POLÍTICA DE SEGURANÇA DA INFORMAÇÃO CIBERNÉTICA DO CERUS BANK

1. OBJETIVO

Esta Política Corporativa tem por objetivo descrever as diretrizes de Segurança da Informação e Cibernética aplicáveis no Cerus Bank, prezando pelos princípios básicos de confidencialidade, integridade e disponibilidade.

2. ABRANGÊNCIA

Esta Política Corporativa deve ser difundida a todos os colaboradores, terceiros e prestadores de serviço que atuam no Cerus Bank. Ajustes podem ser realizados no formato de divulgação desta política para adequação ao público em geral.

As orientações aqui estabelecidas são aplicáveis aos ambientes de computação em nuvem (*cloud)* e local (*on-premises).* O índice de termos de segurança utilizados nesta Política Corporativa, bem como os demais documentos oficiais, está disponível para consulta no portal: https://www.cerusbank.com.br

3. COMPETÊNCIA DE APROVAÇÃO

Gerencia de Segurança - Responsável pela elaboração e manutenção desta política.

Diretoria de Segurança - Responsável pela revisão desta política.

Diretoria Societária Cerus Bank - Responsável pela aprovação desta política.

4. INTRODUÇÃO

Esta política dispõe das diretrizes essenciais de segurança da informação e segurança cibernética. Estas diretrizes são estabelecidas com base nos requisitos de órgãos reguladores, normas e práticas de mercado com foco em uma estratégia eficiente de segurança da informação por meio de controles para reduzir os riscos envolvidos, assim como se precaver de potenciais incidentes de forma tempestiva. E, são aplicáveis a todos os colaboradores, terceiros e prestadores de serviço que atuam no Cerus Bank.

5. ESTRATÉGIA

A Diretoria do Cerus Bank está, desde a sua fundação, comprometida na melhoria contínua dos serviços relacionados com a segurança da informação e cibernética, disponibilizando recursos compatíveis para o desenvolvimento da disciplina na empresa, através da priorização dos projetos voltados a segurança dos produtos e infraestrutura interna, além de considerar os riscos de segurança da informação e cibernética em produtos, projetos e processos.

O objetivo de Segurança no Cerus Bank é garantir a confidencialidade, integridade, disponibilidade, autenticidade, legalidade, não-repúdio e privacidade das informações internas e de seus clientes, por meio da prevenção, detecção, redução das vulnerabilidades e contenção de incidentes relacionados com o ambiente cibernético.

6. PAPEIS E RESPONSABILIDADES

- Diretoria de Segurança: é responsável por estabelecer o plano tático e estratégico de Segurança e Prevenção a Fraudes em linha com a estratégia de negócio e a de tecnologia. Sendo o CISO – *Chief Information Security Officer* possui o papel de evitar e mitigar riscos de vulnerabilidade e ataques cibernéticos.

Além disso, é também responsável por criar uma abordagem eficiente para atingir os objetivos de Segurança e Prevenção a Fraudes. Desta forma, estabelece em sua estrutura as áreas com seus papéis e responsabilidade:

- Governança de Segurança: é responsável por alinhar os objetivos e estratégia de Segurança com os objetivos e estratégia de negócio, apresentando os riscos de segurança para a Diretoria e para as partes interessadas, agregando valor ao negócio do Cerus Bank e endereçando os riscos adequadamente.

- Engenharia de Segurança: é responsável por prover os requisitos de segurança para infraestrutura e aplicações durante todo o ciclo de vida do projeto, por definir a estratégia de arquitetura de soluções e segurança bem como implantá-las em linha com os objetivos definidos e diretrizes oriundas da Política de Segurança da Informação e Cibernética.

- Operação de Segurança e Resposta a Incidentes: é responsável pelas Operações de Segurança (SOC – *Security Operation Center*), e por monitorar os eventos de segurança por meio do sistema de correlação de eventos de segurança (SIEM) e reagir diante de eventuais alertas através do engajamento das partes interessadas. Também agrega a responsabilidade de Resposta a Incidentes (CSIRT – *Cyber*

Security Incident Response Team) com a capacidade de responder aos incidentes de segurança, contendo, erradicando, remediando e acompanhando o reestabelecimento do ambiente de forma tempestiva.

- Segurança de Aplicações e Segurança Ofensiva: é responsável por conduzir a equipe de Segurança Cibernética (*Red Team*) com capacidade de desafiar e testar todos os controles de segurança estabelecidos no ambiente, com o intuito de descobrir novas falhas e agir com o pensamento de um potencial atacante.

- Cultura e Conscientização: é responsável por prover, em linha com as estratégias de Segurança e Prevenção a Fraudes, o Programa de Conscientização, contemplando treinamentos e educação contínua para colaboradores e terceiros, relacionamento com as comunidades de segurança e tecnologia bem como a educação sobre segurança para clientes do Cerus Bank.

- Prevenção a Fraudes: responsável por definir processos e controles evitando que ações fraudulentas sejam executadas através dos produtos ou serviços que o Cerus Bank fornece aos seus clientes. Adicionalmente deverá se manter atualizado nas tendências de práticas de fraudes para providenciar soluções aos produtos e serviços do Cerus Bank, buscando a proteção dos clientes.

7. PRINCIPAIS DISCIPLINAS DE SEGURANÇA

Para alcançar os objetivos de segurança da segurança foram estabelecidas as seguintes disciplinas.

7.1. Criptografia

A criptografia é a ciência de escrever mensagens cifradas, ou seja, de forma inelegível. No Cerus Bank, os recursos de criptografia são utilizados de diversas maneiras para assegurar a confidencialidade, integridade, a autenticidade e não repúdio das informações. Podem ser utilizadas a criptografia de chave simétrica e assimétrica além de funções de resumo (hash), certificados digitais ou ainda outros tipos de métodos.

7.2. Prevenção e detecção de intrusão

Prevenção e detecção de intrusão correspondem aos recursos tecnológicos utilizados na estratégia de proteção da rede do Cerus Bank associada as atividades de monitoramento e bloqueio tempestivo de qualquer comportamento ou tráfego suspeito que pode indicar uma tentativa de ataque ou uma exploração de vulnerabilidade. Os contratos com empresas terceiras e prestadores de serviço devem estabelecer a responsabilidade de colaboração diante um incidente de segurança declarado.

7.3. Classificação das informações

A classificação das informações tem por objetivo orientar proprietários, custodiantes e consumidores a identificar a criticidade, rotular e tratar as informações utilizando os controles aplicáveis a julgar por sua sensibilidade. Informações devem ser classificadas como Públicas, Internas, Restritas ou Confidenciais.

É responsabilidade de todos os colaboradores da Cerus Bank e seus sprestadores de serviços assegurar que as informações são classificadas corretamente e são compartilhadas por meios compatíveis com seu nível de confidencialidade.

7.4. Gestão de Vulnerabilidades

O processo de gestão de vulnerabilidades tem por objetivo identificar constantemente as fragilidades no ambiente tecnológico e avaliar o potencial risco para o negócio, desde a identificação até as atividades de remediação. O Cerus Bank utiliza como insumo para o processo a varredura (scan) de vulnerabilidades em redes, computadores, infraestrutura e aplicações, testes de intrusão, acompanhamento de notificações de fornecedores e contatos com entidades externas de Segurança.

7.5. Cópias de Segurança

São realizadas cópias de segurança (Backups) e testes de recuperação (Restore) das informações corporativas e de clientes que são relevantes ao negócio, com tempo de retenção em linha com as leis e regulações aplicáveis ao segmento financeiro. A estratégia do Plano de Backup deve ser consoante com a criticidade das informações à continuidade do negócio do Cerus Bank, e as rotinas e modalidades de Backup devem ser aplicadas conforme o cenário, considerando o plano tático de maior eficiência operacional. Nos casos em que as atividades de *Backup* e *Restore* são operadas por terceiros, as especificações devem estar previstas nos acordos entre as partes.

7.6. Gestão de Identidades & Acessos

Cerus Bank aplica os controles de gestão de autorização e autenticação dos usuários nos sistemas e ambientes tecnológicos. A concessão de acessos é realizada a partir do princípio de menor privilégio, que significa que um usuário terá acesso apenas as funcionalidades requeridas para o desempenho de sua função.

7.7. Responsabilidade no uso da senha

Todos os colaboradores são responsáveis por zelar por suas informações de autenticação. É vedado o compartilhamento de senha ou seu armazenamento em locais inseguros, além disso, devem atender aos padrões mínimos de segurança exigidos pelo Cerus Bank.

7.8. Utilização dos recursos tecnológicos

O Cerus Bank disponibiliza aos usuários diversos recursos tecnológicos com propósito exclusivo de apoiar o desenvolvimento das atividades inerentes a função dos colaboradores e prestadores de serviço. Para proteger as informações utilizadas nestes recursos, são aplicados parâmetros e controles de segurança como antivírus, anti malware, DLP, entre outros.

Tais recursos são passíveis de monitoramento, bem como armazenar e analisar registros para que possibilitem rastrear ações realizadas pelo usuário custodiante do recurso. Atitudes em dissonância com os valores estabelecidos no Cerus Bank, expressas por meio do comportamento na Internet e uso inadequado dos recursos tecnológicos e do correio eletrônico, seja em meio presencial ou remoto, não são toleradas. E ainda, a instalação de Softwares e Hardwar não autorizados nos recursos tecnológicos da organização não são permitidos.

7.9. Segurança física dos ambientes de operação e processamento

São aplicados controles de segurança física nos ambientes utilizados para processamento de informações, sendo implementados no perímetro interno e externo, para mitigar o risco de acesso indevido e/ou não autorizado às informações.

8. CULTURA E CONSCIENTIZAÇÃO DE SEGURANÇA

Faz parte da estratégia de Segurança fomentar a cultura, conscientização e educação contínua dos colaboradores, terceiros, prestadores de serviço e clientes relacionada a disciplina de Segurança. A missão da Cultura de Segurança é levar de forma contínua às partes interessadas as orientações para proteção das informações internas e de clientes, por meio da disseminação de diretrizes através de treinamentos e eventos, interação com comunidades, comunicações periódicas via canais oficiais do Cerus Bank, portal dedicado para instrução de clientes, e quaisquer outros recursos que sirvam ao propósito de elevar a consciência de todo o público sobre o seu papel fundamental na proteção das informações.

9. RELACIONAMENTO COM FORNECEDORES E PRESTADORES DE SERVIÇO

Segurança possui a responsabilidade de avaliar os aspectos de segurança no relacionamento com fornecedores e prestadores de serviço cujo escopo de trabalho contemple o tratamento de informações de propriedade intelectual do Cerus Bank, visando conhecer o ambiente do parceiro

e mapear o nível de risco cibernético que este relacionamento pode acarretar. São admitidas avaliações pela área de segurança, contemplando auditorias externas e, eventualmente, a realização de testes de intrusão (*pentests*) quando pertinente ao contexto e mediante consentimento do proprietário da informação.

10. PREVENÇÃO, IDENTIFICAÇÃO E TRATAMENTO DE INCIDENTES DE SEGURANÇA

O Cerus Bank contempla em sua estratégia de Segurança a estrutura para prevenção, identificação e tratamento de incidentes de segurança em seu ambiente e em parceria com os provedores de serviço, inclusive aqueles alocados em nuvem.

Os incidentes de segurança serão classificados para tratamento de acordo com fatores como impactos negativos financeiros, de imagem, operacionais, ou que afetem diretamente a estratégia do Cerus Bank, podendo ser classificados desde baixo até críticos. Para acionar a equipe para análise e tratamento de possíveis incidentes cibernéticos poderão ser enviados e-mails aos canais:

O Cerus Bank preza pela privacidade dos titulares independentemente do seu vínculo com a empresa. Desta forma, produtos, projetos, processos, sistemas e controles são desenhados e executados sempre observando o tratamento de dados pessoais de forma adequada, alinhado junto aos titulares e de forma transparente e responsável. São exigidos os mesmos compromissos com a privacidade junto aos prestadores de serviços, parceiros e fornecedores.

Os titulares poderão entrar em contato com Cerus Bank para obter entendimento do tratamento de seus dados, obtendo uma ampla visão dos dados que são utilizados e quais são as respectivas justificativas para tais ações.

11. SANÇÕES

O não cumprimento das diretrizes declaradas nesta Política Corporativa está sujeito a sanções do Cerus Bank, sendo que estes processos devem ser tratados sob sigilo e zelando pela privacidade dos envolvidos.

12. VIGÊNCIA

Esta norma será declarada vigente a partir da aprovação de todas as partes responsavéis pelo processo, e deverá ser atualizada conforme houver alterações significativas no processo, ou após um período de doze meses em caráter ordinário.

13. CENTRAL DE RELACIONAMENTO

Em caso de dúvidas, entre em contato conosco pelos seguintes meios abaixo e demais disponíveis em nossos canais:

- 0800 580 3024(demais localidades);
- 4003 6392(capitais e regiões metropolitanas);
- WhatsApp (85) 4042 1849;
- Chat no site www.cerusbank.com.br
- meajuda@cerusbank.com.br;

Data da última atualização: 18 de abril de 2022.

AGRADECEMOS POR VOCÊ TER LIDO NOSSA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO CIBERNÉTICA DO CERUS BANK

BEM-VINDO(A) À FAMÍLIA CERUS!

CERUSBANK INSTITUIÇÃO DE PAGAMENTO S.A