Política de Segurança da Informação e Cibernética do BDMG

Objetivo

A informação é um dos principais bens de qualquer organização. A Política de Segurança da Informação e Cibernética do BDMG tem por objetivo estabelecer os princípios, diretrizes e responsabilidades de proteção dos dados e das informações de propriedade da instituição, dos clientes e do público em geral.

Abrangência

Esta política aplica-se a todos os funcionários, estagiários e prestadores de serviços do BDMG.

Conceitos

I. Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizados.

II. Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

III. Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.

IV. Segurança da Informação: ações que objetivam assegurar a confidencialidade, a integridade e a disponibilidade da informação, qualquer que seja o meio de armazenamento.

V. Segurança Cibernética: preservação da confidencialidade, da integridade e da disponibilidade da informação no ambiente cibernético.

VI. Incidente de segurança: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança das informações, das redes de computadores ou dos sistemas de informação.

Princípios

I. Toda informação sob responsabilidade do BDMG é patrimônio da Instituição, será usada exclusivamente em seu interesse e estará adequadamente protegida em função do seu grau de sigilo, nos termos da regulamentação e legislação inerentes à atividade bancária.

II. Serão implementados controles e mecanismos necessários para garantir a segurança e proteção dos dados e das informações em todo seu ciclo de vida (criação, guarda, manuseio, transporte e descarte), independentemente do seu formato ou meio de armazenamento.

III. Cada funcionário, estagiário e prestador de serviço é responsável pela proteção das informações, dos recursos computacionais e sistemas de informação dos quais fizer uso.

IV. Os dados dos clientes serão tratados com o devido sigilo e em hipótese alguma serão fornecidos a terceiros, salvo nos casos previstos na regulamentação e legislação vigentes ou com o consentimento do cliente.

V. O funcionário, o estagiário e o prestador de serviço terão acesso somente às informações, recursos computacionais ou sistemas de informação imprescindíveis para o exercício de suas atividades laborais. Este acesso será feito por meio de identificação única, pessoal e intransferível que possibilitará a rastreabilidade das ações executadas.

Responsabilidades

Conselho de Administração:

Aprovar a Política de Segurança da Informação e Cibernética e o plano de ação e de resposta a incidentes, visando à sua implementação.

Comitê de Riscos e Capital:

Avaliar e propor, com periodicidade mínima anual, recomendações ao Conselho de Administração sobre as necessidades de atualização da Política de Segurança da Informação e Cibernética e a efetividade da implementação do plano de ação e de resposta a incidentes.

Diretoria Executiva:

Assegurar a implementação e a efetividade da Política de Segurança da Informação e Cibernética, do plano de ação e de resposta a incidentes;

Aprovar as iniciativas para disseminação da cultura de segurança da informação e cibernética no BDMG.

Gestores:

I. Proteger as informações, recursos computacionais e sistemas de informação em conformidade com esta Política, a legislação e regulamentação pertinente;

II. Classificar a informação quanto ao nível de confidencialidade, independentemente do seu formato ou meio de armazenamento, conforme normativo específico;

III. Autorizar, rever periodicamente ou revogar o acesso às informações, recursos computacionais e sistemas de informação;
IV. Verificar o cumprimento dos requisitos de segurança pelo Custodiante da Informação, quando este existir, e assegurar a adoção de eventuais medidas para adequação;
V. Tomar as ações necessárias à segurança da informação na contratação, transferência de Unidade ou desligamento de empregados, estagiários ou prestadores de serviços;
VI. Garantir a participação da sua equipe nas atividades de educação e treinamento em segurança da informação e cibernética;
VII. Orientar sua equipe para o cumprimento da Política de Segurança da Informação e Cibernética, bem como tomar as medidas corretivas necessárias;
VIII. Registrar e tratar imediatamente qualquer incidente de segurança ocorrido ou suspeito com as informações, recursos computacionais e sistemas de informação.

Funcionários, estagiários e prestadores de serviços:

I. Conhecer e cumprir a Política de Segurança da Informação e Cibernética, a legislação e regulamentação pertinentes;
II. Utilizar as informações, os recursos computacionais e os sistemas de informação somente para o exercício de suas atividades funcionais;
III. Garantir a segurança das informações em todo seu ciclo de vida: criação, guarda, manuseio, transporte e descarte;
IV. Não compartilhar, em nenhuma hipótese, e manter sob rigoroso sigilo sua credencial e senha de acesso às informações, recursos computacionais ou sistemas de informação;
V. Não compartilhar, sem a devida autorização, informações confidenciais de qualquer natureza;
VI. Cumprir os termos e contratos de propriedade intelectual e de licenciamento de software;
VII. Participar das atividades de educação e treinamento em segurança da informação e cibernética;
VIII. Comunicar imediatamente ao Gestor da Informação qualquer incidente de segurança ocorrido ou suspeito e tomar as ações necessárias, conforme normativo específico.