Casa do Crédito

Política de Segurança Cibernética

Casa do Crédito S/A – Sociedade de Crédito ao Microempreendedor

2023

Rua Schilling, n°471 – Vila Leopoldina
São Paulo - SP - Brasil - 05302-001 | +55 11 3034-5004
www.casadocredito.com.br

SUMÁRIO

1. INTRODUÇÃO

A Casa do Crédito S/A – SCM ("Casa do Crédito"), estabelece a presente Política de Segurança Cibernética ("Política") com o intuito de aplicar os princípios de proteção das informações consideradas sensíveis de seus acionistas, diretores, prestadores de serviços, temporários, estagiários, jovens aprendizes, profissionais autônomos ou de empresas parceiras e fornecedores de serviço detentores de informações da Casa do Crédito ("Colaboradores"), assim como de seus clientes.

Esta Política orienta as responsabilidades da Casa do Crédito, de seus Colaboradores e prestadores ou fornecedores de serviços de processamento e armazenamento de dados e de computação em nuvem ("Prestadores de Serviços"), para o cumprimento dos requisitos legais estabelecidos na legislação brasileira, em especial a Resolução 4.893, de 26 de fevereiro de 2021, do Banco Central do Brasil ("BACEN").

2. OBJETIVO

Estabelecer diretrizes e responsabilidades da Casa do Crédito e de seus Colaboradores para o gerenciamento da segurança cibernética, promovendo melhorias contínuas dos procedimentos relacionados à segurança dos dados e informações, assim como definindo os requisitos mínimos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, em conformidade com a legislação vigente. Os objetivos ora estabelecidos visam prevenir, detectar e reduzir fragilidades e incidentes relacionados com o ambiente cibernético, assim como possibilitar a manutenção da confidencialidade, da integridade e da disponibilidade das informações e dados utilizados sob responsabilidade da Casa do Crédito.

3. ABRANGÊNCIA

Esta Política se aplica a todos os Colaboradores da Casa do Crédito, em especial, mas não se limitando, a área de Segurança e Tecnologia da Informação. A Política os submete ao bom cumprimento desta, com a recomendação de estarem em conformidade com este documento, assim como serem diligentes no cumprimento das diretrizes ora estabelecidas.

4. PROCEDIMENTOS E CONTROLES ADOTADOS PARA GARANTIR OS OBJETIVOS DA SEGURANÇA CIBERNÉTICA

É de extrema importância a disseminação da cultura de segurança cibernética para garantir a integridade, confiabilidade e disponibilidade das informações. Para garantir o cumprimento dos princípios dispostos nesta Política, a Casa do Crédito utiliza-se de procedimentos, controles, políticas internas, instruções normativas, legislações vigentes, comunicados corporativos, treinamentos periódicos de segurança da informação/cibernética e compliance.

5. CONTROLES ADOTADOS PARA A SEGURANÇA DAS INFORMAÇÕES

A Casa do Crédito possui diversos controles e procedimentos para garantir a segurança cibernética e das informações sensíveis, conforme descrito nos tópicos abaixo:

5.1 Controle de Acesso e Gerenciamento

A prática de Controle de Acesso e Gerenciamento tem o objetivo de prevenir o acesso de indivíduos não autorizados ao ambiente cibernético e aos sistemas, garantindo assim a confidencialidade das informações. A Casa do Crédito segue as boas práticas no sentido de orientar que todos os usuários devam possuir acesso à informação somente de acordo com as necessidades do negócio. Como controle adicional foi elaborada uma matriz de segregação de função baseada em cargo/função.

A Casa do Crédito possui procedimentos formalizados e a descrição dos fluxos operacionais para a concessão, alteração, revogação e gerenciamento de acessos, sendo que para todos os procedimentos citados acima é respeitado o princípio de menor privilégio e perfil mínimo restrito de acesso, conforme a matriz de segregação de função. Adicionalmente, os procedimentos de concessão e alteração devem ser aprovados pelo gestor responsável, System Owner, Diretoria Executiva, Compliance e Segurança da informação.

A Casa do Crédito realiza periodicamente a revisão de acessos, conforme a presente Política, que tem como objetivo a atualização dos acessos e permissões, procedimento este, que é coordenado pela Área de Segurança da Informação, sendo seu resultado de revisão enviado para a anuência da Diretoria.

5.2 Gerenciamento de Riscos e Tecnologia da Informação

A Casa do Crédito verifica periodicamente o controle de acessos à internet e controla os aplicativos instalados nos computadores. Vale ressaltar que nenhum usuário possui acesso de administrador local, impossibilitando a instalação de qualquer aplicativo. Somente podem ser instalados aplicativos previamente testados e autorizados pela área de Tecnologia da Informação. A Casa do Crédito realiza o monitoramento da rede por meio de software específico.

5.3 Segurança de Rede

A segurança é realizada através do monitoramento e gerenciamento da infraestrutura, sendo que todo acesso às redes internas e acessos à internet são controlados pela Tecnologia da Informação.

5.4 Segurança e gerenciamento de Ativos de Sistemas

Quando disponível, o acesso aos sistemas de informação da Casa do Crédito é integrado com o AD ("Active Directory"). Para os Sistemas de Informação que não estão integrados com AD, existe um pré-requisito mínimo para as parametrizações de senhas. Referente ao gerenciamento das parametrizações de segurança, somente a área de Segurança da Informação possui acesso para alterar as configurações de acesso e segurança nos Sistemas de Informação.

5.5 Gestão de Ameaças e Vulnerabilidades de TI

O ambiente possui instalado software de antivírus para a proteção contra vírus, arquivos e softwares maliciosos, atualizados periodicamente. Todas as atualizações de segurança do Windows são gerenciadas e atualizadas frequentemente.

5.6 Dispositivos e Controles de Mídia

Somente pessoas previamente autorizadas pela Diretoria Executiva tem acesso aos dispositivos móveis e acessos ao leitor de DVD e USB do computador.

5.7 Segurança Física

Os recursos e instalações de processamento de informações críticas para as atividades da Casa do Crédito são mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e recursos para controle de acesso. Os equipamentos críticos possuem proteção contra desastre físico e recursos para combate a desastres naturais incêndio.

A Casa do Crédito possui sistema para controle do acesso dos colaboradores, prestadores de serviços ou fornecedores aos locais restritos por meio de monitoramento de câmeras.

6. REGISTRO E ANÁLISE DA CAUSA DOS EFEITOS DE INCIDENTES RELEVANTES E DE VULNERABILIDADES

O registro e análise dos efeitos de incidentes relevantes e de vulnerabilidades são atividades cruciais para minimizar impactos negativos para a Casa do Crédito, a nível operacional e reputacional.

A Casa do Crédito se preocupa com as empresas que prestam serviços terceirizados para a instituição. As informações recebidas por estas empresas são objeto de NDA (*Non Disclosure Agreement*), contempladas em registro específico e objeto de análise complementar no que se refere a impactos dos efeitos de incidentes e vulnerabilidades.

A Casa do Crédito possui os controles que permitem detectar e identificar os cenários e casos de incidentes e vulnerabilidades que afetam o ambiente de Segurança Cibernética, conforme delimitado no item “7. DIRETRIZES GERAIS” desta Política.

Prestadores de Serviço, fornecedores e empresas conveniadas devem adotar procedimentos e controles compatíveis com os riscos envolvidos na prestação de serviços relevantes prestados junto aos clientes, preservando, inclusive, a continuidade das operações e negócios da Casa do Crédito. Os eventos de TI são registrados em sistema para o adequado controle e gerenciamento de riscos.

7. DIRETRIZES GERAIS

7.1 Teste de Continuidade de Negócios

A Casa do Crédito assume o compromisso de manter a continuidade dos negócios em caso de incidentes que possam comprometer o funcionamento normal de suas atividades, através do Programa de Continuidade de Negócios (“PCN”), sendo constantemente revisado com o objetivo contínuo de melhoria.

O programa possui o objetivo de identificar e elaborar os cenários que possam comprometer a continuidade da sua atividade, analisar o seu impacto e promover a resiliência organizacional, dotando a organização da capacidade de prevenir ou, na sua impossibilidade, responder de forma eficaz a estes eventos.

O PCN é constituído por 04 (quatro) fases, Planejamento, Operação, Avaliação/Revisão e Melhoria contínua. Estas fases contemplam todas as responsabilidades dos órgãos responsáveis pela coordenação do programa, as reponsabilidades das áreas envolvidas, os procedimentos para a realização da avaliação/revisão do programa, bem como testes e relatórios de reporte.

7.2 Prestadores de Serviços de Tecnologia

Os procedimentos e controles voltados à prevenção e ao tratamento de incidentes em relação aos prestadores de serviço de Tecnologia são previamente definidos em contratos. Especificamente em relação aos fornecedores de Infraestrutura e SPB, SPI, SAR, SERAP,C3, CETIP e SELIC, a Casa do Crédito recebe mensalmente relatórios com os incidentes ocorridos e, em caso de necessidade, é elaborado um plano de ação corretivo, que é acompanhado pela área de Tecnologia até o seu encerramento.

7.3 Classificação da criticidade dos Incidentes

Os incidentes relacionados à Segurança Cibernética seguem 03 (três) fatores de criticidade, crítica, de emergência e evento inesperado.

7.3.1 Plano de Ação de Resposta a Incidentes

Caso ocorra um incidente, ele deve ser analisado e, após análise, é elaborado um plano de ação para corrigir e/ou melhorar o ambiente e/ou processo com o objetivo de minimizar a possibilidade de nova ocorrência. A elaboração e acompanhamento do plano de ação são coordenados pela Área de Tecnologia da Informação com participação de outras Áreas.

8. TREINAMENTO DE SEGURANÇA NA CASA DO CRÉDITO

A Casa do Crédito incentiva e promove uma cultura de segurança dentro da instituição, visando proteger os objetivos citados nesta política, e principalmente proteger a informação.

A cultura de Segurança Cibernética é disseminada internamente através de programas de capacitação ministrados periodicamente para todos os colaboradores, garantindo assim que todos estejam cientes das possíveis ameaças e vulnerabilidades que podem ocorrer no âmbito da Segurança Cibernética, bem como quais são os procedimentos que devem ser adotados em casos de incidentes.

A Casa do Crédito tem consciência que as atividades no âmbito de Segurança Cibernética estão em constante evolução, sendo assim, os procedimentos e controles relacionados com o tema devem ser revistos com periodicidade no mínimo anualmente, promovendo assim uma melhoria contínua do ambiente de Segurança Cibernética da Casa do Crédito.

9. PUBLICIDADE

A Casa do Crédito disponibiliza esta Política por meio de seu website (www.casadocredito.com.br) a todos os interessados, assim como para seus colaboradores e prestadores de serviços, que por meio do Termo de Compromisso (Anexo II), declaram o pleno conhecimento das diretrizes aqui estabelecidas e o seguimento desta Política.

10. SANÇÕES DISCIPLINARES

Ações que violem esta Política, suas diretrizes, normas e procedimentos, ou que quebrem os controles e procedimentos aqui estabelecidos, serão passíveis de investigações internas, podendo implicar em sanções disciplinares, administrativas e contratuais previstas nas normas internas da Casa do Crédito e na legislação vigente, sem prejuízo das demais medidas administrativas, cíveis e penais cabíveis.

11. COMPARTILHAMENTO DE INFORMAÇÕES

A Casa do Crédito buscando sempre atuar com transparência e objetivando a melhoria dos seus procedimentos relacionados à segurança cibernética, tem o compromisso de compartilhar com o BACEN todos os incidentes relevantes, tempestivamente, sempre que solicitado.

12. CONTRATAÇÃO E GESTÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO DE NUVEM

Toda contratação de serviços de processamento e armazenamento de dados e de computação em nuvem devem estar aderentes com as diretrizes indicadas na Resolução CMN 4.893 do BACEN.

13. MÉTRICAS/INDICADORES DE ACOMPANHAMENTO DO PROCESSO DE SEGURANÇA CIBERNÉTICA

Mensalmente, a área de Tecnologia da Informação disponibiliza o KRI (*Key Risk Indicator*) de acompanhamento de incidentes às áreas de Risco Operacional e Controles Internos da Casa do Crédito.

14. RELATÓRIO ANUAL

A Casa do Crédito, em virtude das apurações decorrentes da implementação da presente Política, expedirá anualmente o "Relatório de Implementação e Acompanhamento do Plano de Ação e Resposta a Incidentes" ("Relatório Anual"), nos termos do Plano de Ação e Resposta a Incidentes. De acordo com a Resolução 4.893 do BACEN, anualmente, até o 31 de março, a Casa do Crédito deverá emitir um relatório sobre a implementação do plano de ação de respostas a incidentes contendo:

- A efetividade da implementação das ações a serem desenvolvidas pela instituição para adequar suas estruturas aos princípios e às diretrizes da política de Segurança Cibernética;
- O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes;
- Os incidentes relevantes ocorridos no período;
- Resultado dos testes de continuidade de negócios.

15. DOCUMENTAÇÃO MÍNIMA A SER ARQUIVADA DECORRENTE DA RESOLUÇÃO CMN 4.893

A Casa do Crédito, disponibilizará todas as documentações que envolvem o procedimento e validade da presente Política, à disposição do BACEN, pelo prazo de 05 anos, contados da sua emissão, incluindo:

- A presente Política;
- Ata da Diretoria com a aprovação da Política;
- Documento relativo ao plano de ação e de resposta a incidentes;
- Relatório anual;
- Documentação sobre os procedimentos;
- Documentação que trata no caso de serviços prestados no exterior;
- Os contratos de prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem;
- Os dados, os registros e as informações relativas aos mecanismos de acompanhamento e de controle que visam assegurar a implementação e a efetividade da política se Segurança Cibernética.

16. AVALIAÇÃO

A Política, os processos e procedimentos ora estabelecidos estão sujeitos a revisões anuais ou quando se fizerem necessárias para atender a legislação vigente ou, ainda, para refletir as possíveis modificações em procedimentos internos da Casa do Crédito, sujeitos a aprovação da Diretoria da instituição.

17. PROPRIEDADE INTELECTUAL

A propriedade intelectual é composta por bens imateriais, tais como marcas, sinais distintivos, slogans publicitários, nomes de domínio, nomes empresariais, indicações geográficas, patentes de invenção e de modelo de utilidade, obras intelectuais (tais como obras literárias, artísticas e científicas, base de dados, fotografias, desenhos, ilustrações, projetos sistêmicos, obras musicais, obras audiovisuais, textos e etc.), programas de computador e segredos empresariais (inclusive segredos de indústria e comércio). Quaisquer informações e propriedade intelectual que pertençam a Casa do Crédito, ou por ela disponibilizadas, não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas, inferidas ou desenvolvidas pelo próprio colaborador em seu ambiente de trabalho.

ANEXO I - CONCEITOS

Ativo de informação – elemento com valor para a Casa do Crédito, para as suas atividades e para a continuidade destas, incluindo as tecnologias de informação e comunicação (TIC) e os recursos de informação da Casa do Crédito que a apoiam no desempenho das suas funções.

Ameaça – causa potencial de incidente indesejável que pode resultar em danos para a Casa do Crédito, para a sua informação ou sistemas de informação. Estas ameaças podem ser acidentais ou deliberadas.

Colaboradores – qualquer pessoa que seja membro da Diretoria, Diretor Executivo, funcionário, estagiário, prestador de serviços ou mandatário, a título permanente ou ocasional, da Casa do Crédito.

Incidente de segurança de informação – qualquer evento que afete ou possa afetar a integridade, disponibilidade, privacidade, confidencialidade, autenticidade, auditabilidade e/ou fiabilidade da informação ou sistemas de informação da Casa do Crédito, incluindo qualquer ação ou omissão, deliberada ou não, que viole a regulação vigente em matéria de segurança de informação.

Informação – todos os dados e registros, tangíveis ou intangíveis, incluindo voz e imagem, independentemente do seu formato, modo de tratamento, meio de transmissão e tipo de suporte, físico ou lógico, relativos à vida da instituição.

Informação da Casa do Crédito – englobam-se neste conceito:

i. toda a informação que é propriedade da Casa do Crédito e aquela que, não sendo da sua propriedade, esteja, para efeitos legais, contratuais ou funcionais, sob a responsabilidade direta ou indireta de qualquer das suas estruturas/áreas;

ii. todos os processos, sistemas, aplicações, serviços, dispositivos, tecnologias, infraestrutura e demais meios de suporte utilizados para criar, registrar, recolher, processar, usar, armazenar, publicar, comunicar, transmitir, transferir, transportar, proteger, recuperar ou eliminar informação, independentemente da sua localização, física e lógica, e da entidade;

iii. responsável por tais atividades.

Prestador de Serviços – pessoa física ou jurídica que presta qualquer tipo de serviços a Casa do Crédito.

Segurança da Informação - preservação adequada da confidencialidade, integridade e disponibilidade da informação; envolve também a capacidade para resistir, com um adequado nível de confiança, a ações que comprometam a confidencialidade, integridade ou disponibilidade dos dados armazenados, transmitidos ou tratados ou a segurança de serviços conexos da Instituição.

Sistema de Informação – conceito abrangente associado ao uso de tecnologias de informação e comunicação no âmbito dos mais variados processos e procedimentos associados à informação.

Tecnologias de Informação e Comunicação (TIC) – expressão que engloba todas as tecnologias, hardware e software, utilizados para criar, registrar, recolher, processar, usar, armazenar, publicar, comunicar, transmitir, transferir, transportar, proteger, recuperar ou eliminar informação.

Vulnerabilidade de segurança de informação – vulnerabilidade técnica, insuficiência dos controles ou outra condição associada a um ativo ou conjunto de ativos de informação que pode ser explorada ou iniciada por ameaças, podendo dar origem ou potenciar a ocorrência de algum incidente de segurança de informação.

Vulnerabilidade técnica – falha, erro, lacuna, fragilidade, insuficiência ou configuração inadequada de um componente tecnológico que processa, transmite e/ou armazena informação (sistemas operativos, bases de dados, aplicações, equipamentos de rede) que pode resultar numa quebra de segurança ou de qualquer outra forma potencializar a ocorrência de incidentes de segurança.