Política de Segurança Cibernética- BRB

INTRODUÇÃO

A informação é um ativo essencial para os negócios do conglomerado BRB. Alinhado com os objetivos e requisitos do negócio, o conglomerado BRB estabelece nesta Política de Segurança Cibernética regras e direcionamentos a serem seguidos e aplicados a pessoas, processos, tecnologias e demais normativos internos, para proteger as informações do BRB, de seus clientes, fornecedores e parceiros de negócios.

OBJETIVOS

Nossa Política de Segurança Cibernética tem como objetivo estabelecer princípios, diretrizes, papéis e responsabilidades sobre os principais aspectos relacionados à segurança cibernética, visando: assegurar a confidencialidade, integridade, disponibilidade, autenticidade e irretratabilidade dos dados e dos sistemas de informação utilizados pelo conglomerado BRB; cumprir a legislação aplicável; promover a cultura organizacional sobre o tema.

Esta Política leva em consideração o porte, perfil de risco e o modelo de negócios; a natureza das operações e a complexidade dos produtos, serviços, atividades e processos da instituição; e a sensibilidade dos dados e das informações sob responsabilidade do BRB.

PRINCÍPIOS

Entendemos a segurança cibernética como um conjunto de tecnologias, processos e práticas projetados para proteger redes, computadores, sistemas e dados de ataques, danos ou acessos não autorizados. A segurança cibernética contribui para a segurança da informação, e é norteada pelos seguintes princípios:

Confidencialidade: a informação somente será acessada por pessoas efetivamente autorizadas;

Integridade: o conteúdo da mensagem não será alterado ou violado indevidamente, ou seja, viabilizamos a exatidão da informação e de seus métodos de modificação, manutenção e validade.

Disponibilidade: os colaboradores autorizados obterão acesso à informação e aos sistemas correspondentes sempre que necessários, nos períodos e ambientes aprovados pela empresa;

Autenticidade: as entidades (informação, equipamentos ou usuários) identificadas em um processo de comunicação como remetentes ou autores são exatamente aqueles que dizem ser.

Irretratabilidade: uma pessoa ou entidade não poderá negar a autoria da informação fornecida.

DIRETRIZES

Temos processos para monitorar a publicação de normativos por entes reguladores nos temas relacionados à segurança cibernética e consequente realização de atividades para conformidade.

Adotamos procedimentos e controles para prevenir, detectar e reduzir as vulnerabilidades da instituição, contribuindo para mitigar incidentes relevantes, buscando garantir a segurança das informações sensíveis e atender aos demais objetivos da segurança cibernética. Entre os procedimentos e controles adotados, destacam-se: a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra *softwares* maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações.

Elaboramos requisitos para o desenvolvimento e aquisição de *software* seguro com base nos procedimentos e controles mencionados objetivando a redução de vulnerabilidades.

Implementamos os controles para garantir a rastreabilidade e segurança de dados e informações consideradas sensíveis.

Classificamos os dados e informações geradas na instituição segundo critérios de sensibilidade e de relevância aprovados e vigentes.

Elaboramos cenários de incidentes de segurança cibernética nos testes de continuidade de negócio com o objetivo de aprimorar os controles.

Implementamos programa de capacitação e de avaliação periódica de empregados e colaboradores.

Avaliamos a relevância dos incidentes cibernéticos mediante parâmetros definidos.

Definimos os requisitos de segurança para internalização de novas tecnologias.

Definimos procedimentos e controles voltados à prevenção, a detecção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição.

Realizamos análises de riscos cibernéticos nos serviços contratados de processamento e/ou armazenamento de dados em nuvem.

Registramos a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição, abrangendo, quando necessário, informações recebidas de empresas prestadoras de serviços a terceiros.

Compartilhamos informações sobre os incidentes relevantes em plataformas especializadas.

Adotamos procedimentos a serem seguidos no caso da interrupção de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem contratados.

Prestamos informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros.

GOVERNANÇA CORPORATIVA

Dispomos de estrutura pautada em normas e *frameworks* internacionais para manutenção dos processos que garantem a segurança cibernética do BRB, a conformidade com a Resolução CMN 4.893/21 e os demais normativos de entes reguladores, e o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados à segurança cibernética.

ÂMBITO E VIGÊNCIA

As diretrizes e os princípios estabelecidos neste documento devem ser observados por todos os administradores, empregados, prestadores de serviço e demais colaboradores do Conglomerado BRB.

Esta política possui vigência a partir de sua publicação.