Política de Segurança Cibernética

O objetivo desta Política de Segurança da Informação e Segurança Cibernética é definir processos e controles que a NATIVO PAGAMENTOS EIRELE (doravante referido como Nativo Pagamentos), empresa inscrita no CNPJ sob n.º 35.282.275/0001-40 está sempre atenta às operações e estabelece para proteção da informação e tratamento dos riscos e ameaças relacionadas à Segurança da Informação e Segurança Cibernética, com base na Resolução nº 4893, de 26 de fevereiro de 2021 do Banco Central do Brasil e demais normas e disposições aplicáveis.

A Política orienta e se aplica a todos os colaboradores, prestadores de serviço e estagiários da NATIVO PAGAMENTOS.

A área responsável na NATIVO PAGAMENTOS pelo tema de Segurança da Informação, Segurança Cibernética e referida política é a área de Tecnologia da Informação estabelece as seguintes diretrizes gerais:

I. Garantir e asseverar a confidencialidade, integridade e disponibilidade das informações da Organização, por meio de mecanismos e controles de Segurança da Informação e Segurança Cibernética.

II. Garantir e asseverar a proteção adequada das informações e dos sistemas de informação contra acessos indevidos e não autorizados.

III. Garantir e asseverar a existência de processos para continuidade de negócios e gestão de incidentes de segurança para proteção, detecção, resposta e recuperação contra os ataques cibernéticos.

IV. Asseverar que todos os ativos de informação sejam utilizados apenas para as finalidades aprovadas pela Organização, estando sujeitos à monitoração, rastreabilidade e auditoria.

V. Garantir e asseverar programas de conscientização, educação e capacitação de pessoal, campanhas de Segurança da Informação e Segurança Cibernética, programas de treinamento do quadro de pessoal e avaliação periódica.

VI. Informar aos clientes, colaboradores, terceiros e fornecedores sobre as precauções de Segurança da Informação e Segurança Cibernética necessárias na utilização de produtos e serviços oferecidos pela Organização.

VII. Garantir e asseverar que as informações sejam devidamente classificadas, independentemente da forma como estão armazenadas ou do meio em que sejam transportadas e assegurar que controles voltados para a rastreabilidade da informação sejam aplicados.

VIII. Garantir o cumprimento desta Política, das Normas, dos Padrões e das Diretrizes de Segurança da Informação e Segurança Cibernética da Organização.

IX. Asseverar o comprometimento da alta administração com a melhoria contínua dos processos e recursos necessários para Segurança da Informação e Segurança Cibernética.

Definição

Objetivos da Segurança da Informação É a disciplina que concentra esforços contínuos à proteção dos ativos de informação, auxiliando a Organização a cumprir sua missão e valores. Para tanto, tem como objetivos:

Confidencialidade: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;

Integridade: garantir que as informações sejam mantidas íntegras, sem modificações indevidas (acidentais ou propositais);

Disponibilidade: garantir que as informações estejam disponíveis às pessoas autorizadas;

Responsabilidades

Através da função de PSIRT (Product Security Incident Response Time) pelo e-mail security@nativopagamentos.com , é responsável por estabelecer, por meio da definição de políticas, padrões, procedimentos e controles, a integridade, disponibilidade e confidencialidade das informações contidas nos ambientes da Organização, minimizando possíveis impactos e vulnerabilidades e, reduzindo a ocorrência de incidentes de segurança que afetem os negócios do NATIVO PAGAMENTOS. Também é responsável por entender, gerenciar, reportar e escalar o risco de Segurança Cibernética em sua área (incluindo ativos relevantes, informações, sistemas e terceiros).

Demais atribuições específicas:

- Governança e Gestão de Políticas de Segurança da Informação;
- Gestão de Acessos (Definição de Regras e Critérios) e Segregação de Funções;
- Atendimento das Auditorias e Certificação de Controles Internos de Segurança da Informação;

Demais atribuições específicas:

- Governança e Gestão de Políticas de Segurança da Informação;
- Gestão de Acessos (Definição de Regras e Critérios) e Segregação de Funções;
- Atendimento das Auditorias e Certificação de Controles Internos de Segurança da Informação;
- Definição de Requisitos e Análise de Segurança em Projetos;
- Disseminação da Cultura, Treinamento e Conscientização de Segurança da Informação, através de cursos disponíveis na Intranet, palestras e demais conteúdos eletrônicos;
- Gestão de Riscos e de Indicadores de Segurança da Informação;
- Gestão de Riscos de Segurança da Informação em Fornecedores;
- Gestão e Detecção de Vulnerabilidades;
- Testes de Invasão;
- Busca e Antecipação de Ameaças e Ataques Cibernéticos;
- Garantir que a NATIVO PAGAMENTOS esteja fazendo uso de Sistemas de Detecção e Prevenção de Ataques a Redes;
- Resposta a Incidentes de Segurança Cibernética em conjunto com o Santander;
- Apoiar o Encarregado de Privacidade nos temas pertinentes;

Objetivos da Segurança

Cibernética Segurança cibernética é a capacidade de identificar, prevenir, proteger, detectar, responder e recuperar rapidamente de uma ameaça cibernética, a fim de proteger a

confidencialidade, integridade e disponibilidade dos ativos tecnológicos e informações. Neste contexto:

Espaço cibernético: engloba a internet, os sistemas de informação, os dispositivos móveis e as tecnologias digitais que dão suporte aos negócios, a infraestrutura e os serviços; Incidente de segurança cibernética: todo e qualquer evento não esperado que gere algum tipo de instabilidade, quebra de política ou que possa causar danos à NATIVO PAGAMENTOS;

Ataque cibernético: é a exploração por parte de um agente malicioso para tirar proveito de ponto(s) fraco(s) com a intenção de alcançar um impacto negativo no alvo. Os atacantes podem ter como alvo os clientes, fornecedores e parceiros da NATIVO PAGAMENTOS para causar impacto significante para a Organização;

Risco à segurança cibernética: advêm de dentro e de fora da Organização. O impacto do risco à segurança cibernética engloba perda financeira, danos à reputação, multas regulatórias, perda de vantagem estratégica e interrupção de operações;

Ativos tecnológicos: é qualquer dispositivo físico ou digital, equipamento ou outro componente do ambiente que suporte atividades relacionadas à informação;

Threat intelligence: consiste em todo conhecimento baseado em monitoramento, evidências, contexto, mecanismos e indicadores sobre ameaças existentes, correlacionando com os ativos tecnológicos que podem ser comprometidos a partir da exploração e concretização dessa ameaça.

Vazamento de Dados: é a violação da confidencialidade de informações internas da NATIVO PAGAMENTOS.

Privacidade do Titular: informações de colaboradores, clientes ou terceiros que devem ser preservadas, mantidas em segurança e preservando a identidade do titular. Todas as informações coletadas do titular devem ter seu consentimento explícito.

Princípios de Segurança da Informação

Proteção da Informação

Toda informação gerada ou desenvolvida por qualquer colaborador, prestador de serviço ou estagiário constitui ativo e propriedade intelectual desta, essencial à condução de negócios. Independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente à finalidade à qual foi autorizada pelo gestor da informação. É diretriz que toda informação de propriedade da Organização seja

protegida de forma a não comprometer a sua confidencialidade, integridade ou disponibilidade, como também os dados pessoais ou dados pessoais sensíveis devem ter o consentimento dos titulares desses dados. POLÍTICA Confidencial

Gestão e Controle de Acessos

O gestor de cada sistema é quem deve autorizar o acesso à informação e ao sistema, além de realizar as revisões de acesso conforme especificado pela Organização. Além disso, o gestor deve considerar a conformidade com a política de Privacidade, pois somente pessoas autorizadas devem ter acesso às informações referentes a dados pessoais e dados pessoais sensíveis. Detalhes constam na política de Segregação Funcional.

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 pelo gestor (e quando aplicável pelo proprietário da informação) responsável conforme a necessidade mínima ao cumprimento de suas funções e são rastreados através de logs fornecidos pelos Sistemas de Informação e mecanismos de prevenção a vazamentos de dados. Estas recomendações também são aplicadas com o acesso e o uso de sistemas de informação com terceiros e empresas parceiras.

Autenticação e Senha

Todo colaborador, estagiário ou prestador de serviços é responsável por todos os atos executados com seu identificador (login/sigla de acesso), que é único e acompanhado de senha exclusiva para identificação/autenticação individual no acesso à informação e aos recursos de tecnologia, deve seguir os requisitos da Política e Uso de Senhas nos Sistemas da Empresa, impedir o uso de seu equipamento por outras pessoas enquanto este estiver "logado" e bloqueá-lo ao se ausentar. Detalhes constam na política de Segregação Funcional.

SMS

Para garantir sua segurança, a NATIVO PAGAMENTOS utiliza token SMS para validar o acesso a sua conta. Mantenha seu número de telefone atualizado, assim você garante o recebimento do código de validação.

SSL- CERTIFICADO DE SITE SEGURO

Esta Política aborda as diretrizes, atribuições e responsabilidades no processo de Segurança Cibernética da NATIVO PAGAMENTPOS EIRELE. “NATIVO PAGAMENTOS”.

O certificado de site seguro é um cadeado que apresenta na barra de endereço no site do banco indicando que você está em uma área segura. O certificado é emitido por uma certificadora autorizada e aparecerá na tela confirmando sua autenticidade. Esta é a garantia que você está navegando em um site seguro. Observe sempre se este cadeado apresenta no site do NATIVO PAGAMENTOS que você está acessando. A informação é uma boa forma de segurança.

Prevenção Contra Vírus, Arquivos e Softwares Maliciosos

A Organização possui 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.

Manutenção e Cópias de Segurança O banco Santander, como contratado para prover soluções de tecnologia, possui política e procedimentos específicos para garantir a recuperação de dados e informações. A NATIVO PAGAMENTOS deve garantir que estes processos estejam sendo executados e revisá-los anualmente. POLÍTICA Confidencial

Classificação dos Dados e das Informações

A Organização adota quatro categorias, conforme especificações abordadas no Manual de Classificação de Informação, para efeitos de classificação da informação:

- Público;
- Interno;
- Confidencial;
- Confidencial Restrito;
- Secreto.

O gestor responsável pelo determinado sistema deve garantir que nenhum dado pessoal ou dado sensível seja classificado como informação pública.

Desenvolvimento Seguro e Criptografia

A Organização possui procedimentos específicos relativos a prática de desenvolvimento seguro de sistemas e criptografia. Detalhes constam nos manuais de Boas práticas de desenvolvimento seguro e de gestão de criptografia.

Avaliação de Fornecedores

Provedores e fornecedores que armazenam e processam dados, contratados pela NATIVO PAGAMENTOS são avaliados sob o ponto de vista de Segurança da Informação e Segurança Cibernética e devem seguir seus papéis e responsabilidades. Detalhes constam na política de fornecedores da empresa.

Registro, Resposta e Tratamento de Incidentes de Segurança Cibernética

A política de Gerenciamento de incidentes de Privacidade aborda com maiores detalhes sobre o processo que deve ser seguido pela NATIVO PAGAMENTOS.

Classificação da Relevância dos Incidentes Cibernéticos

A classificação consiste em verificar o impacto causado pelo incidente. Os impactos classificados como P0, P1, P2, são considerados incidentes cibernéticos críticos. Os impactos classificados como P3+, P3, P4 ou P5, são considerados incidentes cibernéticos não críticos. Detalhes constam no manual Cyber Security: Classificação de Cyber Incidente. Devem ser seguidos, pelo prestador de serviços de segurança contratado pela NATIVO PAGAMENTOS, os processos de detecção, responsabilidade pelo registro e mitigação de todos os incidentes cibernéticos classificados como críticos e não críticos e comunicados para a NATIVO PAGAMENTOS sempre que a empresa for impactada.

Origem e Registro dos Alertas dos Incidentes Cibernéticos

Atividades suspeitas ou incidentes identificados através do colaborador ou por qualquer área da NATIVO PAGAMENTOS devem ser comunicados ao CISO através de e-mail específico. Os eventos originados através das ferramentas de monitoração de segurança (SOC), quando envolverem a NATIVO PAGAMENTOS, devem ser comunicados ao CISO da empresa. Provedores e fornecedores que armazenam e processam dados, contratados pela NATIVO PAGAMENTOS, devem reportar os incidentes cibernéticos através do CISO e seguir as diretivas descritas na política de Cyber Security - Gestão de Incidentes de Origem Cibernética.

Prevenção a Incidentes Cibernéticos Threat Intelligence:

Permite que o CISO da NATIVO PAGAMENTOS obtenha informações referentes à possíveis riscos cibernéticos, ameaças, fraudes e incidentes de segurança cibernética às instituições financeiras gerando planos de ação preventivos a partir destas informações.

Cenários de Incidentes Cibernéticos na Gestão de Continuidade de Negócios

O CISO deve comunicar a função de Gestão de Continuidade de Negócios (GCN) caso seja necessário realizar a ativação dos processos abaixo:

- Planos de Continuidade de Negócios: A comunicação deve ser realizada em cenários que ofereçam impacto significativo e risco grave para as áreas de negócios da organização (P0, P1 ou P2).

- Plano de Recuperação de Desastre (PRD): A comunicação deve ser realizada em cenários particularmente sensíveis que ofereçam impacto à infraestrutura tecnológica da organização e impactos as áreas de negócios (P0, P1 e P2).

- Gestão de Situações Especiais: A comunicação deve ser realizada em cenários que ofereçam alto risco às atividades ou que possa acarretar uma deterioração grave na situação financeira da Organização ou do Grupo, causando impactos reputacionais, financeiros ou operacionais (P0, P1 e casos específicos P2).

- O Chief Information Security Officer (CISO): É responsável por comunicar aos demais órgãos reguladores os incidentes cibernéticos ocorridos classificados como P0, P1 e P2 conforme os critérios da NATIVO PAGAMENTOS de classificação e escalonamento de incidentes cibernéticos. Também é responsável por comunicar o Encarregado sobre os incidentes categorizados pela Lei Geral de Proteção de Dados Pessoais (LGPD). Para tanto deverá seguir o modelo de "relatório" de incidentes para os casos aplicáveis. Detalhes constam no manual Cyber Security: Comunicação a demais órgãos reguladores.

Violação da Política e Sanções

Os princípios de Segurança da Informação e Segurança Cibernética estabelecidos nesta política possuem total aderência da Alta Administração da Organização e devem ser observados por todos na execução de suas funções. As violações de segurança devem ser informadas ao gestor imediato e, simultaneamente, à área de Riscos da empresa. Toda violação ou desvio às diretrizes desta política e de outras derivadas da mesma, é investigado para determinação das medidas necessárias e sujeita colaboradores e estagiários a ações disciplinares e trabalhistas e, aos prestadores de serviços e parceiros de negócios, inclui-se a rescisão de contratos e penas de responsabilidade civil e criminal na máxima extensão que a lei permitir. O não cumprimento de algum ponto desta política, intencional ou não, pode levar o colaborador, o estagiário ou o prestador de serviço a sanções disciplinares ou legais, dependendo do caso.

Violação da Política e Sanções

Este documento deve ser revisado pelo menos a cada 12 meses ou a qualquer momento decorrente de mudança regulatória ou alteração de processo relevante.

Controle de Alterações

RESPONSAVEL TECNICO: SAVIO JOSE COLODIANO – EMPRESA SISTEMA SOLUCOES COMPLETAS DENOMINADA "PROSYSTEM SC".

Data Criação: 20/02/2022

Tipo de Documento: Política

Áreas Envolvidas: Cyber Security

Esta Política foi aprovada por comitê virtual em 16/02/2022.