GREEN NET INSTITUIÇÃO DE PAGAMENTO LTDA.

POLÍTICA DE SEGURANÇA CIBERNÉTICA

Julho 2022

Sumário

1. OBJETIVOS

1.1. As diretrizes aqui descritas visam garantir as melhores práticas a serem adotadas para mitigar os riscos relacionados à Segurança Cibernética a fim de assegurar a confidencialidade, integridade e disponibilidade das informações geridas pelo grupo.

1.2. disponibilizamos aqui um resumo de nossa Política de Cibersegurança ("Política") para que você possa saber mais sobre nossas diretrizes para proteção de seus dados.

2. PÚBLICO ALVO

2.1. Esta política contém informações indispensáveis para todos os envolvidos nas operações e processos de negócios da GREEN NET incluindo e não se limitando aos colaboradores, terceiros e prestadores de serviços.

3. DISPOSIÇÕES GERAIS

3.1. DEFINIÇÕES

a. **Confidencialidade:** Garantia que o acesso à informação seja obtido somente por pessoas autorizadas;
b. **Integridade:** Garantia da completude e exatidão da informação e dos métodos de processamento;
c. **Disponibilidade:** Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário;
d. **Risco:** Qualquer evento que possa impactar a organização e os objetivos de negócio;
e. **Ameaça:** Evento ou atitude indesejável que possa remover, danificar, desabilitar ou destruir um ativo ou informação;
f. **Vulnerabilidade:** Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;
g. **Incidente:** Qualquer evento que não faz parte da operação normal de um serviço e que pode causar interrupção de serviços ou redução de sua qualidade;
h. **Cloud / Nuvem:** Rede integrada na internet que oferece serviços de tecnologia com manutenção e recursos terceirizados.

4. DESCRIÇÃO DAS REGRAS/PROCEDIMENTOS

4.1. DE RISCOS CIBERNÉTICOS

4.1.1. A GREEN NET INSTITUIÇÃO DE PAGAMENTO LTDA. faz a gestão de riscos cibernéticos de forma contínua a fim de mitigar as ameaças, riscos e possíveis

consequências que estes possam trazer aos negócios do grupo. Tal gestão é realizada através de medidas práticas utilizando-se de ferramentas de mercado e políticas e treinamentos para conscientização de seus colaboradores.

5. RESPONSABILIDADE E CONTROLE DE ATIVOS

5.1. Todos os ativos possuem um proprietário, que é responsável por garantir a proteção e o correto uso deles, assegurando também a classificação e análise crítica do uso e acesso dos ativos. Os equipamentos de uso comum, pertencentes à estrutura da GREEN NET permanecem sob responsabilidade do gestor da área, sendo o mesmo o responsável pelo controle do uso dos equipamentos.

5.2. Identificamos, analisamos, avaliamos e tratamos os riscos que envolvam os ativos de informação, por meio de avaliações periódicas, a intervalos regulares.

6. CRIPTOGRAFIA DE DADOS

6.1. Informações consideradas sensíveis, como senhas e dados de portadores, devem ser armazenados utilizando controles criptográficos. Os sistemas utilizados pela GREEN NET devem conter criptografia em dados sensíveis, garantindo a confidencialidade das informações.

7. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

7.1. O processo de gestão de incidentes de segurança da informação tem como objetivo garantir que eventos de segurança da informação associados a ativos de informação da GREEN NET sejam comunicados a Área de Segurança da Informação.

7.2. É de responsabilidade da Área de Segurança da Informação coordenar todas as atividades pertinentes ao processo de gestão de incidentes de segurança da informação. É dever de todos os usuários de informação comunicar um incidente de segurança da informação para área responsável. Esse item tratamos melhor no plano de ação e de resposta a incidentes.

7.3. Monitoramos de forma contínua os ativos de informação e utilizamos processos, controles e tecnologias de prevenção e resposta a ataques cibernéticos.

8. ANÁLISE E GESTÃO DE NÃO CONFORMIDADES

8.1. A GREEN NET possui uma política que direciona o tratamento dos incidentes que venham a acontecer e de não conformidades com as políticas internas.

9. GESTÃO DE CONTINUIDADE DE NEGÓCIOS

9.1. Plano de Continuidade de Negócios é uma estratégia documentada para a continuidade das operações caso acontecerem eventos que impactem o negócio de forma negativa. Para sua perpetuidade, as práticas lá estabelecidas devem ser seguidas à risca.

10. CONSCIENTIZAÇÃO E TREINAMENTOS

10.1. Os usuários devem conhecer as suas obrigações e responsabilidades em cada um dos sistemas, sendo o Gestor da Área o responsável ou designar um colaborador apto a realizar o treinamento dos colaboradores perante as responsabilidades de cada um.

10.2. Concedemos a funcionários e a terceiros somente o acesso às informações necessárias ao desempenho de suas funções e atribuições previstas em contrato ou por determinação legal.

11. REGULAMENTAÇÃO

11.1. Resolução BCB Nº 85, de 8 de abril de 2021;

Data da última revisão: 01.07.2022.