras de segurança, redundância de recursos e outros controles de segurança física;
g. softwares para proteção contra malware;
h. recursos para detecção e resposta automatizadas;
i. ferramentas para monitoramento e gestão de eventos de segurança;
j. recursos para backup e recuperação de informações;
k. recursos de tolerância a falhas e alta disponibilidade.

18.5. Os controles de segurança listados devem ser planejados e implementados conforme plano de tratamento de riscos aprovado para cada cenário. A não implementação de um controle planejado deve ser justificada e estar alinhada aos critérios para aceitação de riscos estabelecidos pela organização.

18.6. O MGB deve estabelecer documentos, processos e ferramentas adequados para a gestão e a proteção de identidades e acessos, sobretudo de acessos privilegiados. Estes controles devem incluir determinações sobre mecanismos de autenticação, autorização, monitoramento e auditoria; inclusive prevendo, sempre que possível, a implementação de recursos para autenticação multifatorial (MFA) como forma de mitigar acessos indevidos através do comprometimento de identidades da organização.

18.7. Todo desenvolvimento de sistemas conduzido pelo MGB deve observar melhores práticas de desenvolvimento seguro, sempre que possível com a adoção de frameworks reconhecidos de mercado para esta finalidade.

18.8. Todos os acessos privilegiados devem ser devidamente justificados, autorizados pelo proprietário da informação, atribuídos, sempre que possível, seguindo os princípios de segurança anteriormente mencionados e documentados em inventários ou sistemas previamente homologados para esta finalidade.

18.9. Convém que sejam mantidas um mínimo de duas e um máximo de quatro contas de usuário com privilégios administrativos máximos (geralmente referenciados como “system admin”, “global admin”, “superusuário” ou “root user”) para todos os sistemas e serviços de TIC em uso pelo MGB.

18.10. Convém que recursos de complexidade de senhas e autenticação multifatorial (MFA) sejam habilitados para todas as identidades e acessos do MGB, sempre que estiverem disponíveis.

18.11. Convém que sistemas e serviços de TIC que não suportam MFA não sejam contratados ou sejam substituídos por soluções que suportem este recurso.

18.12. Convém que registros (“logs”) de acessos bem-sucedidos e de tentativas malsucedidas sejam mantidos por um período mínimo de 30 dias, conforme recursos disponíveis de cada sistema.

18.13. Convém que identidades e acessos sejam revisados regularmente pelo Departamento de TI para assegurar que usuários inativos e acessos não mais necessários sejam desabilitados.

19. USO ACEITÁVEL DE RECURSOS DE TIC

19.1. O MGB deve estabelecer, documentar e promover regras e diretrizes para o uso aceitável de recursos de TIC disponibilizados pela organização aos sócios, colaboradores/prestadores, fornecedores e outras partes pertinentes, conforme apropriado.

19.2. Colaboradores/prestadores do MGB devem tomar ciência e, quando aplicável, receber treinamentos sobre regras e diretrizes para o uso aceitável de qualquer recurso de TIC disponibilizado, como contas de usuários para sistemas, contas de e-mail, computadores, laptops, smartphones, periféricos, entre outros. Estas regras devem incluir informações sobre como acessar, utilizar, manter, devolver e descartar tais recursos de TIC.

19.3. O uso de dispositivos do próprio colaborador para acesso a informações da organização e/ou exercício de atividades funcionais, prática conhecida como “*Bring Your Own Device*” (BYOD), pode ser permitido pelo MGB, desde que o dispositivo seja homologado através de procedimento interno previamente aprovado e sejam implementados controles de segurança adequados para mitigar eventuais riscos.

19.4. O acesso remoto a recursos de TIC, por exemplo, por colaboradores/prestadores trabalhando remotamente ou fornecedores que precisem realizar manutenção em um sistema, deve receber atenção especial na implementação de controles aptos a mitigar brechas de segurança cibernética.

20. SEGURANÇA FÍSICA E DE AMBIENTE

20.1. O MGB deve implementar melhores práticas de segurança da informação para o ambiente de trabalho, endereçando a segurança física de redes, dispositivos *endpoint*, mídias removíveis, multifuncionais, impressoras e outros periféricos.

20.2. Convém que o acesso físico às instalações e escritórios restritos (sem acesso ao público) mantidos pelo MGB esteja autorizado aos colaboradores/prestadores durante o horário previsto para realização de suas atividades funcionais, seja controlado e monitorado.

20.3. Convém que instalações e escritórios do MGB sejam monitorados por circuito fechado de TV (CFTV).

20.4. Convém que sejam estabelecidas como regras para impressão, guarda, arquivamento e organização de documentos impressos, alinhadas aos requisitos de confidencialidade, conforme esquema de classificação estabelecido pelo MGB, incluindo, por exemplo, regras para mesa limpa e tela limpa, e minimizando os riscos associados à exposição de informações confidenciais em meios impressos.

20.5. Convém que o MGB revise e aprove políticas e procedimentos de segurança física alinhados às necessidades de segurança da informação, considerando os seguintes controles, conforme aplicável para cada cenário:

- **a.** sistemas para controle de acesso físico a escritórios e instalações;
- **b.** serviços de segurança e vigilância;
- **c.** recursos para identificação de colaboradores/prestadores e visitantes;
- **d.** acesso de visitantes controlado e supervisionado;
- **e.** recursos para prevenção e mitigação de incêndios, ameaças ambientais e urbanas;
- **f.** sistemas de circuito fechado de TV (CFTV);
- **g.** redundância de links de internet;
- **h.** sistemas para prevenção e detecção de intrusos.

20.6. Convém que os CPDs do MGB:

a. sejam localizados em salas ou instalações dedicadas para esta finalidade;
b. estejam protegidos contra intempéries naturais, problemas estruturais e ameaças humanas;
c. sejam mantidos trancados e tenham seu acesso controlado e autorizado apenas a colaboradores/prestadores do Departamento de TI, membros da diretoria e fornecedores autorizados;
d. possuam recursos de tolerância a falhas provocadas pela interrupção de serviços essenciais como energia elétrica ou internet;
e. contem com recursos para de climatização e controle de umidade apropriados conforme padrões aceitos de mercado;
f. contem com câmeras de segurança cobrindo acessos e área interna com ponto e contraponto, conforme o necessário.

20.7. Convém que a impressão de informações confidenciais seja evitada.

20.8. Os colaboradores/prestadores devem atentar para não deixar documentos contendo informações confidenciais em impressoras, multifuncionais ou scanners.

20.9. Qualquer informação confidencial em formato físico, como impressa ou gravada em mídias como HD externo, pen drive, CD ou DVD, deve ser armazenada em cofres, armários ou gavetas trancados.

21. RELAÇÕES INTERNAS

21.1. O MGB deve gerenciar riscos na seleção, contratação, relações, mudança ou encerramento de contrato com colaboradores/prestadores conforme regras desta Política.

21.2. O MGB deve respeitar as bases legais e princípios estabelecidas pela LGPD para o tratamento de dados pessoais de todos os colaboradores/prestadores.

21.3. Convém que o processo de seleção para novos colaboradores/prestadores ocorra conforme melhores práticas reconhecidas de mercado para determinar a identidade do colaborador, qualificações alegadas e reduzir riscos para a organização.

21.4. Convém que o colaborador contratado pelo MGB assine, no ato de sua contratação, um termo onde constem:

- **a.** declaração de sua responsabilidade para com segurança da informação e privacidade;
- **b.** declaração de sua ciência sobre esta Política e outros documentos relevantes de segurança da informação e privacidade para sua função;
- **c.** declaração de seu compromisso em cumprir treinamentos sobre segurança da informação e privacidade;
- **d.** cláusulas de confidencialidade e não-revelação compatíveis com as informações às quais terá acesso;
- **e.** cláusulas relacionadas ao tratamento de dados pessoais, relevantes para a LGPD e outros regulamentos aplicáveis;
- **f.** cláusulas sobre regras de propriedade intelectual;
- **g.** declaração de sua concordância com regras estabelecidas para a mudança ou encerramento da contratação.

21.5. Deve ficar estabelecido que o compromisso com a confidencialidade não se extingue com o encerramento do contrato celebrado e que o colaborador permanece obrigado a manter este compromisso com o sigilo sobre informações recebidas por tempo indeterminado, inclusive abstendo-se de utilizar tais informações reveladas pelo MGB.

21.6. Convém que o MGB assegure que cada colaborador receba apenas os acessos estritamente necessários para suas funções, pelo tempo indispensável e com o menor privilégio possível para executar suas atividades, em conformidade com os princípios de necessidade de conhecer (*need-to-know*) e menor privilégio (*least privilege*).

21.7. O MGB pode permitir a utilização de dispositivos do próprio colaborador para acesso a informações e/ou exercício de atividades funcionais, prática conhecida como "*Bring Your Own Device*" (BYOD). Dispositivos BYOD devem ser homologados através de um procedimento interno aprovado pelo Responsável pelo TI.

21.8. Convém que o desligamento de qualquer colaborador seja informado com antecedência cabível ou imediatamente, em caso de dispensa não planejada, ao Departamento de TI para que os que acessos aos sistemas e recursos tecnológicos sejam revogados.

21.9. Em situações de mudança de cargo ou função, os acessos atribuídos ao colaborador devem ser ajustados à nova função, com a revogação dos acessos que não forem mais necessários, evitando o acúmulo de acessos (*access creep*).

21.10. Todo encerramento de contrato ligado a funções de segurança da informação e privacidade, tanto com colaboradores/prestadores quanto fornecedores, deve ser avaliado quanto ao seu impacto em atividades importantes ou efetividade de controles aplicados pela organização.

22. RELAÇÕES COM FORNECEDORES

22.1. A seleção, contratação, relações, mudança ou encerramento de contratação de fornecedores e prestadores de serviços pelo MGB deve ocorrer conforme regras desta Política.

22.2. Fornecedores identificados como operadores de dados pessoais, nos casos em que o MGB atuar como controladora, devem demonstrar conformidade com a LGPD e demais regulamentos aplicáveis. Essa comprovação deve ocorrer como parte da devida diligência promovida no ato da contratação e, de forma planejada, ao longo da prestação dos serviços contratados (devido cuidado).

22.3. Convém que o MGB promova a avaliação de riscos referente aos serviços contratados conforme o **Procedimento para Avaliação de Riscos na Contratação de Fornecedores** para determinar a contratação ou renovação de contratos com seus fornecedores, sobretudo com aqueles que acessam informações confidenciais ou fornecem serviços críticos para a organização.

22.4. Para fornecedores já contratados na data de emissão desta Política, convém que seja realizada uma avaliação de riscos conforme o **Procedimento para Avaliação e Riscos na Contratação de Fornecedores** para a renovação do contrato, priorizando fornecedores conforme criticidade e nível de acesso à infraestrutura de TIC crítica e informações confidenciais do MGB.

22.5. Convém que sejam considerados para os contratos com fornecedores que tratem informações confidenciais ou forneçam serviços críticos para o MGB seções e/ou cláusulas que abordem os seguintes tópicos conforme aplicável:

a. requisitos legais, regulatórios ou contratuais, como, por exemplo, referentes à privacidade e proteção de dados, ou propriedade intelectual, que possam estar relacionados ao contrato firmado;
b. cláusulas de confidencialidade e não-revelação adequadas à sensibilidade das informações tratadas;
c. adequação do fornecedor à LGPD e outras legislações e regulamentos aplicáveis para proteção da privacidade aplicáveis;
d. métodos e regras para compartilhamento e acesso de informações confidenciais;
e. Acordo de Nível de Serviço (*Service Level Agreement*, SLA na sigla em inglês) que estabeleça requisitos para os serviços prestados compatíveis com as obrigações legais ou contratuais do MGB;
f. requisitos de treinamento e conscientização de prepostos do fornecedor que tenham acesso a informações do MGB;
g. regras relacionadas a subcontratação, incluindo processo de devida diligência e controles que precisem ser implementados;
h. requisitos e procedimentos para gestão de incidentes de segurança da informação e privacidade, incluindo obrigações e prazo para notificação por parte do fornecedor em caso de incidente;
i. regras para a mudança ou encerramento da contratação, abordando inclusive a retenção, transferência ou exclusão de informações pertencentes ao MGB.
j. obrigação do fornecedor em apresentar políticas, normas, planos, procedimentos, relatórios de auditoria, relatórios de vulnerabilidades, testes de invasão ou outros documentos que evidenciem a implementação de controles para assegurar um nível adequado de segurança da informação e privacidade;
k. direito de auditar processos e controles do fornecedor relacionados ao escopo do contrato;
l. regras para retenção e descarte de informações pertencentes ao MGB durante e após o encerramento da contratação;
m. obrigação de o fornecedor colaborar com o MGB, fornecendo suporte necessário no caso de mudança ou encerramento da contratação.

22.6. Convém que em contratos com fornecedores que tratem dados pessoais de sócios, colaboradores/prestadores, clientes e outras partes interessadas do MGB, sejam consideradas também, além dos itens da cláusula anterior, seções e/ou cláusulas que abordem:

a. registro de operações de tratamento de dados pessoais (Record of Processing Activities, ROPA na sigla em inglês) de dados pessoais tratados conforme requisitos da LGPD e outras legislações e regulamentos aplicáveis;
b. acordo de processamento de dados (data process agreement, DPA na sigla em inglês);
c. dados para contato do encarregado de dados (DPO) do fornecedor;
d. relatório de impacto a proteção de dados pessoais (RIPD).

22.7. Os contratos de serviços em nuvem são geralmente predefinidos e por adesão. Por este motivo, na contratação de serviços em nuvem deve-se verificar se o provedor de serviços indica em seu termo de adesão e políticas publicadas atender às questões de segurança da informação e privacidade relevantes para os serviços contratados.

22.8. Para serviços em nuvem que armazenem informações confidenciais, provisionem infraestrutura ou cargas de trabalho críticas para o MGB, convém que sejam contratados apenas fornecedores com certificação ISO/IEC 27001:2022 e relatórios SOC 2 Type II atualizados, ou equivalentes.

22.9. Deve ser determinado como o MGB vai assegurar controles de segurança da informação e privacidade aplicáveis para os recursos que são de sua responsabilidade na contratação dos serviços, incluindo se conta com ferramentas tecnológicas, responsabilidades e qualificação da equipe interna ou contratada para gerenciar tais recursos.

22.10. O MGB deve determinar se o armazenamento de dados disponibilizado pelo fornecedor de serviços em nuvem ocorre em países ou regiões aprovados conforme requisitos para conformidade com a LGPD e outras legislações e regulamentos aplicáveis.

22.11. Convém que o MGB mantenha um inventário de fornecedores com fornecedores ativos, incluindo informações sobre o risco do fornecedor mapeadas.

22.12. Convém que fornecedores, sobretudo de elevada importância para o MGB, sejam monitorados e avaliados regularmente sobre aderência aos acordos firmados.

22.13. Convém que antes de comunicar ao fornecedor a mudança ou encerramento da contratação, seja determinado o impacto desta mudança para o MGB, levando em conta fatores como:

a. acessos mantidos pelo fornecedor a informações, infraestrutura ou serviços de TIC do MGB;
b. questões de propriedade intelectual;
c. equipamentos do fornecedor alocados nas premissas do MGB;
d. portabilidade de informações em caso de alteração do fornecedor ou internalização.

22.14. Caso trate-se de uma mudança de fornecedor, a transferência de informações e/ou serviços utilizados pelo MGB deve ser supervisionada e documentada pelo responsável direto pelo contrato com o fornecedor.

22.15. Convém que o MGB documente uma estratégia para alterar ou interromper o uso de serviços em nuvem, incluindo estratégias para troca de fornecedores e soluções alternativas.

22.16. Convém que seja avaliada a necessidade de se obter declaração formal do fornecedor quanto à exclusão de informações do MGB, conforme requisitos do contrato firmado.

23. RESPOSTA A INCIDENTES E CONTINUIDADE DE NEGÓCIOS

23.1. O MGB estabelece um **Plano de Resposta a Incidentes e Continuidade de Negócios** com objetivo de implementar controles aptos a detectar e responder a incidentes de segurança cibernética, assim como estar pronto para recuperar informações, infraestrutura, sistemas e serviços de TIC dentro dos objetivos de tempo de recuperação (RTO) e de ponto de recuperação (RPO) determinados.

23.2. Convém que o MGB defina e capacite um time de resposta a incidentes de segurança cibernética com colaboradores/prestadores da organização, que devem receber orientação, treinamento e realizar exercícios, conforme apropriado.

23.3. Convém que sejam estabelecidos planos de contingência para assegurar a continuidade operacional no caso de falhas e disrupções potenciais mapeadas para mudanças críticas para o MGB.

23.4. Convém que sejam estabelecidos planos de contingência para assegurar a continuidade operacional no caso de falhas e disrupções potenciais mapeadas para mudanças críticas para o MGB.

23.5. Convém que o MGB assegure que recursos de TIC sejam planejados, implementados, testados e monitorados para assegurar a continuidade de negócios em caso de incidente, violação ou qualquer disrupção.

23.6. Convém que sejam estabelecidos o objetivo de tempo de recuperação (RTO) e o objetivo de ponto de recuperação (RPO) para as infraestruturas, sistemas e serviços de TIC críticos para a organização.

23.7. Convém que o MGB planeje, implemente, teste e monitore controles de segurança capazes de garantir a continuidade de negócios em caso de incidentes graves, violações ou qualquer disrupção, estando aptos a recuperar informações e assegurar operações dentro do RTO e RPO estabelecidos para cada recurso de TIC.

23.8. O MGB deve estabelecer uma rotina cópias de segurança (“backups”) de documentos, sistemas, serviços de TIC e bancos de dados importantes para a organização.

23.9. Convém que backups sejam testados regularmente quanto a sua integridade e a capacidade de atender ao RTO e RPO estabelecidos.

23.10. Convém que o MGB mantenha redundância de toda infraestrutura de TIC considerada crítica para a organização.

23.11. Incidentes não-cibernéticos de segurança da informação e privacidade, como por exemplo, o vazamento de um documento impresso com informações confidenciais, devem ser tratados pelo CGSIP com objetivo de mitigar danos e cumprir com obrigações quanto à notificação de partes, conforme aplicável.

24. CONSCIENTIZAÇÃO E COMUNICAÇÃO

24.1. O MGB deve assegurar a comunicação e disponibilidade digital desta Política e de outros documentos da sua estrutura de segurança da informação e privacidade para os colaboradores/prestadores que precisam conhecê-los, e deve avaliar requisitos para comunicação com partes externas conforme legislações, regulamentos e contratos aplicáveis à organização.

24.2. O MGB deve assegurar que a comunicação de qualquer questão relativa à segurança da informação e privacidade ocorra em conformidade com requisitos e obrigações legais, regulatórias e contratuais.

24.3. O MGB deve promover a conscientização sobre segurança da informação e privacidade, assegurando que colaboradores/prestadores, fornecedores e outras partes interessadas estejam cientes de sua contribuição para os esforços de segurança da informação e privacidade da organização, e das implicações da não conformidade com os requisitos, políticas e diretrizes estabelecidos pela organização.

24.4. Todos os documentos de segurança da informação e privacidade devem ser comunicados a quem precisa conhecê-los e estar sempre disponíveis para os colaboradores/prestadores do MGB em um diretório digital com permissão de acesso conforme classificação do documento e direitos de acesso atribuídos.

24.5. O MGB deve promover treinamentos obrigatórios sobre segurança da informação e privacidade para todos os colaboradores/prestadores que abranjam os seguintes temas:

- **a.** técnicas, ferramentas e conhecimento comum aplicáveis sobre defesa cibernética para usuários, abrangendo temas como *phishing*, engenharia social, autenticação segura e uso aceitável de recursos de TIC;
- **b.** políticas e outros documentos de segurança da informação e privacidade aplicáveis;
- **c.** conhecimento sobre a LGPD e outros regulamentos para proteção da privacidade aplicáveis;
- **d.** orientações sobre identificação e relato de eventos que possam consistir em incidentes de segurança cibernética.

24.6. Os treinamentos obrigatórios devem ser gravados, atualizados regularmente, conforme o necessário, e fazer parte do processo de integração de novos colaboradores/prestadores.

24.7. Convém que outras medidas para promover a conscientização sobre segurança da informação e privacidade sejam consideradas, incluindo, mas não se limitando à contratação de plataformas de conscientização, realização de testes de *phishing* e uso de estratégias de gamificação.

24.8. Convém que o MGB considere a elaboração e promoção de treinamentos para funções específicas ou sobre temas relevantes para os objetivos de segurança da informação e privacidade, conforme apropriado.

25. PROGRAMA DE AUDITORIA

25.1. Convém que o MGB planeje, implemente e mantenha um programa de auditoria em segurança da informação e privacidade, compatível com as suas necessidades, incluindo diretrizes sobre frequência, métodos, responsabilidades, requisitos de planejamento, relatórios e tratamento de não conformidades.

26. TRATAMENTO DE EXCEÇÕES

26.1. As exceções para diretrizes e regras desta Política e outros documentos de segurança da informação e privacidade devem ser revisadas, aprovadas pelo CGSIP e documentadas.

26.2. Toda não conformidade com regras estabelecidas por esta Política deve ser avaliada e tratada, observando seu impacto para os objetivos de segurança da informação e privacidade do MGB.

26.3. Todo desvio de regras estabelecidas por esta Política deve ser avaliado para identificar se trata de um incidente ou violação de segurança da informação e privacidade.

27. PROCESSO DISCIPLINAR

27.1. As violações, mesmo que por mera omissão ou tentativa não consumada, desta Política, bem como das demais políticas, planos, normas e procedimentos de segurança da informação e privacidade, devem ser passíveis de penalidades conforme processo disciplinar interno da organização.

27.2. No caso de violações que infrinjam a legislação vigente, constituam atividades ilegais, incorram ou possam incorrer em dano ao MGB, o infrator será responsabilizado pelos prejuízos causados, cabendo aplicação das medidas judiciais e indenizatórias pertinentes, sem prejuízo de processo criminal quando aplicável.

27.3. No caso de prestadores de serviço e terceiros contratados, as sanções devem ocorrer conforme contrato estabelecido.

28. MELHORIA CONTÍNUA

28.1. O conteúdo desta Política e demais documentos de segurança da informação e privacidade deve ser revisado sempre que for considerado necessário, nunca ultrapassando 24 meses, e apenas pode ser modificado mediante a aprovação pelo CGSIP.

28.2. Convém que o desempenho dos esforços de segurança da informação e privacidade, incluindo os controles implementados pela organização, seja medido, monitorado, analisado e avaliado, levando em conta o que precisa ser mensurado, método que deve ser aplicado, quando os resultados devem ser analisados e quem deve analisar e avaliar estes resultados, mantendo todo o processo documentado.

28.3. Convém que o MGB analise criticamente e busque melhorar continuamente a pertinência dos seus objetivos, diretrizes e controles estabelecidos, bem como seu alinhamento contínuo ao seu propósito, cultura, objetivos de negócio e estratégia de mercado, levando em conta fatores como:

a. situação das análises críticas anteriores;
b. mudanças nas questões internas e externas;
c. mudanças no contexto do mercado de atuação da organização;
d. mudanças em legislações vigentes aplicáveis à organização;
e. resultados de avaliações de riscos;
f. situação de planos de tratamento de riscos;
g. não-conformidades e ações corretivas aplicadas;
h. estratégias, processos, tecnologias ou técnicas que possam melhorar o desempenho dos esforços de segurança da informação e privacidade da organização.

29. DOCUMENTOS COMPLEMENTARES

29.1. Esta Política não esgota em si todos os instrumentos que direcionam e regulamentam os esforços para assegurar a confidencialidade, integridade e disponibilidade de informações e outros ativos associados pertencentes ao MGB, ou tratados sob sua responsabilidade.

29.2. Esta política é diretamente complementada por outras políticas e planos relacionados a temas específicos, que podem ser complementados por normas internas, planos, procedimentos, inventários, modelos e outros documentos.

29.3. Os documentos mencionados ao longo desta Política, que a complementam diretamente são:

a. Inventário de Informações e Processos de Negócio;
b. Inventário de Sistemas, Serviços de TIC e Softwares;
c. Lista Mestre de Documentos de Segurança da Informação e Privacidade;
d. Plano de Resposta a Incidentes e Continuidade de Negócios;
e. Plano para Gestão de Riscos de Segurança da Informação e Privacidade;
f. Política de Privacidade;
g. Procedimento para Avaliação de Riscos na Contratação de Fornecedores
h. Procedimento para Registro das Operações de Tratamento de Dados Pessoais (RoPA)
i. Registro das Operações de Tratamento de Dados Pessoais (RoPA);
j. Termos e Definições de Segurança da Informação e Privacidade.

29.4. Deve ser mantido um inventário dos documentos de segurança da informação e privacidade do MGB na **Lista Mestre de Documentos de Segurança da Informação e Privacidade**.

29.5. No caso de conflito entre diretrizes estabelecidas por esta Política e qualquer outro documento relacionado à segurança da informação e privacidade, deve prevalecer o que está disposto nesta Política.

30. CONTROLE DE VERSÕES

Versão	Data	Responsáveis	Ações
1	13/06/2025	Rodrigo Lopes Demétrius Fernandes	▪ Elaboração inicial
1	30/06/2025	Leandro Corrêa	▪ Revisão geral do Departamento de TI
1	26/09/2025	Monique Campos	▪ Revisão Recursos Humanos
1	08/10/2025	Renato Bello Sergio Augusto de Resende	▪ Aprovação

Sérgio Augusto Guerra De Resende

Sérgio Augusto Guerra de Resende

CPF: 865.258.326-91

Renato Belo Pereira

CPF: 043.620.346-41

Relatório de Assinaturas

Datas e horários em UTC-0300 (America/Sao_Paulo)
Última atualização em 17 Outubro 2025, 14:53:12

Status: Assinado
Documento: MGB - Política Geral De Segurança Da Informação E Privacidade.Pdf
Número: d6165e27-038e-4203-90be-cd6acfc6a124
Data da criação: 10 Outubro 2025, 14:41:23
Hash do documento original (SHA256): dcdca54c04a4bd2ac414740061818ce1634159625ba81c661a806037d2e9094a

Assinaturas

2 de 2 Assinaturas

Assinado via ZapSign by Truora

RENATO BELO PEREIRA

Data e hora da assinatura: 10/10/2025 15:45:15
Token: 651bcd1d-58e1-43c8-8e0d-898389e909e3

Assinatura

RENATO BELO PEREIRA

Pontos de autenticação:

Telefone: + 5527996411814

E-mail: renato.bello@motorgroupbrasil.com.br

Localização aproximada: -19.961729, -43.956843

IP: 146.75.191.36
Dispositivo: Mozilla/5.0 (iPhone; CPU iPhone OS 18_6_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Mobile/15E148 Safari/604.1

Assinado via ZapSign by Truora

SÉRGIO AUGUSTO GUERRA DE RESENDE

Data e hora da assinatura: 17/10/2025 14:53:12
Token: e1bcf995-1cac-4ebe-8174-359b3951ba52

Assinatura

Sérgio Augusto Guerra de Resende

Pontos de autenticação:

Telefone: + 5531999813633

E-mail: sergio@gpvia.com.br
Nível de segurança: Validado por código único enviado por e-mail

IP: 187.1.183.61
Dispositivo: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36 Edg/141.0.0.0

INTEGRIDADE CERTIFICADA - ICP-BRASIL

Assinaturas eletrônicas e físicas têm igual validade legal, conforme MP 2.200-2/2001 e Lei 14.063/2020.
Confirme a integridade do documento aqui.

Este Log é exclusivo e parte integrante do documento número d6165e27-038e-4203-90be-cd6acfc6a124, segundo os Termos de Uso da ZapSign , disponíveis em zapsign.com.br