POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

Código da Circular	Anexo	Data de Publicação	Versão
SI-01	**---**	**14.08.2024**	**04**

RESUMO

Estabelece os conceitos, critérios e diretrizes da Plantae S/A – Crédito, Investimento e Financiamento para minimizar possíveis ameaças cibernéticas na segurança da informação.

ÍNDICE

1. OBJETIVO

O objetivo dessa política é estabelecer conceitos, diretrizes e responsabilidades para o gerenciamento da segurança da informação cibernética e promover a melhoria continua dos procedimentos relacionados com a segurança dos dados e informação, para prevenir, detectar e reduzir vulnerabilidade a incidentes relacionados com o ambiente cibernético, possibilitar a manutenção da confidencialidade, da integralidade e da disponibilidade de informações sob responsabilidade da Plantae S/A – Crédito, Financiamento e Investimento.

2. PÚBLICO-ALVO

Esta política se aplica a todos os funcionários em período integral, contratados, consultores, funcionários em meio período, trabalhadores temporários e pessoal autorizado que possuem equipamentos e serviços de TI fornecidos pela Plantae S/A – Crédito, Financiamento e Investimento.

3. CONCEITOS

A Segurança Cibernética, constitui-se da preservação das propriedades da informação, permitindo o uso e o compartilhamento da informação de forma controlada com monitoramento e tratamento de incidentes provenientes de possíveis ataques cibernéticos incluindo os controles relacionados aos serviços de Nuvem contratados. Podemos definir como conjunto de tecnologias, processos e práticas projetados para proteger redes, computadores, sistemas e dados de ataques, danos ou acesso não autorizado. São pilares da Segurança Cibernética:

Segurança da Informação: Conjunto de conceitos, técnicas e estratégias, as quais visam proteger os ativos de informação como um todo da Informação deve proteger o ativo “informação” como um todo (físico ou digital), ou seja, precisa proteger tecnologia, procedimentos e pessoas. A base da Segurança da Informação continua sendo a tríade conhecida como CID:

Confidencialidade: garante que as informações sejam acessíveis somente por pessoas, entidades ou processos autorizados;

Integridade: garante que os dados sejam precisos e confiáveis; protege a informação de sofrer alterações não autorizadas;

Disponibilidade: garante que as informações estejam sempre acessíveis e disponíveis para acessos autorizados.

Outros atributos importantes da Segurança da Informação são:

Autenticidade: garante que a informação é proveniente da fonte anunciada e que não foi alvo de alterações ao longo de um processo;

Irretratabilidade: garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita;

Conformidade: garante que o sistema deve seguir as leis e regulamentos associados ao processo.

Riscos Cibernéticos: São riscos de ataques cibernéticos, internos ou externos, provenientes de software malicioso, ataques de rede, sabotagem, técnicas de engenharia social, violação de acessos e privacidade que podem desproteger dados e sistemas causando danos a reputação ou imagem e danos financeiros.

4. ABRANGÊNCIA

Esta política deverá ser seguida por todos os funcionários, prestadores de serviços, correspondentes no país e conveniados.

A divulgação das atualizações dessa política se dará por meio de comunicação via e-mail e ficará disponível para consulta a qualquer tempo:

Prestadores de Serviços, Correspondentes no País e Conveniados: via e-mail.

5. DIRETRIZES

Com relação a Segurança Cibernética a Plantae S/A – Crédito, Financiamento e Investimento possui as seguintes diretrizes gerais:

5.1. Gestão de Ativos da Informação e Gestão de Acessos

Os ativos da informação devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos, de eventuais adulterações de dados e ter documentação e planos de manutenção atualizados. Para tanto deverá resguardar a proteção dos dados adotando as seguintes medidas:

Todos os funcionários, correspondentes no país, parceiros ou prestadores de serviço com acesso aos sistemas deverão ter um perfil de usuário definido pela instituição, que identificará suas alçadas de acessos aos serviços de rede e aos sistemas de informação;

Os sistemas de informação e os sistemas operacionais e de rede deverão garantir o acesso apenas a usuários autorizados e restringir o acesso às áreas designadas no perfil do usuário;

A identidade do usuário deverá ser estabelecida através de um nome de usuário e ser protegida por senha que deverá ser periodicamente alterada. A senha deverá obedecer à regra de formação e repetição incorporada no sistema, sendo de uso pessoal e intransferível;

Os eventos de tentativas de acesso não autorizados deverão ser registrados pelos sistemas operacionais, de rede e de informações, com aviso ao administrador e verificação periódica.

Zelar pela integridade da infraestrutura tecnológica na qual são armazenados, processados ou de qualquer outra forma tratados os Dados, adotando as medidas necessárias para prevenir ameaças lógicas, como vírus, programas nocivos ou outras falhas que possam ocasionar acessos, manipulações ou usos não autorizados a Dados internos e confidenciais, por meio, dentre outros aspectos: (i) da manutenção de softwares antivírus e firewall instalados e atualizados; (ii) da manutenção dos programas de computador instalados no ambiente;

Os servidores e equipamentos de rede deverão ser protegidos fisicamente contra acesso indevido, seja por meio da sua montagem em racks fechados a chave, seja em salas fechadas e exclusivas. A continuidade operacional deverá ser garantida mediante o abastecimento ininterrupto de energia, com operação de desligamento dos servidores por software, em caso de falha prolongada.

As estações de trabalho deverão:

a) Ser utilizadas exclusivamente por usuários autorizados, mediante identificação do mesmo e protegida por senha e negado o acesso a usuários não autorizados;

b) O uso de pen drive ou outros meios de entradas e saída de informações deverá ser restrito às estações e usuários autorizados, sendo obrigatório a desabilitação nas estações não autorizadas;

c) Somente poderão ser utilizados nas estações de trabalhos software homologado e licenciado, instalado sob supervisão e administração da rede.

Todas as linhas de comunicação de dados, temporárias (discadas) ou prementes (linhas privadas) deverão ser aprovadas e instaladas pela administração de rede. O acesso externo a dados da rede

interna, se existente, deverá ser objeto de projetos próprios que assegurem a confidencialidade, sigilo e proteção das informações.

5.2. Classificação da Informação

Quanto a classificação as informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, abrangendo inclusive a criptografia de dados e de acordo com a classificação dos níveis de relevância: Confidencia, Restrita, pública e Interna, seguindo os conceitos abaixo:

Confidencial: informação que, se divulgada, poderá causar danos à imagem, perda financeira às instituições ou clientes, e violação de requisitos legais ou regulamentares;

Restrita: informação cujo acesso deverá ser mais limitado que a confidencial, restrita apenas a alguns níveis de gerência ou a um grupo restrito de funcionários, conforme designado pela Diretoria responsável pela área de atuação.

Pública: informação livremente disponível no mercado;

Interna: informação relativa a produtos, procedimentos, normas, comunicações;

5.3. Gestão de Riscos

Os riscos devem ser mapeados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação da Plantae S/A – Crédito, Financiamento e Investimento, a fim de que sejam endereçadas as proteções adequadas, que deverá seguir os mecanismos abaixo:

Análise de Impacto nos Negócios (BIA): análise dos processos de negócios que relaciona os efeitos qualitativos e quantitativos em caso de sua interrupção, proporcionando uma visão executiva sobre os processos mais impactantes para a Instituição, denominados processos críticos;

Gestão de Continuidade dos Negócios: processo de gestão abrangente responsável por oferecer uma estrutura que permita à instituição desenvolver resiliência organizacional e capacidade de resposta a eventos inesperados, salvaguardando os interesses das partes interessadas, a reputação e as marcas das instituições;

Gestor de Negócios: diretor ou gerente responsável por processo(s) ou função(ões) crítica(s) dos negócios;

Objetivos de Recuperação: requisitos para a recuperação de um processo ou função crítica, que dependem do impacto causado pela interrupção;

Plano de Continuidade dos Negócios (PCN): guia que documenta e formaliza as estratégias e procedimentos de respostas às emergências, retomada das funções vitais das instituições, alternativas e prazos necessários. Anualmente ou sempre que ocorrerem alterações nos sistemas dos negócios, deverá ser revisado e testado o PCN, com o compromisso de controlar os resultados, visando aprimorar os procedimentos adotados às novas mudanças.

Testes de Acionamentos de Contingência:

São utilizados para garantir que em uma emergência os procedimentos de respostas e retomada das funções vitais ocorram de forma segura e dentro do estabelecido pelo PCN.

Grupo de Respostas às Crises

Grupo de ação específica para tratar crises de maior relevância que afetem as instituições, com objetivo de proteger as pessoas, preservar a imagem, minimizar perdas nos negócios e danos operacionais e promover a retomada da normalidade das operações.

Os incidentes no âmbito da segurança cibernética, inclusive os ocorridos em sistemas operados ou instalados em empresas contratadas que prestam serviços relevantes, devem ser mantidos em registros organizados, com as respectivas análises de causas e da adoção de controles para minimizar a ocorrência de novos eventos, para tanto a Instituição deverá possuir um Plano de Respostas a Incidentes (IRP) alinhado às políticas estabelecidas e aos objetivos de negócios da companhia, possuindo no mínimo as seguintes fases:

- Preparação: como estar preparado e agir diante de um incidente?
- Identificação: quais os critérios de identificação de incidentes?
- Contenção: como conter o incidente? Erradicação: como eliminar a causa-raiz do problema?
- Recuperação: o que fazer para restabelecer a normalidade de todos os sistemas?
- Lições aprendidas: o que fazer para que os mesmos erros não ocorram novamente;

Garantia da Continuidade de Negócios:

O gerenciamento de riscos deve garantir a manutenção da continuidade dos negócios, abrangendo serviços relevantes e a capacidade de continuar a entrega de produtos ou serviços em um nível mínimo aceitável e previamente definido, quando da ocorrência de um evento que interrompa as operações. Para tanto as ações que garantam a continuidade de Negócios deverão estarem previamente estabelecidos no Plano de Continuidade de Negócios.

5.4. Disseminação da cultura de Segurança da Informação e Cibernética

A Instituição deve garantir a disseminação dos princípios e diretrizes de Segurança Cibernética por meio de programas de conscientização e capacitação, fortalecendo a cultura de segurança cibernética e informação, em todos os níveis operacionais para tanto realizará:

- A implementação de programa de treinamento anual para colaboradores;
- A implementação de programa de avaliação periódica de colaboradores quanto ao nível de conhecimento do tema segurança da informação e cibernética;
- A prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos, através da disponibilização a todos os usuários Política de Privacidade que regulará o tratamento de dados fornecidos para usuários e clientes e observará também o disposto na Lei Geral de Proteção de Dados (Lei nº 13.709/2018).
- A ampla divulgação dessa política aos colaboradores, prestadores de serviços e correspondentes no país além de ter a obrigatoriedade de conter clausulas especificas de confidencialidade e de divulgação, não divulgação das informações nos contratos que regem essas relações, e possui desde já o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança da informação e cibernética.

5.6. Processamento, armazenamento de Dados e Computação em Nuvem:

A Instituição, quando da utilização de serviços em nuvem, atenderá fielmente ao Capítulo III – da Resolução CMN Nº 4.893, considerando a avaliação de risco que estes representam para o negócio.

5.7. Responsabilidades e Canal de Comunicação:

Quanto ao cumprimento dessa Política é responsabilidade de:

Colaboradores, Prestadores de Serviços, Correspondentes no País: Cumprir fielmente o disposto na presente política, atuando de forma ética quando tomar conhecimento de incidentes, compartilhando informações com os responsáveis pelo tratamento em tempo hábil. É imprescindível que cada pessoa compreenda o papel da segurança da informação em suas atividades diárias e participe dos programas de conscientização.

Compliance:

Cumprir as diretrizes estabelecidas nesta Política, mantê-la atualizada anualmente de forma a garantir que quaisquer alterações no direcionamento da Instituição sejam incorporadas a mesma e esclarecer dúvidas relativas ao seu conteúdo e a sua aplicação.

Receber e direcionar aos responsáveis para o tratamento as comunicações de quaisquer indícios de irregularidades citadas nesta política ou no plano de respostas a incidentes.

Manter a disposição do Bacen pelo prazo de 5 (cinco) anos a documentação disposta no artigo no Art. 23 da Resolução CMN Nº 4.893.

Alta Administração: Comprometer-se com a melhoria contínua dos procedimentos de controles relacionados a essa política e a construção de mecanismo que possibilitem a iniciativas para compartilhamento de informações sobre os incidentes relevantes, com as demais instituições autorizadas a funcionar pelo Bacen.

Quanto ao Canal de Comunicação: Quaisquer indícios de incidentes ou irregularidades citadas nesta Política, devem ser comunicadas imediatamente para a área de Compliance da Plantae S/A – Crédito, Financiamento e Investimento, pelo e-mail: compliance@plantaeagrocredito.com.br

Acesso a compartilhamentos de arquivos ou bancos de dados para trabalhar com material de propriedade da empresa que o funcionário precisa executar suas funções de trabalho.

- Usando navegadores da Web para obter informações comerciais de sites comerciais.
- Usando e-mail para comunicação comercial.

6. DOCUMENTOS RELACIONADOS

Resolução BACEN 4.474/2016: Procedimentos para a produção e a gestão de documentos digitalizados relativos às operações e às transações realizadas.

Bacen - Resolução 5.089/2023 CMN: Dispõe sobre a estrutura de gerenciamento de riscos e a estrutura de gerenciamento de capital.

Bacen - Resolução 4.893/21 CMN: Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.

Lei 13.709, 14/08/2018: Dispõe sobre a Lei Geral de Proteção de dados.

Lei Complementar nº 105 10/01/2001: Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.

INFORMAÇÕES DE CONTROLE

Versão	Item alterado	Descrição resumida da alteração	Motivo	Data da Publicação
01	Não se aplica	Não se aplica	1ª. Versão	01.01.2020
02	Todos	Revisão geral para adequação à Resolução 4.893 de 26.02.21	Revisão	01.08.2021
03	Domínios	Substituição de domínio: @plantaeif.com.br	@plantaeagrocredito.com.br	21.03.2023
04	Documentos Relacionados	Resolução CMN nº 4.557/2017	Substituída: Resolução CMN nº 5.089/2023	14/08/2024

Responsáveis pelo documento

	Nome	E-mail	Nome da área
Revisão	Antonio Carlos Shiro Hachisuca	antonio.shiro@plantaeagrocredito.com.br	Diretoria
Aprovação	Wolney de Medeiros Arruda	wolney.arruda@plantaeagrocredito.com.br	Diretoria Presidente

Gerência de Riscos, Controles Internos e Compliance