KEB Hana Bank

POLITICA DE SEGURANÇA CIBERNETICA

I. Introdução

A informação é um dos ativos de maior valor para qualquer organização e com a crescente utilização do Espaço Cibernético na disponibilização e acesso das informações, o Banco KEB Hana do Brasil, com o intuito de formalizar seus procedimentos e adequá-los às normas vigentes, estabelece a Política de Segurança Cibernética em adição à Política de Segurança da Informação, documento DTI-MN002-Política_Segurança_Informação.

A Política de Segurança Cibernética visa garantir que as informações do Banco KEB Hana do Brasil, e de seus clientes, estejam sendo tratadas de forma segura e protegida no Espaço Cibernético.

A Segurança Cibernética é a capacidade de identificar, proteger, detectar, responder e recuperar rapidamente de uma ameaça cibernética, a fim de garantir os princípios da Confidencialidade, Integridade e Disponibilidade no Espaço Cibernético.

Conceitos Gerais:

- **Informação:** ativo essencial para o negócio. Pode estar na forma escrita, impressa, verbal, e em meio digital ou físico;
- **Segurança da Informação**: é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio.
- **Segurança Cibernética:** é a capacidade de identificar, proteger, detectar, responder e recuperar rapidamente de uma ameaça cibernética, a fim de garantir os princípios da Confidencialidade,

Integridade e Disponibilidade no Espaço Cibernético.

- **Espaço Cibernético**: o Espaço Cibernético é caracterizado pelo ambiente resultante da interação de pessoas, software e serviços na Internet por dispositivos de tecnologia e redes conectadas a ele, ao qual não existe uma forma física
- **Evento de Segurança**: ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança ou falha de controle, ou uma situação previamente desconhecida.
- **Incidente de Segurança:** um evento ou uma série de eventos indesejados e inesperados que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação ou Segurança Cibernética.
- **Ameaça:** causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.
- **Vulnerabilidade:** fragilidade de um ativo que pode ser explorada por uma ou mais ameaças.

II. Objetivo

Estabelecer as diretrizes que norteiam a Segurança Cibernética no Banco KEB Hana do Brasil caracterizada pela preservação dos princípios:

Confidencialidade – garantia de que a informação seja acessível somente por pessoas com acesso autorizado;

Integridade – é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;

Disponibilidade – garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.

III. Abrangência

A Política de Segurança Cibernética do Banco KEB Hana do Brasil aplica-se a todo corpo de funcionários e colaboradores, independente do seu nível hierárquico ou função, bem como, prestadores de serviços do Banco KEB Hana do Brasil.

IV. Referências (Documentação Interna)

- DTI-MN001-Política_Plano_Estrategico_TI
- DTI-MN002-Polítttica_Segurança_Informação
- DTI-MN003-Política_Segurança_Senhas
- DTI-MN004-Política_Segurança_Procedimento_Backup
- DTI-MN005-Política_Segurança_Sistema_TOTVS
- DTI-MN006-Política_Segurança_Sistema_Exchange
- DTI-MN007-Política_Segurança_Auditoria_Sistemas
- DTI-MN008-Política_Segurança_Procedimento_Atualizacao
- DTI-MN009-Política_Segurança_Procedimento_Correcao

- DTI-MN011-Plano de Contingência Geral
- Resolução 4658 – Banco Central do Brasil – dispõe sobre a política de Segurança Cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e computação em nuvem.

V. Diretrizes Gerais

- A Política de Segurança Cibernética do Banco KEB Hana do Brasil deve ficar disponível para acesso de todos os colaboradores e protegida contra alterações.

- A Política de Segurança do Banco KEB Hana do Brasil deve ser revisada anualmente.

- O Banco KEB Hana do Brasil deve manter um processo educativo de campanhas de sensibilização com o objetivo de promover a cultura de Segurança Cibernética.

VI. Diretrizes Para Controles de Segurança Cibernética

Prevenção Contra Vírus, Arquivos e Softwares Maliciosos

O Banco KEB Hana do Brasil deve possuir controles para prevenir que vírus e outros tipos de softwares maliciosos entrem e espalhem-se nos sistemas e servidores através de arquivos e softwares não homologados cuja instalação e uso são proibidos por colocarem em risco a segurança das informações.

Prevenção e Detecção de Intrusão

O Banco KEB Hana do Brasil deve possuir controles para detectar e prevenir ameaças, a fim de aumentar a capacidade de prevenção contra ataques cibernéticos.

Varredura de Vulnerabilidades

O Banco KEB Hana do Brasil deve realizar periodicamente testes e varreduras para detecção de vulnerabilidades no ambiente de tecnologia.

Manutenção e Cópias de Segurança

O Banco KEB Hana deve possuir norma e procedimentos específicos para garantir a recuperação de dados e informações.

Acesso a Sistemas, Recursos de Rede e Rastreabilidade

O acesso e o uso de todos os sistemas de informação, diretórios de rede, bancos de dados e demais recursos devem ser restritos a pessoas autorizadas conforme a necessidade mínima ao cumprimento de suas funções e devem ser rastreados através de logs fornecidos pelos Sistemas de Informações e mecanismos de prevenção a vazamentos de dados.

Desenvolvimento Seguro e Criptografia

O Banco KEB Hana do Brasil deve adotar as melhores práticas de desenvolvimento seguro de sistemas bem com criptografar os dados e informações sensíveis.

Classificação dos Dados e das Informações

O Banco KEB Hana do Brasil deve classificar os dados e informações de forma que recebam um nível adequado de proteção.

A classificação dos dados e informações deve observar as seguintes diretrizes:

- A sensibilidade dos dados e das informações;
- A criticidade dos dados e das informações;
- Valor dos dados e das informações;

- Requisitos legais.

VII. Diretrizes Para Tratamento de Incidentes

- Os incidentes de Segurança Cibernética devem ser registrados e tratados;
- As atividades suspeitas ou incidentes identificados pelos colaboradores devem ser reportados ao e-mail: tecnologia@bancokebhana.com.br;
- Ferramentas de monitoramento de segurança devem ser implementadas, a fim de prevenir e detectar ataques cibernéticos;
- As ferramentas de segurança deverão gerar registro e alertas de incidentes cibernéticos;
- O Plano de Continuidade do Negócio, documento DTI-MN011-Plano de Contingência Geral, deve ser acionado caso os incidentes de segurança cibernéticos causem uma indisponibilidade dos processos críticos do negócio por um tempo superior ao RTO (tempo objetivo de recuperação) determinado no BIA (análise de impacto nos negócios).

VIII. Diretrizes Para Contratação de Fornecedores de Serviços de Processamento e Armazenamento de Dados e Computação em Nuvem

- Provedores e fornecedores contratados que armazenam e processam dados do Banco KEB Hana do Brasil devem ser avaliados sob o ponto de vista de Segurança Cibernética.
- Provedores e fornecedores devem conhecer e observar a Política de Segurança Cibernética do Banco KEB Hana do Brasil.