POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

1. OBJETIVO

Definir um conjunto de diretrizes estabelecidos pelo Grupo Financeiro Bmg para a preservação e proteção da informação e dados pessoais contra ameaças, incidentes e riscos relacionados à Segurança da Informação e Cibernética.

2. ESCOPO

Esta política aplica-se a todos os colaboradores, prestadores de serviços, fornecedores, parceiros, temporários e estagiários, abrangendo a informação em todo o seu ciclo de vida dentro do Grupo Financeiro Bmg.

3. DEFINIÇÕES E SIGLAS

No âmbito desta norma, considera-se:

- **Ativo:** Refere-se a qualquer bem que agregue valor ao negócio.
- **Informação:** Ativo essencial para os negócios do Grupo Financeiro Bmg. Conjunto de dados relacionados entre si que levam à compreensão de algo e que trazem conhecimento, sendo apresentada como imagens, áudios, vídeos, impressões, em meios digitais ou físicos.
- **Dado Sensível:** Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião pública, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico quando vinculado a uma pessoa natural.
- **Dado Pessoal:** Informação relacionada a uma pessoa natural identificada ou identificável, ou seja, qualquer Informação que possa identificar uma pessoa, tais como nomes, números, códigos de identificação, endereços.
- **Informação Relevante:** Qualquer informação que contenha dados pessoais ou sensíveis.
- **Serviços Relevantes:** Serviços prestados por terceiros que armazenam ou processam informações relevantes.

- **Gestor da informação:** Também conhecido como proprietário da informação, é o responsável por garantir a classificação e também o sigilo das informações produzidas ou alteradas por processos de sua área. É o responsável pelo sigilo das informações produzidas ou alteradas pelos processos de sua área.
- ***Chief Information Security Officer (CISO):*** Executivo responsável por desenvolver e implementar um programa de *Cybersecurity*, incluindo esta política, manuais e procedimentos relacionados com o objetivo de proteger as comunicações da empresa, sistemas e ativos tanto contra ameaças externas quanto de ameaças internas. O CISO também é o responsável por gerenciar situações de recuperação de incidentes e continuidade do negócio.
- **Fórum Executivo de *Cyber* Segurança, Privacidade e Prevenção a fraudes:** em relação à Governança da Segurança da Informação, existe um Comitê Executivo de TI, Segurança da Informação e Fraudes que visa administrar, acompanhar e deliberar sobre o alinhamento estratégico das ações do negócio quanto a esses temas.
- **Confidencialidade:** Garantia de que a informação não será acessada ou revelada a indivíduos, entidades ou processos não autorizados.
- **Integridade:** Garantia de que a informação não sofreu alteração indevida, assegurando a salvaguarda da exatidão e completeza da informação.
- **Disponibilidade:** Garantia de que a informação estará acessível aos colaboradores autorizados e aos órgãos reguladores sempre que necessário.
- **Autenticidade:** Garantia de que a informação, produto ou documento é do autor a quem se atribui certificado por instrumento ou testemunho público.
- **Irretratabilidade (não repúdio):** Impossibilidade de negar a autoria em relação a atos realizados anteriormente.
- **Legalidade:** Garantia de que ações sejam realizadas em conformidade com os preceitos legalmente estabelecidos e que seus produtos tenham validade legal e jurídica.
- **Ciclo de Vida da Informação:** Conjunto de etapas que compreendem a interação do usuário com a informação e onde devem ser aplicados controles a fim de evitar quebra de sigilo: recebimento, criação, cópia, armazenamento, transporte ou transmissão e descarte.
- **Segurança da Informação:** Proteção da Informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre o investimento e as oportunidades de negócio. A Segurança da Informação é aumentada a partir da implantação de uma série de controles na organização em ambientes, processos, pessoas e tecnologias.

- **Sigilo Bancário:** Direito, garantido por lei, de que todos os cidadãos têm resguardadas as suas movimentações bancárias.
- **Princípio do menor privilégio:** Aquele que preza por delegar somente os privilégios necessários para que uma pessoa possa realizar suas funções na organização.
- **Espaço Cibernético:** ambiente complexo resultante da interação de pessoas, software e serviços na internet por dispositivos de tecnologia e redes conectadas a ele, ao qual não existe em qualquer forma física.
- **Ataque:** Tentativa de destruir, expor, alterar, inutilizar, roubar ou obter acesso ou fazer uso não autorizado de um ativo.
- **Incidente de Segurança:** Qualquer evento não esperado que cause alguma interferência na operação do negócio, quebra de diretrizes desta política, normas e procedimentos relacionados que podem ou não causar danos ao Grupo Financeiro Bmg.
- **Vazamento de Informações Relevantes:** Vazamento de Dados é um tipo de incidente de Segurança que envolve informações Relevantes e compromete a: (i) confidencialidade; (ii) integridade; e (iii) disponibilidade. Dependendo das circunstâncias, um vazamento de dados pessoais pode envolver confidencialidade, integridade e disponibilidade de dados pessoais, isoladamente, ou qualquer combinação deles.
- **Log de dados:** Arquivo de texto gerado por um software para descrever eventos sobre o seu funcionamento.

4. RESPONSABILIDADES

4.1. DIRETORIA EXECUTIVA

- Assegurar as diretrizes desta política de forma a ser possível sua operacionalização no ambiente do Grupo Financeiro Bmg;
- Assegurar a cultura de segurança da informação através de um programa de conscientização e treinamento em segurança da informação;
- Assegurar e acompanhar as ações relacionadas a continuidade do negócio;
- Garantir os recursos necessários para a implantação dos controles de segurança da informação conforme as necessidades do negócio; e
- Avaliar criticamente esta política periodicamente.

4.2. FÓRUM EXECUTIVO DE CYBER SEGURANÇA, PRIVACIDADE E PREVENÇÃO A FRAUDES

- Gerenciar a implantação dos controles de Segurança da Informação, avaliando periodicamente por meio de indicadores, recomendações, ações corretivas e preventivas quanto ao ambiente do Grupo Financeiro Bmg;
- Planejar, orientar e controlar esta política, seus objetivos e diretrizes em alinhamento com as diretrizes do Grupo Financeiro Bmg;
- Planejar atividades com a finalidade de garantir a conformidade com requisitos de segurança da informação, alinhado ao processo de identificação, análise e tratamento dos riscos de segurança da informação;
- Comunicar a todos os stakeholders sobre a importância de atender à essa política através da observância de seus princípios, objetivos e atendimento às responsabilidades apresentadas;
- Promover avaliações e auditorias com foco em Segurança da informação e cibernética;
- Garantir recursos para implantação e operação da Segurança da informação e cibernética;
- Análise crítica, com o objetivo de avaliar a efetividade/eficácia, promovendo a melhoria contínua da segurança da informação e cibernética;
- Monitorar os incidentes de segurança cibernética de forma a promover a melhoria contínua do desempenho e de controles;
- Monitorar as violações às políticas, normas e procedimentos de segurança da informação e segurança cibernética, observadas sua natureza e gravidade;
- Monitorar, analisar, avaliar criticamente e tratar os riscos de comprometimento da confidencialidade, integridade e disponibilidade dos ativos de informação de acordo com sua criticidade;
- Cumprir e observar os requisitos legais, regulamentares e estatutários pertinentes à Segurança Cibernética e os direitos de propriedade intelectual; e
- Definir controles para a prevenção e tratamento de incidentes, a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais o Grupo Financeiro Bmg.

4.3. SEGURANÇA DA INFORMAÇÃO

- Assegurar a efetividade dessa política, normas e procedimentos relacionados;
- Desenvolver um plano diretor de segurança da informação visando apresentar à diretoria as ações necessárias para operacionalizar esta política;

- Definir as diretrizes e gestão de acessos;
- Gerir os incidentes de segurança da informação (incluindo vazamento de informações relevantes) e segurança cibernética;
- Comunicar à diretoria, os incidentes de segurança, conforme os critérios adotados pelo Grupo Financeiro Bmg para escalonamento e classificação de criticidade;
- Fazer a gestão das vulnerabilidades do ambiente de tecnologia do Grupo Financeiro Bmg;
- Como medida de prevenção, executar e responder a testes de invasão;
- Detectar, e quando necessário responder a ameaças e ataques cibernéticos;
- Disseminar a cultura de segurança da informação através de treinamentos, campanhas de conscientização, eventos e conteúdo em outros meios de divulgação;
- Avaliar a maturidade da segurança da informação da organização, de prestadores de serviço e de parceiros.
- Atender a leis, normas, diretrizes e regulamentações referentes ao assunto Segurança da Informação;
- Atender auditorias internas e externas;
- Prover recursos suficientes para estabelecer um PDCA para os controles e procedimentos relacionados à Segurança da Informação e Cibernética;
- Revisar com periodicidade mínima anual esta política, planos de ação e resposta a incidentes em conformidade com a regulamentação CMN 4893-21; e
- Prestar informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros.

4.4. GOVERNANÇA E PRIVACIDADE DE DADOS

- Gerir os incidentes de Segurança da Informação e Cibernética em conjunto com a Gerência de Segurança da Informação;
- Notificar, quando necessário e exigido por lei, a Autoridade Nacional de Proteção de Dados e os titulares de Dados Pessoais; e
- Realizar o gerenciamento dos dados pessoais, sensíveis e corporativos do Grupo Financeiro Bmg.

4.5. PROPRIETÁRIO DA INFORMAÇÃO

- Garantir a classificação e o sigilo das informações produzidas ou alteradas pelos processos de sua área;
- Gerir os acessos aos sistemas a que sua área é responsável; e

- Garantir que sua (s) equipe (s), esteja (m) ciente (s) sobre a importância de conhecer e seguir as diretrizes de segurança da informação definidas através das políticas de segurança da informação, disponíveis na intranet.

4.6. COLABORADORES E PRESTADORES DE SERVIÇO

- Conhecer e cumprir as políticas, normas e procedimentos de Segurança da Informação;
- Responder por todo o prejuízo ou dano causado ao Grupo Financeiro Bmg em decorrência da não observação às diretrizes aqui referidas;
- Participar das campanhas de conscientização e treinamentos de Segurança da Informação;
- Responder única e exclusivamente por todas as ações executadas com sua identificação de acesso e proteger os ativos e informações que estejam sob sua custódia;
- Proteger as informações e reportar qualquer situação que represente desvio ou violação de segurança (incidentes de segurança da informação), sempre que os identificar, através dos canais específicos para essa finalidade;
- Estar comprometido com a confidencialidade dos dados alinhado com o acordo de sigilo e responsabilidade (NDA);
- Seguir essa política, normas, procedimentos e controles definidos para a prevenção e tratamento das informações, assim como normas e procedimentos relacionados a prestação de serviços à instituição; e
- Em suas atividades, seguir procedimentos e controles voltados ao tratamento e proteção de dados e informações e a prevenção e ao tratamento dos incidentes.

4.7. *COMPLIANCE*

- Após receber as informações, comunicar aos órgãos reguladores os incidentes de segurança, conforme exigências legais e os critérios adotados pelo Grupo Financeiro Bmg para escalonamento e classificação de criticidade;
- Buscar mecanismos de mitigação dos problemas e danos relacionados à imagem do Grupo Financeiro Bmg;
- Realizar o monitoramento regulatório e direcionar os normativos aplicáveis às áreas responsáveis pela avaliação dos riscos;
- Trabalhar para que as atividades do Grupo Financeiro Bmg estejam em conformidade com as normas; e
- Após receber as informações, comunicar ao Banco Central do Brasil sobre a contratação de serviços relevantes

de processamento, armazenamento de dados e de computação em nuvem.

4.8. FORNECEDORES

- Garantir a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações do Grupo Financeiro Bmg que processa ou armazena;
- Garantir o acesso aos dados e às informações do Grupo Financeiro Bmg que processa ou armazena.
- Assegurar o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados; e
- Atender a todos os requisitos de segurança da informação e cibernética, legais e regulatórios aplicáveis e outros estabelecidos pelas normas, regimentos e procedimentos definidas pelo Grupo Financeiro Bmg, autoridades, federações e órgãos reguladores.

4.9. AUDITORIA INTERNA

- Verificar o cumprimento desta política, normas e procedimentos relacionados à Segurança da Informação, e quando necessário, recomendar as ações corretivas necessárias;
- Avaliar os riscos estratégicos e negócio do Grupo Financeiro Bmg; e
- Avaliar e revisar a eficácia, suficiência e aplicação dos controles implementados pela instituição.

5. PRINCÍPIOS E OBJETIVOS DE SEGURANÇA

Esta política tem como premissa a proteção das informações da organização, seus clientes, colaboradores e partes interessadas de forma a preservar os seguintes princípios:

- **Confidencialidade:** Garantia de que a informação não será acessada ou revelada a indivíduos, entidades ou processos não autorizados.
- **Integridade:** Garantia de que a informação não sofreu alteração indevida, assegurando a salvaguarda da exatidão e completeza da informação.
- **Disponibilidade:** Garantia de que a informação estará acessível aos colaboradores autorizados sempre que necessário.

Apesar de definirmos estes como nossos princípios, não se exclui de nossas premissas a garantia de Autenticidade, Irretratabilidade (não repúdio) e Legalidade.

Além destes princípios, os objetivos de segurança da informação são estabelecidos e gerenciados pela organização através do seu Sistema de Gestão de Segurança da Informação.

6. DIRETRIZES

6.1. DIREITO DE PROPRIEDADE

Toda informação gerada ou processada pelo Grupo Financeiro Bmg, e que possua consenso das partes envolvidas, será considerada propriedade e ativo importante para o negócio, sendo de sua responsabilidade implementar controles que garantam níveis adequados de proteção.

6.2. SEGURANÇA ORIENTADA AO NEGÓCIO

As ações de segurança são planejadas e aplicadas de acordo com a identificação, avaliação e tratamento dos riscos associados com a perda de confidencialidade, integridade e disponibilidade da informação seguindo as diretrizes de negócios do Grupo Financeiro Bmg, produzindo resultados comparáveis, válidos e consistentes.

A disponibilidade, uso, acesso e proteção das informações e seus recursos devem ocorrer sempre de forma a preservar a continuidade e a competitividade do negócio do Grupo Financeiro Bmg.

6.3. ACORDO DE SIGILO E RESPONSABILIDADE (NDA)

Quando do ingresso de colaborador ou terceiro na organização, deverá ser atestado por meio do Acordo de Sigilo e Responsabilidade (NDA), o compromisso e aceite quanto ao cumprimento ao disposto nessa política, demais normas complementares e o conhecimento dos controles de Segurança da Informação, o qual está alinhado com as diretrizes gerais do Grupo Financeiro Bmg.

6.4. GESTÃO DE PERFIS DE ACESSO

Partindo do princípio do menor privilégio, ao colaborador e prestador de serviços do Grupo Financeiro do Bmg será concedido acesso aos recursos e ativos necessários à realização de suas funções na organização, sendo ele responsável pelo uso consciente de suas permissões e sigilo de sua senha e outras informações.
O gestor da informação, também conhecido como proprietário da informação, é o responsável por autorizar e revisar periodicamente o acesso aos sistemas relacionados à sua área, garantindo assim a aplicabilidade da política de Gestão de Acessos.

6.5. CLASSIFICAÇÃO, USO E O TRATAMENTO DA INFORMAÇÃO

As informações devem ser devidamente classificadas e rotuladas, independentemente de seu formato, meio de armazenamento, processamento ou transmissão/transporte.

Os colaboradores, prestadores de serviço, fornecedores e parceiros devem identificar, classificar, rotular e tratar de forma adequada as informações, de forma a manter o sigilo de acordo com classificação e a sensibilidade da informação, impedindo quaisquer tipos de acesso, alteração, cópia e destruição não autorizada, assim como qualquer forma de descarte inadequado.

Para a retirada de ativos que contenham informações críticas do Grupo Financeiro Bmg, sejam em meio físico ou eletrônico é necessária uma autorização dos responsáveis pelos ativos.

O Grupo Financeiro Bmg deve aplicar controles e ferramentas voltados para a rastreabilidade da informação e prevenção de perda de dados.

Toda informação produzida e armazenada no ambiente do Grupo Financeiro Bmg é considerada patrimônio e propriedade da instituição, sendo usada exclusivamente em seu interesse, portanto devendo estar adequadamente protegida, em qualquer que seja o meio de armazenamento, contra violação, alteração, destruição, acesso não autorizado e divulgação indevida. Os responsáveis por seu armazenamento, guarda e manuseio responderão por sua integridade, uso, tratamento ou a divulgação.

6.6. CULTURA E CAPACITAÇÃO EM SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

O Grupo Financeiro Bmg entende que um dos pontos mais importantes para proteção da Informação é a disseminação da cultura de Segurança da Informação, e por esse motivo implementa um programa de

conscientização e capacitação em segurança da informação, além de divulgar continuamente a política de Segurança da Informação e Cibernética, e outras normas relativas à segurança e proteção para todos os seus colaboradores, prestadores de serviços, fornecedores, parceiros, temporários, estagiários e público em geral.

O objetivo desse programa é fornecer aos colaboradores e prestadores de serviço do Banco Bmg o conhecimento necessário para proteger os ativos de tecnologia e as suas informações, além de criar engajamento quanto a Cultura de Segurança da Informação. São utilizados diferentes mecanismos para conscientização distribuídos em campanhas e ações programadas ao longo do ano, além de divulga orientações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros do Banco Bmg.

É de responsabilidade de seus colaboradores e prestadores de serviços do Grupo Financeiro Bmg a participação em todos os cursos de capacitação da temática de Segurança da Informação e Cibernética definidos como obrigatórios pela organização.

6.7. GESTÃO DE FORNECEDORES

Todos os fornecedores, prestadores de serviços, provedores e parceiros que processam e armazenam dados do Grupo Financeiro Bmg são submetidos à avaliação de controles de Segurança da Informação e Cibernética para que seja possível identificar sua maturidade quanto às diretrizes desta política e também definir suas responsabilidades e papéis dentro dos processos relacionados ao serviço que será prestado. Devem atender a todos os requisitos de segurança da informação e cibernética, legais e regulatórios aplicáveis e outros estabelecidos pelas normas, regimentos e procedimentos definidas pelo Grupo Financeiro Bmg, autoridades, federações e órgãos reguladores.

6.8. GESTÃO DE VULNERABILIDADES

O processo de Gestão de Vulnerabilidades é contínuo e sistêmico, ao qual efetua-se o diagnóstico de todo o ambiente tecnológico do Grupo Financeiro Bmg. Este diagnóstico busca a coleta de informações de forma a identificar as vulnerabilidades dos sistemas de informação, de acordo com as diretrizes estabelecidas na norma de Gestão de Vulnerabilidades.

6.9. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

O Grupo Financeiro Bmg possui diretrizes estabelecidas para a gestão e resposta dos Incidentes de Segurança da Informação e Cibernética, para que sejam tratados conforme as exigências legais, regulatórias e as melhores práticas de mercado, diminuindo os riscos e os impactos para a instituição.

Essas diretrizes estão definidas na Norma Operacional Gestão de Incidentes de Segurança da Informação e Cibernética e no Plano de Reposta a Incidentes.
Qualquer incidente ou suspeita de incidente identificado por um cliente, colaborador, prestador de serviço, fornecedor ou parceiro, deve ser comunicado a área responsável através da caixa de e-mail corporativa (abuse@bancobmg.com.br) e, também através de nossos canais oficiais de atendimento.

6.10. GESTÃO DE CONTINUIDADE DO NEGÓCIO

O Grupo Financeiro Bmg adota processos para garantir a continuidade do negócio de acordo com as melhores práticas de mercado, incluindo em seu escopo processos e parceiros do negócio.

São estabelecidos e mantidos um processo de Gestão de Continuidade de Negócio, bem como procedimentos operacionais e testes periódicos de acordo com a sua necessidade, com foco em reduzir os impactos decorrentes da interrupção de serviços devido a desastres, crises, indisponibilidades ou falhas da segurança em seu ambiente ou ambientes de terceiros contratados.

7. PROCEDIMENTOS E CONTROLES DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

O Grupo Financeiro Bmg possui em seu ambiente controles e procedimentos de segurança da informação e cibernética, de forma a reduzir as vulnerabilidades e o impacto de ameaças, além de manter um monitoramento, registro e rastreabilidade quanto às atividades relacionadas ao tema. Também é adotado frameworks e tecnologias compatíveis com o grau de risco e criticidade das informações, além de ações relacionadas a proteção de todo o

ambiente tecnológico e cibernético, sempre com o objetivo de aumentar a segurança e proteção das informações de seus negócios, clientes, colaboradores, prestadores de serviço, fornecedores e parceiros.

Dentre os controles adotados, destaca-se, mas não se limitando a:

- Proteção e Prevenção a perda de dados: soluções de prevenção (DLP), proteção quanto a banco de dados (DBF), monitoramento (DAM), backup de dados, além de mecanismos de proteção como criptografia e classificação de informação;
- Controle de acesso e autenticação: gestão de identidades (IAM) e implementação de duplo fator de autenticação (MFA);
- Proteção de perímetros: soluções de prevenção e detecção de instrução (IPS/IDS), proteção de tráfego (*Firewall)*, proteção de aplicações (WAF), DDoS, CASB e *Proxy*;
- Proteção de ativos: soluções de proteção contra softwares maliciosos (AV), proteção contra mensagens maliciosas (ANTISPAM), proteção avançada (ATP/EDR); e
- Gestão de vulnerabilidades: utilização de ferramentas para varredura de vulnerabilidades de forma a tratá-las antes que sejam exploradas por ameaças. Os processos relacionados a esse tema são periódicos e sistêmicos.

O Grupo Financeiro Bmg também possui mecanismos para detecção de possíveis riscos cibernéticos através de soluções de SOC (Centro de Operações de Segurança) e Serviços de *Threat Intelligence* (Monitoramento de Riscos Cibernéticos), além de adotar iniciativas para compartilhamento de informações com as instituições e órgãos reguladores quanto aos incidentes relevantes identificados.

8. ANÁLISE CRÍTICA POR ALTA GESTÃO

O Grupo Financeiro Bmg se compromete com a melhoria contínua das diretrizes definidas nesta política. Este comprometimento é garantido através da realização periódica de análise crítica por parte da Alta Gestão.

9. *COMPLIANCE* E DIREITO DE PROPRIEDADE INTELECTUAL

O Grupo Financeiro Bmg busca evitar a violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e cibernética. Tais requisitos são identificados, documentados e mantidos atualizados para cada sistema de informação da organização.

Procedimentos adequados são implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais relacionados com os direitos de propriedade intelectual e sobre o uso de produtos de softwares proprietários.

10. MELHORIA CONTÍNUA

O Grupo Financeiro Bmg busca melhorar continuamente o seu Sistema de Gestão da Segurança da Informação, através de ações para analisar criticamente, controlar, determinar as causas e corrigir as não conformidades identificadas, e implementar oportunidades de melhorias, tratar consistentemente riscos, vulnerabilidades e incidentes de segurança da informação, através de controles apropriados e alinhados com as diretrizes dessa políticas e outras definidas pela organização.

11. AUDITORIA E MONITORAMENTO

O Grupo Financeiro Bmg se reserva no direito, em qualquer tempo e sem necessidade de aviso prévio de monitorar, auditar e intervir nos recursos fornecidos, e executar auditoria em ativos, processos e serviços, além de monitorar a utilização de sistemas e informações acessadas interna ou externamente, acessos de dados que trafegam na internet, logs de transações, entre outros que fizerem necessário de modo a salvaguardar os interesses corporativos de acordo com as legislações, normas e resoluções aplicáveis, no intuito de garantir a confidencialidade, integridade e disponibilidades das informações.

12. SANÇÕES

Em nenhum momento será admitido a qualquer colaborador ou prestador de serviço do Grupo Financeiro Bmg, alegar o desconhecimento desta política, normas e procedimentos de segurança para justificar violações ou descumprimentos.

Todo e qualquer caso de descumprimento ou inobservância desta política será passível de aplicação de sanções disciplinares, conforme normas internas existentes e aplicáveis.