Política de Segurança Cibernética da Green Net

Sumário

1. OBJETIVO

A presente Política de Segurança Cibernética ("Política") foi elaborada em conformidade com a Resolução do Banco Central do Brasil (BCB) nº 85, de 8 de abril de 2021 ("Resolução BCB nº 85"), e estabelece as diretrizes mínimas para garantir a segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem da GREEN NET INSTITUIÇÃO DE PAGAMENTO LTDA. ("Green Net").

O objetivo da Política é garantir a proteção das informações e dos sistemas da Green Net contra ameaças cibernéticas. A Política estabelece diretrizes para prevenir, detectar e reduzir vulnerabilidades a incidentes cibernéticos, assegurando a confidencialidade, integridade e disponibilidade dos dados, bem como a continuidade das operações.

2. ABRANGÊNCIA

A Green Net é uma empresa que compõe o Grupo Econômico formado por CARGUERO INOVAÇÃO LOGÍSTICA E SERVIÇOS S.A., CARGUERO S LTDA. e DABHE 2 PARTICIPAÇÕES LTDA. ("Companhia").

Esta Política aplica-se a todas as áreas da Green Net, bem como a seus respectivos colaboradores, fornecedores, clientes, parceiros comerciais e administradores no desenvolvimento de suas atividades, ainda que diretamente ligados a qualquer das outras empresas da Companhia.

Recomenda-se, ainda, que fornecedores, prestadores de serviços, parceiros comerciais e quaisquer terceiros, quando do seu relacionamento com ou representando a Green Net, conheçam o conteúdo deste documento e pautem suas ações considerando o disposto nesta Política.

3. DEFINIÇÕES

Para os fins desta Política, os termos definidos abaixo terão o seguinte significado:

- ***Cloud* (Nuvem):** Rede integrada na internet que oferece serviços de tecnologia com manutenção e recursos terceirizados.
- ***Malware***: É qualquer software intencionalmente feito para causar danos a um computador, servidor ou a uma rede de computadores.
- **Risco:** Qualquer evento que possa impactar a organização e os objetivos de negócio.
- **Vulnerabilidade:** Fragilidade que apresenta riscos potenciais que caso sejam materializados podem gerar danos à organização.

4. PRINCÍPIOS

A Política de Segurança Cibernética é fundamentada na preservação dos seguintes princípios:

I. Confidencialidade: Garantir que as informações sejam acessíveis exclusivamente a indivíduos autorizados.

II. Integridade: Assegurar que as informações, tanto em trânsito quanto armazenadas, permaneçam completas, precisas e imunes a alterações ou remoções não autorizadas.

III. Disponibilidade: Garantir que as informações estejam sempre acessíveis e prontamente disponíveis quando necessárias.

5. DIRETRIZES

5.1. GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

A Green Net mantém uma abordagem contínua na gestão de riscos de segurança da informação, visando mitigar, prevenir ou transferir eventuais riscos e suas consequências para suas operações. Essa administração é conduzida por meio de ações práticas, envolvendo o uso de ferramentas de mercado, implementação de políticas, estabelecimento de processos e a conscientização de colaboradores e terceiros.

5.2. GESTÃO DE VULNERABILIDADES TÉCNICAS

O gerenciamento de vulnerabilidades tem como objetivo identificar, tratar e mitigar os riscos decorrentes de falhas técnicas ou sistêmicas nos produtos e serviços da Green Net. A identificação de vulnerabilidades é realizada por meio de uma combinação de testes de intrusão, ferramentas automatizadas e análises qualitativas e quantitativas, conduzidas pelas equipes de segurança e especialistas envolvidos.

5.3. CRIPTOGRAFIA DE DADOS

A utilização de mecanismos criptográficos é fundamental para garantir a preservação da integridade e confidencialidade de dados críticos e sensíveis ao negócio. Ao empregar técnicas de criptografia de dados, a Green Net assegura que as informações vitais permaneçam protegidas contra acessos não autorizados, contribuindo assim para um ambiente mais seguro e confiável.

5.4. CONTROLE DE MALWARE

O *malware é um código malicioso, projetado para prejudicar sistemas e computadores e* representam ameaças significativas, podendo comprometer a integridade, confidencialidade e a

disponibilidade dos dados. Dessa forma, a Green Net emprega medidas técnicas, por meio de ferramentas de mercado e processos robustos, para assegurar a proteção dos ambientes digitais.

5.5. CÓPIAS DE SEGURANÇA

As cópias de segurança representam uma salvaguarda essencial contra perdas de dados causadas por incidentes como falhas de *hardware*, ataques de *malware*, exclusões acidentais ou outros eventos catastróficos. Ao criar e manter cópias regularmente atualizadas dos dados, a Green Net garante a capacidade de restaurar informações vitais em caso de imprevistos. Isso não apenas protege contra a perda irreparável de dados valiosos, mas também contribui para a continuidade operacional, conformidade com regulamentações vigentes e assegura a confiança das partes interessadas.

5.6. PREVENÇÃO E DETECÇÃO DE INTRUSÃO

Com o intuito de aderir plenamente às diretrizes estabelecidas, a Green Net implementa medidas proativas que aprimoram suas defesas contra ameaças digitais. Esse comprometimento abrange a adoção de *firewalls* robustos, a implementação de segurança de borda, a otimização da eficácia do Centro de Operações de Segurança (SOC), a utilização de sistemas de detecção de anomalias e a manutenção constante da atualização de softwares, visando mitigar vulnerabilidades conhecidas.

5.7. GESTÃO DE ACESSOS

Os acessos físicos às instalações e dependências da Green Net estão sujeitos a controles rigorosos para assegurar que apenas indivíduos autorizados tenham permissão de entrada. Esse processo inclui monitoramento constante e a proteção adequada dos registros associados.

No que diz respeito aos acessos lógicos, a responsabilidade pela gestão é da área de Segurança da Informação da Green Net, isso garante um controle eficaz sobre o ciclo de vida das credenciais de acesso, seguindo a premissa de conceder apenas os privilégios mínimos necessários.

5.8. VAZAMENTO DE INFORMAÇÕES

A Green Net adota medidas rigorosas para prevenir e mitigar potenciais vazamentos de dados. No âmbito técnico, destaca-se a utilização do *Data Loss Prevention* (DLP), cujo propósito é evitar a perda de dados decorrente de possíveis violações. Esse sistema atua por meio do monitoramento, detecção e bloqueio de dados confidenciais durante sua utilização, em trânsito ou em repouso. Além disso, o DLP abrange a proteção de dados pessoais e sensíveis, garantindo uma abordagem abrangente na segurança da informação.

5.9. DESENVOLVIMENTO SEGURO

No que concerne ao ciclo de desenvolvimento e na implementação de novas tecnologias, a Green Net garante que os controles e processos estabelecidos para identificar e corrigir vulnerabilidades sejam realizados antes que entrem em ambiente de produção.

5.10. GESTÃO DE TERCEIROS E FORNECEDORES

A Green Net controla o acesso dos dados organizacionais compartilhados aos fornecedores e terceiros, garantindo que eles acessem apenas as informações necessárias para a execução dos serviços.

5.11. SEGURANÇA NAS COMUNICAÇÕES

As transmissões das informações são protegidas com o objetivo de garantir sua segurança. Logo, as redes possuem controles implementados que asseguram que os serviços a ela conectados não sofram acessos desautorizados.

5.12. CLASSIFICAÇÃO DA INFORMAÇÃO

A Green Net valoriza a informação como um ativo fundamental para a execução de seus objetivos institucionais. Com esse entendimento, a Instituição implementa diretrizes que tem como propósito direcionar a classificação das informações, visando adotar medidas de proteção apropriadas, levando em consideração seu valor, requisitos legais, sensibilidade e importância.

5.13. SERVIÇOS RELEVANTES

A contratação de serviços em nuvem na Green Net atende requisitos estipulados pelo Banco Central do Brasil e são documentados, considerando a criticidade do serviço e a sensibilidade dos dados e das informações a serem processadas, armazenadas e gerenciadas pelo prestador de serviços em nuvem, levando em conta, inclusive, a classificação das informações.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem é comunicada ao Banco Central do Brasil, informando a denominação da empresa contratada, os serviços relevantes contratados e a indicação dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados armazenados, quando aplicável.

Caso a contratação de serviços relevantes de processamento, armazenamento e de computação em nuvem seja prestado no exterior, a Green Net garantirá o atendimento aos requisitos estipulados no Art.16 da Resolução BCB nº 85.

Quanto aos contratos para prestação de serviços relevantes de processamento, armazenamento e de computação em nuvem, contém cláusulas-padrão que atendem os requisitos estipulados no Art. 17 da Resolução BCB nº 85.

5.14. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

O incidente de segurança da informação é toda ocorrência, confirmada ou sob suspeita, que pode comprometer a confidencialidade, integridade e disponibilidade no ambiente.

Todo incidente de segurança da informação é reportado para análise da área de Segurança da Informação e são classificados conforme sua criticidade para a continuidade do negócio, o impacto na usabilidade dos serviços e o impacto financeiro.

Em caso de suspeita ou confirmação de um incidente de segurança da informação, o usuário deverá informar imediatamente a Green Net, por meio do e-mail: csirt@strada.log.br

Em conformidade com a Resolução BCB nº 85, a Green Net comunicará tempestivamente ao Banco Central do Brasil as ocorrências de incidentes relevantes e das interrupções dos serviços relevantes, que configurem situação de crise pela Green Net, bem como das providências para o reinício das suas atividades. Além disso, disponibilizará um Relatório Anual sobre a Implementação do Plano de Ação e de Resposta a Incidentes, considerando todos os aspectos desde a identificação e a tratativa do incidente.

5.15. CONSCIENTIZAÇÃO E TREINAMENTOS

A Green Net se compromete a treinar e conscientizar continuamente seus colaboradores e terceiros, com o objetivo de disseminar a cultura de segurança cibernética na Instituição, como também prestar informações aos usuários, de modo geral, sobre precauções em segurança cibernética na utilização de produtos e serviços oferecidos.

6. MEIO DE CONTATO

Para quaisquer questões relacionadas a essa Política, entre em contato com a área de Segurança da Informação pelo endereço de e-mail: csirt@strada.log.br

Aprovado pela Diretoria da Strada no dia 27 de Março de 2025.