POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

ÍNDICE

Este documento contém informação PÚBLICA. Destes do conteúdo que estão sendo compartilhados e utilizados são fiéis aos princípios da CID. Em caso de modificação do conteúdo ou compartilhamento fora do contexto original a classificação da informação quanto a sua sensibilidade deve ser reavaliada

1. OBJETIVO

A Política de Segurança da Informação e Cibernética tem como objetivo formalizar os conceitos e as diretrizes que visam à proteção dos ativos de informação e de dados pessoais com eficiência e eficácia, de modo seguro e transparente, garantindo a confidencialidade, integridade e disponibilidade das informações de propriedade ou sob a guarda do Grupo Financeiro Bmg.

Também são objetivos desta Política:

- Proteger o valor e a reputação da instituição;
- Identificar violações de segurança cibernética, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e lógicos, objetivando a mitigação dos riscos cibernéticos;
- Assegurar através de mecanismos de controle de acesso que as informações de propriedade do Grupo Financeiro Bmg sejam acessadas e utilizadas apenas para as finalidades e pessoas devidamente autorizadas;
- Implementar controles de forma a prevenir o vazamento e uso indevido de informações ou outras vulnerabilidades através de procedimentos e controles tecnológicos;
- Garantir a continuidade de seus negócios, protegendo os processos críticos de interrupções causadas por incidentes cibernéticos ou desastres significativos;
- Atender aos requisitos legais, regulamentares e às obrigações contratuais pertinentes a atividade da instituição;
- Conscientizar, capacitar e treinar os colaboradores a respeito da segurança cibernética;
- Melhorar e monitorar continuamente o sistema de gestão de segurança da informação.

Além disso, os objetivos de segurança da informação e cibernética estão estabelecidos e gerenciados pela instituição através do seu próprio Sistema de Gestão de Segurança da Informação (SGSI).

2. PÚBLICO ALVO

Esta Política se aplica a todos os colaboradores, sejam eles diretores, executivos, gestores, funcionários, estagiários, aprendizes, prestadores de serviços, consultores, fornecedores, parceiros e demais que tenham ou venham a ter acesso aos dados e aos sistemas de informação controlados pelo Grupo Financeiro Bmg.

Mantendo também esta Política disponível e publicada para órgãos integrantes do sistema financeiro nacional, instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil, entidades de classe e público em geral.

3. PRINCÍPIOS DE SEGURANÇA

Esta política tem como premissa a proteção das informações da instituição de forma a preservar os seguintes princípios:

- Confidencialidade: garantir que as informações são disponibilizadas ou divulgadas apenas a indivíduos, entidades ou processos autorizados;
- Integridade: garantir que as informações são precisas, completas e protegidas de alterações indevidas, intencionais ou acidentais;
- Disponibilidade: garantir que as informações são acessíveis, bem como utilizáveis sob demanda por indivíduos, entidades ou processos autorizados.

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

Desta forma, a proteção e a privacidade dos dados controlados pelo Grupo Financeiro Bmg refletem os valores da instituição e reafirmam o seu compromisso com a melhoria contínua da eficácia do processo de Proteção de Dados.

4. DEFINIÇÕES E SIGLAS

No âmbito desta norma, considera-se:

- **Ativo:** Refere-se a qualquer bem que agregue valor ao negócio.
- **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.
- **Dado Sensível:** Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião pública, filiação a sindicato ou a instituição de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico quando vinculado a uma pessoa natural.
- **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.
- **Informação Relevante:** Qualquer informação que contenha dados pessoais ou sensíveis.
- **Sigilo Bancário:** Direito, garantido por lei, de que todos os cidadãos têm resguardadas as suas movimentações bancárias.
- **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.

- ***Backup*:** Cópia de segurança realizada por meio de reprodução e/ou espelhamento de uma base de arquivos, com capacidade de recuperação plena em caso de incidente, necessidade de restauração ou qualquer outra justificada pelo Bmg.
- **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 instituição em ambientes, processos, pessoas e tecnologias.
- **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.
- **Princípio do menor privilégio:** Aquele que preza por delegar somente os privilégios necessários para que uma pessoa possa realizar suas funções na instituição.
- **Serviços Relevantes:** Serviços prestados por terceiros que armazenam ou processam informações relevantes.
- **Risco:** Combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos.
- **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.
- **Ameaça:** Risco ou potencial perigo de incidente que pode resultar em dano a instituição.
- **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.

Este documento contém informação PÚBLICA. Desde de conteúdo que estão sendo compartilhados e utilizados são forma os princípios da CID. Em caso de modificação de conteúdo ou compartilhamento fora do contexto original a classificação da informação quanto a sua sensibilidade deve ser reavaliada.

- **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.
- **PCN:** Plano de Continuidade dos Negócios.

5. RESPONSABILIDADES

5.1. 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.

5.2. 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;

Este documento contém informação PÚBLICA. Dentro do contexto que estão sendo compartilhadas e utilizadas são foram os princípios da CID. Em caso de modificação do conteúdo ou compartilhamento fora do contexto original a classificação da informação quanto a sua sensibilidade deve ser reavaliada.

- 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.

5.3. GERÊNCIA DE *CYBER SECURITY*

- 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 instituição, 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.

5.4. 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.

5.5. GESTOR DA INFORMAÇÃO

- Garantir e definir o nível de classificação e o sigilo das informações produzidas ou alteradas pelos processos de sua área;
- Avaliar a necessidade e, se for o caso, definir critérios para reclassificação de suas informações;
- 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 no site e sistemas internos.
- Avaliar o impacto no negócio quando da classificação e reclassificação da informação;
- Decidir sobre o compartilhamento das informações sob sua gestão, monitorar o uso e tomar ações para prevenir e/ou interromper o uso indevido, considerando os atributos da confidencialidade, integridade e disponibilidade da informação;
- Estruturar e manter atualizado o Inventário dos ativos de informação (documentais e informacionais eletrônicos e não eletrônicos);

- Atentar para as particularidades da rede externa e entidades ligadas ao Grupo Financeiro Bmg referentes ao acesso de terceiros, observadas as orientações do Gestor responsável pelo relacionamento com esses entes.

5.6. COLABORADORES E PRESTADORES DE SERVIÇO

- Conhecer e cumprir as políticas, normas e procedimentos de Segurança da Informação e Cibernéticas;
- Responder por todo o prejuízo ou dano causado ao Grupo Financeiro Bmg em decorrência da não observação às diretrizes referidas nesta Política e demais normas;
- Participar imprescindivelmente das campanhas de conscientização, capacitação e treinamentos de Segurança da Informação e Proteção de Dados;
- 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 das informações alinhado e formalizado através de acordo de sigilo e responsabilidade (NDA);
- Em suas atividades, seguir procedimentos e controles voltados ao tratamento e proteção de dados e informações e a prevenção e ao tratamento dos incidentes.
- Fazer uso das informações do Banco Bmg somente no interesse do serviço, observadas as limitações contratuais, não podendo utilizar, acessar, reproduzir, transportar, transmitir e distribuir tais informações sem expressa autorização do gestor da informação e do gestor do contrato no Banco Bmg;
- Tratar as informações do Banco Bmg às quais tiver acesso, de acordo com critérios de tratamento da informação definidos conforme sua classificação;
- Não utilizar equipamentos, informações e os sistemas informatizados do Banco Bmg para assuntos pessoais ou privados ou que extrapolem o estritamente previsto no contrato;
- Manter sigilo sobre as informações do Banco Bmg e direcionar cuidados adicionais com informações que envolvam especificações técnicas ou comerciais, inovações e aperfeiçoamentos dos produtos, serviços ou processos às quais venha a tomar conhecimento, ou que lhe venham a ser confiadas, não podendo, sob qualquer pretexto reproduzir, transmitir e distribuir tais informações sem que haja expressa autorização do gestor da informação e do gestor do contrato;

Este documento contém informação PÚBLICA. Destes do conteúdo aqui estão sendo compartilhados e utilizados são frente os princípios da CID. Em caso de modificação do conteúdo ou compartilhamento fora do contexto original a classificação da informação aponta a sua responsabilidade deve ser atualizada

- As senhas vinculadas ao Código de Usuário e demais credenciais de acesso que vier a receber do Banco Bmg para acesso aos ativos da informação, são de uso pessoal, exclusivo e intransferível, devendo zelar pela sua proteção e sigilo, assumindo a responsabilidade por todas as transações efetuadas sob esse código, bem como pela divulgação e/ou fragilização do sigilo das respectivas credenciais e senhas;
- Sob nenhum pretexto, tentar acessar informações, arquivos ou ambientes para os quais não esteja autorizado e/ou que não possuam relação direta com os serviços/atividades objetos do contrato;
- Não enviar mensagens que contenham vírus eletrônico ou códigos maliciosos (*malware*, *spyware* e etc) ou que representem risco à segurança da rede ou que contrariem legislação vigente podendo causar danos ao Banco Bmg;
- Respeitar os direitos de propriedade intelectual e/ou autorais, de acordo com a legislação vigente.

5.7. 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.

5.8. *COMPLIANCE* REGULATÓRIO

- 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 e pelo cumprimento das obrigatoriedades;
- Trabalhar em conjunto com as áreas 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

Este documento contém informação PÚBLICA. Dentro do contexto que estão sendo compartilhadas e utilizadas não ferem os princípios da CID. Em caso de modificação do conteúdo ou compartilhamento fora do contexto original a classificação da informação poderá ser reavaliada pelo responsável.

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

5.9. 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.

6. DIRETRIZES

6.1. 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.

6.2. 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.

6.3. GERENCIAMENTO DE ATIVOS

O gerenciamento de ativos do Grupo Financeiro Bmg é conduzido com as melhores práticas de segurança, mantendo normas, procedimentos e inventário de ativos que são periodicamente revisados e atualizados, assim garantindo o acesso devido e seu descarte seguro.

Todo ativo do Grupo Financeiro Bmg não pode ser retirado ou acessado sem autorização do gestor responsável, e

são transmitidos/transportados em condições adequadas que assegurem sua integridade física e lógica.

6.4. PROTEÇÃO DE DADOS E PRIVACIDADE

O Grupo Financeiro Bmg estruturou sua governança e processos pautado nas boas práticas no tratamento de dados pessoais, em cumprimento a Lei 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), seguindo os princípios da legislação e respeito com nossos clientes, colaboradores, prestadores de serviço, fornecedores e parceiros.

O Grupo Financeiro Bmg, na execução das suas operações tem como objetivo fundamental atuar no primeiro nível de sua instância o conceito de proteção e privacidade dos dados independentemente do fundamento do seu tratamento. A área de Governança da Privacidade de Dados Pessoais, com o total apoio deste programa, considera e pondera os interesses estratégicos da instituição no tratamento de dados de seus titulares.

6.5. CLASSIFICAÇÃO, USO E O TRATAMENTO DA INFORMAÇÃO

As informações é um importante ativo do Grupo Financeiro Bmg e devem ser preservadas e devidamente classificadas e rotuladas, independentemente de seu formato, meio de armazenamento, processamento ou transmissão/transporte, mantendo a conformidade com suas políticas, normas, procedimentos e controles internos, bem como, com as leis e regulamentos dos órgãos reguladores e autorreguladores sobre o tema, sempre de acordo com os requisitos especificados na Norma de Proteção de Dados.

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. GESTÃO DE PERFIS DE ACESSO

Os acessos às informações são controlados, monitorados, restringidos à menor permissão e privilégios possíveis, revistos periodicamente com a aprovação do gestor do responsável, da informação ou sistema, e cancelados ou revogados conforme o prazo estabelecido, na revisão periódica ou tempestivamente ao término do contrato de atuação do colaborador ou do prestador de serviço.

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 instituição, sendo ele responsável pelo uso consciente de suas permissões e sigilo de sua senha e outras informações.

O gestor da informação, é o responsável por autorizar e revisar periodicamente os acessos aos sistemas de informações relacionados à sua área, garantindo assim a aplicabilidade da política de Gestão de Acessos.

6.7. ACORDO DE SIGILO E RESPONSABILIDADE (NDA)

Todo ingresso de colaborador ou prestador de serviço, na qual venham ser o usuário/custodiante das informações controladas pelo Grupo Financeiro Bmg, deverá ser atestado por meio do Acordo de Sigilo e Responsabilidade (NDA), bem como o compromisso e aceite quanto ao cumprimento ao disposto nessa política, demais normas complementares e o conhecimento dos controles de Segurança da Informação e Cibernética, o qual está alinhado com as diretrizes gerais do Grupo Financeiro Bmg.

6.8. 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.

Este documento contém informação PÚBLICA. Dentro do contexto que estão sendo compartilhadas e utilizadas não ferem os princípios da CID. Em caso de modificação do conteúdo ou compartilhamento fora do contexto original a classificação da informação quanto a sua sensibilidade deve ser reavaliada.

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 instituição.

6.9. 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.

6.10. AVALIAÇÃO DE RISCOS CIBERNÉTICOS DE PRODUTOS OU SERVIÇOS

A área de Cyber Security é envolvida nas recomendações sobre controles e proteções de segurança da informação e cibernética no desenvolvimento de novos produtos ou serviços do Grupo Financeiro Bmg, bem como na avaliação de riscos dos mesmos, buscando identificar ameaças e impactos sobre os ativos de informação.

6.11. 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.

6.12. 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 (gesim-gsi@bancobmg.com.br / lgpd@bancobmg.com.br) e, também através de nossos canais oficiais de atendimento.

6.13. GESTÃO DE CONTINUIDADE DO NEGÓCIO

O Grupo Financeiro Bmg adota processos para garantir a continuidade do negócio de acordo com as melhores práticas, 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 fornecedores de serviços contratados.

6.14. GOVERNANÇA EM TECNOLOGIA DA INFORMAÇÃO

O Grupo Financeiro Bmg possui uma área de Governança de TI ligada diretamente à Alta Administração e todas as iniciativas, métodos e procedimentos são reportados a diretoria da Instituição e também ao Comitê de TI que trata os processos e melhorias. Neste Comitê são discutidas as principais estratégias, os valores, riscos, recursos e desempenho dos projetos, otimização e operações da estrutura do Gestão/Gerenciamento de TI.

6.15. SEGURANÇA FÍSICA

A Segurança das agências, abrangendo suas filiais e setores alocados em outros edifícios contemplam um conjunto

de medidas para salvaguardar a integridade física dos colaboradores e clientes, evitando assim eventos delituosos e/ou sinistros.

6.16. PROTEÇÃO DO AMBIENTE

O Grupo Financeiro Bmg possui controles e responsabilidades pela gestão e operação dos recursos de processamento das informações que garantem a segurança na infraestrutura tecnológica de redes locais e internet, através de um gerenciamento efetivo no monitoramento, tratamento e respostas aos incidentes, para minimizar o risco de falhas e a administração segura de redes de comunicações.

O Data Center Principal e o Secundário do Grupo Financeiro Bmg contam com sistemas de monitoração e combate a incêndio bem como uma estrutura de redundância elétrica sendo gerenciado e monitorado com as melhores práticas de segurança física e os acessos podem ocorrer somente após autorização e agendamento prévio do Departamento de Infraestrutura e Tecnologia da Informação.

6.17. GESTÃO DE MUDANÇA

O processo de Gestão de Mudança tem como objetivo assegurar métodos e procedimentos padronizados que são utilizados para garantir a eficácia e eficiência no manuseio autorizado, para todas as mudanças no ambiente de TI (Tecnologia da Informação), de maneira a minimizar o impacto adverso na qualidade dos serviços, de qualquer incidente relacionado a tais mudanças, e, consequentemente, melhorando as tarefas do dia a dia dos processos de negócio do Grupo Financeiro Bmg.

6.18. CÓPIAS DE SEGURANÇA E RECUPERAÇÃO

São estabelecidos diretrizes para o processo de *backup* e *restore* das informações da instituição, que estão sob a guarda de Produção e Monitoramento, pertencente à Gerência de Tecnologia da Informação, visando garantir a disponibilidade das informações relevantes para o pleno funcionamento das atividades do Grupo Financeiro Bmg.

O processo de *backup* deve ser orientado para a restauração das informações no menor tempo possível, principalmente havendo indisponibilidade de serviços que dependam da operação de *restore*.

A realização de testes periódicos possibilita validar os *backups*, validando sem possíveis riscos de ocorrência de falhas

operacionais, perda de informações e com isso garantindo e assegurando possíveis necessidades de recuperação de dados.

7. MEDIDAS DE SEGURANÇA CIBERNÉTICA

O Grupo Financeiro Bmg possui em seu ambiente medidas automatizadas e soluções de segurança cibernética, de forma a reduzir as vulnerabilidades e o impacto de ameaças internas e externas, além de manter um monitoramento, registro e rastreabilidade quanto às atividades relacionadas ao tema.

Também mantém implementado no ambiente medidas e recomendações de *frameworks* de segurança com referências de mercado, e compatíveis com o grau de risco e criticidade das informações da instituição.

Além das ações relacionadas, mantém iniciativas de melhoria contínua quanto 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 as medidas adotados, destaca-se, mas não se limitando a:

- Governança de privacidade de dados: ONE TRUST - SOLUÇÃO PARA SUPORTE AS DEMANDAS DE PRIVACIDADE.
- Segurança e proteção de dados: DLP - TRELLIX ENDPOINT, DLP - SKYHIGH - CASB - NUVEM, DLP - SKYHIGH - SHADOW DLP - PROXY, DLP - FORCEPOINT - REDE, DLP - MICROSOFT - EXCHANGE, DATA ENCRYPTION - ENDPOINT - BITLOCKER(WINDOWS), DATA ENCRYPTION - ENDPOINT - FILEVAULT(MAC), AIP - CLASSIFICAÇÃO DA INFORMAÇÃO, IMPERVA DBF - DATA BASE FIREWALL - MONITORAMENTO DE BANCO DE DADOS, IMPERVA DAM - DATA ACT MONITORING - MONITORAMENTO DE BANCO DE DADOS, CYBERQUANT - AVALIAÇÃO E CÁLCULO DE RISCO CIBERNÉTICO BMG E FORNECEDORES, SECURITY SCORECARD - AVALIAÇÃO DE SCORE DE RISCOS BMG E FORNECEDORES, ZANCHIN - AVALIAÇÃO DE CONTROLES DE SEGURANÇA EM NUVEM.
- Conscientização e Treinamento: KNOWBE4 - Plataforma de treinamento, HACKER RANGER, JORNADA, PLATAFORMA DE *PHISHING* PARA COLABORADORES E CLIENTES.
- Atendimento gestão de acessos (humano/não humano): MT, AS, IGI, GSC, MFA, SENHASEGURA.
- IDM e automatizações: IGI, NET ADMIN, VARONIS, QRADAR.
- Auditoria e *Compliance*: IGI, NET ADMIN.

- Operação de Cyber: ANTISPAM, TUFIN, PROXY WEB REPUTATION, IPS/IDS, ZTNA, VPN / VPN COMPLIANCE, CROWDSTRIKE, DARKTRACE, PROTEÇÃO DE SERVIDORES (EDR) TREND - VIRTUAL PATCH, PROTEÇÃO DE MOBILE (INTUNE), HSM, COFRE DE SENHAS, FEATURES DE SEGURANÇA FIREWALL, AKAMAI, PROGRAMA BEE.
- Prevenção a ameaças, monitoramento e prevenção cyber fraudes: ANTI DDOS, LUMU, QRADAR, APPDOME / DEXGUARD, TOPAZ, GUARDCORE, VARONIS, ELASTIC, NETADMIN.
- Proteção, resposta e recuperação: TANIUM - HARDENING, CYMYLATE.
- Arquitetura de cyber infrasec: AWS ADVISOR, ZANCHIN, CASB - CLOUD SECURITY POSTURE MANAGEMENT (CSPM).
- Gerenciamento de ameaças cybersegurança ofensiva: TANIUM, TESTES AUTOMATIZADOS (CYMULATE/RTREAT), NESSUS, BURP, CASB - SKYHIGH, ESCHECKER, TRAPX, FERRAMENTAS DE TESTES DEVULNERABILIDADE OPEN SOURCE (20), ZANSHIN, BRIGHT - DAST, SCAN DE HARDCODE.
- Proteção de aplicações e segurança digital: SONARQUBE, SYNOPSYS -SAST, APPDOME, DEXGUARD/GUARDSQUARE, SCAN DE HARDCODED.

Além disso, o Grupo Financeiro Bmg também possui mecanismos para detecção de possíveis riscos cibernéticos, por meio de soluções de SOC (Centro de Operações de Segurança) e Serviços de *Threat Intelligence* (Monitoramento de Riscos Cibernéticos).

E, também adota iniciativas para compartilhamento de informações com as instituições e órgãos reguladores quanto aos incidentes relevantes identificados, através de plataformas como MISP (*Malware Information Sharing Platform*) e o Centro de Análise e Compartilhamento de Informações de Serviços Financeiros (FS-ISAC).

8. ANÁLISE CRÍTICA POR ALTA GESTÃO

O Grupo Financeiro Bmg se compromete com a melhoria contínua dos procedimentos e controles relacionados nesta Política, os quais são garantidos através da realização periódica de análise crítica por parte da Alta Gestão e objetos de pautas recorrentes em Comitês internos da instituição.

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 instituição.

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. 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, realizando 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 da instituição, de acordo com as legislações, normas e regulamentações aplicáveis, no intuito de garantir a confidencialidade, integridade e disponibilidades das informações.

11. MELHORIA CONTÍNUA

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

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 quanto a segurança da informação ou cibernética 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.

13. REFERÊNCIAS

- NBR ISO / IEC 27001:2013 - Sistemas de Gestão de Segurança da Informação - Requisitos.
- NBR ISO / IEC 27002:2013 - Código de Prática para a Gestão da Segurança da Informação.
- NBR ISO / IEC 27701:2019 - Gerenciamento de Informações de Privacidade.
- Resolução CMN nº 4.893, de 26 de fevereiro de 2021.
- Resolução CMN nº 4.553. de 30 de janeiro de 2017.
- Resolução CMN nº 4.557, de 23 de fevereiro de 2017.
- Resolução CMN nº 4.968, de 25 de novembro de 2021.
- Resolução BCB nº 265, de 25 de novembro de 2022.
- Lei Geral de Proteção de Dados nº 13.709/2018.