POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

Versão 1.2 | 2025

1 INTRODUÇÃO

A Política de Segurança da Informação e Cibernética (“Política”) tem por objetivo estabelecer as regras, procedimentos e controles de segurança da informação da Greenn Pagamentos e Tecnologia Ltda. EPP (“Greenn”), conforme as previsões regulatórias.

A Segurança da Informação pode ser entendida como a capacidade de prevenir, detectar, responder e de se recuperar rapidamente de uma ameaça cibernética, a fim de proteger a confidencialidade, integridade e disponibilidade dos ativos tecnológicos e informações.

Dessa forma, o objetivo desta política é descrever o uso aceitável de equipamentos de informática da Greenn. Essas regras estão em vigor para proteger nossos parceiros, Colaboradores que fazem parte do escopo PCI e a própria empresa do uso inapropriado desses ativos, que possam expor a Greenn a riscos, incluindo ataques de vírus, comprometimento de sistemas e serviços de rede, situações reputacionais e violações legais.

Por meio desta Política, buscamos manter os Princípios do *Privacy by Design*, mantendo a funcionalidade total das operações. Isso quer dizer que o documento não tem o objetivo de impor restrições que sejam contrárias à cultura estabelecida na Greenn de abertura, confiança e integridade e sim ter uma abordagem *risk oriented*, contra ações ilegais ou prejudiciais por parte de indivíduos, conscientes ou não.

Ainda, esta Política visa viabilizar a identificação de possíveis violações de segurança da Informação, por meio da definição de ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e digitais, a fim de mitigar, assim, os riscos de segurança da informação, garantindo, ainda, a continuidade de seus negócios, protegendo os processos críticos de interrupções causadas por falhas ou desastres.

Ressalta-se que esta Política é condizente com:

I - o porte, o perfil de risco e o modelo de negócio da Greenn;

II – a natureza das suas atividades e a complexidade dos serviços e produtos por ela fornecidos;

III – a sensibilidade dos dados e das informações sob responsabilidade da Greenn.

2 NORMAS DE REFERÊNCIAS

Normas que servem de referência para a elaboração desta Política:

Lei nº13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados;
Resolução CD/ANPD nº 2 de 27 de janeiro de 2022: Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte;
Standard PCI DSS v.4.0.1: framework das especificações, ferramentas, medições e recursos de suporte para ajudar as organizações a garantirem o manuseio seguro das informações do titular do cartão em todas as etapas exigidos pelo *PCI Security Standards Council*.

3 ÂMBITO DE APLICAÇÃO

A presente Política será aplicável a todos os Colaboradores, principalmente os que fazem parte do escopo *PCI*, membros da Alta Administração, Terceiros e quaisquer outras pessoas, sejam físicas ou jurídicas, que tenham ou venham a ter acesso aos dados controlados e ao sistema de informação da Greenn.

3.1 O não cumprimento desta Política

O não cumprimento desta Política acarretará sanções administrativas, podendo acarretar o desligamento do colaborador ou rescisão do contrato vigente e a reparação de danos, de acordo com a gravidade da ocorrência.

4 DEFINIÇÕES

Visando auxiliar na interpretação e aplicação desta Política, as palavras com iniciais maiúsculas, seja no singular ou no plural, devem ser entendidas da seguinte forma:

Alta Administração: membros que compõem a diretoria executiva e o conselho da administração, caso esteja implementado.
ANPD: Autoridade Nacional de Proteção de Dados.
Clientes: usuários que adquirem ou utilizam de alguma forma os serviços da Greenn.

Colaborador(es): Prestadores de Serviços que fazem parte do escopo PCI.

Incidente de segurança com dados pessoais: "Incidente de segurança com dados pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais" (Definição da ANPD).

Payment Card Industry Data Security Standard (PCI DSS): Padrão de Segurança de Dados da Indústria de Pagamento com Cartão.

Segurança Cibernética: proteção de dados e informações de fontes externas no ciberespaço ou na internet.

Segurança da Informação: proteção de informações e sistemas de informações contra uso, modificação e/ou remoção não autorizada.

Terceiros: parceiros comerciais, dentre outras pessoas jurídicas ou físicas que se relacionam comercialmente com a Greenn.

5 GOVERNANÇA EM PROTEÇÃO DE DADOS

A Governança tem o objetivo de organizar e implementar políticas, procedimentos, estruturas, cultura de proteção de dados na empresa, bem como definir papéis e responsabilidades de cada agente de tratamento para atender às necessidades atuais e futuras das questões referentes à proteção de dados.

A Greenn, por intermédio de sua Governança, adotou a estrutura operacional híbrida de Grupo de Trabalho composto por integrantes de áreas-chave da empresa, capazes de deliberar e decidir sobre assuntos relacionados à privacidade e proteção de dados: Compliance, Jurídico, Estratégia e Governança, Tecnologia da Informação, Financeiro e Administrativo.

Os principais objetivos dessa estrutura operacional híbrida composto por integrantes de áreas-chave são gerenciar e garantir a aplicação do programa de privacidade e proteção de dados pessoais, devendo-se reunir trimestralmente ou sempre que necessário, para apresentação e acompanhamento do programa. Nesse sentido, poderá deliberar e tomar decisões de maneira autônoma a respeito de atividades de tratamento que envolvem riscos avaliados como baixo e médio.

Já para aqueles avaliados como alto ou muito alto, a decisão deverá ser escalada à Alta Direção da Greenn.

6 DIRETRIZES GERAIS DE RESPONSABILIDADE E CONFORMIDADE

Esta Política tem o intuito de assegurar a proteção dos ativos de informação contra ameaças, internas ou externas, reduzir a exposição a perdas ou danos decorrentes de falhas de segurança da informação e garantir que os recursos adequados estarão disponíveis, mantendo um programa de segurança efetivo e conscientizando Colaboradores e Terceiros acerca do tema, principalmente dos que fazem parte do escopo PCI.

A gestão e a aplicação do programa de privacidade e proteção de dados pessoais deverão ser conduzidas, gerenciadas e controladas pelo *Chief Compliance Officer (CCO)*, para que possa facilitar o controle de conteúdo, datas de publicação, prazos para revisão e demais medidas e procedimentos envolvendo as Políticas, além de realizar auditorias periódicas para verificar suas conformidades.

O Chief Technology Officer (CTO) é responsável por desenvolver e manter a Política de Segurança da Informação, supervisionar a implementação de medidas de segurança em toda a organização e promover a conscientização sobre segurança da informação entre todos os funcionários ao passo que o DevOps é responsável por implementar e manter controles de segurança nos ambientes de desenvolvimento, teste e produção, garantindo que todas as mudanças no ambiente de TI e CDE sejam avaliadas quanto ao impacto na segurança da informação, monitorar e responder a incidentes de segurança imediatamente 24/7.

Os processos de segurança de dados e da informação da Greenn devem assegurar a:

- **Confidencialidade**: Garantia de que a informação somente estará acessível para pessoas autorizadas;
- **Integridade**: Garantia de que a informação, armazenada ou em trânsito, não sofrerá qualquer modificação não autorizada, seja esta intencional ou não;
- **Disponibilidade**: Garantia de que a informação estará disponível sempre que for necessário.

- **Autenticidade**: Garantia sobre a fonte segura da informação;
- **Não repúdio**: Garantia de monitoramento de uso, evitando negativa de autoria.

Ainda, a Greenn assegura que:

- Todos os dados pessoais coletados serão tratados conforme a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/ 2018), sendo utilizados somente para a finalidade para a qual foram coletados;
- Baseará a gestão de seus sistemas e ambientes virtuais com base em análises de riscos revisadas periodicamente;
- A definição e implementação de controles terá como parâmetro normas nacionais e internacionalmente reconhecidas na área de sistemas de gestão de segurança da informação e segurança da informação;
- Com base nas avaliações de riscos e perfil da organização será elaborado cenário de incidentes considerados nos testes de continuidade dos serviços;
- Classifica os dados e as informações quanto à relevância;
- Divulga e capacita a sua equipe, a fim de disseminar a cultura de segurança da informação.

Ainda, todos os processos e indicadores são reportados à Alta Administração como processo de prestação de contas, tomada de decisões estratégicas e desempenho da segurança da informação. Os indicadores utilizados nestes casos são incidentes de segurança relatados ou detectados, conformidade, vulnerabilidades identificadas, segurança da infraestrutura de TI, treinamento e conscientização de colaboradores e eventuais prestadores de serviço, assim como o grau de adesão à esta Política de Segurança da Informação e Segurança Cibernética.

6.1 Diretrizes gerais de responsabilização e conformidade

Ainda, a Greenn poderá realizar auditorias e monitoramento em suas redes, dispositivos e sistemas periodicamente para garantir a conformidade com esta Política.

6.1.1 Novos Dispositivos

Para que novos dispositivos sejam incluídos na rede e ao sistema, a aprovação explícita pelo gestor competente é necessária.

6.1.2 Autenticação

Todo uso de tecnologia ou dispositivos deve ser autenticado com ID de usuário e senha ou outro item de autenticação (por exemplo, *token*), conforme Política de Senha Segura.

6.1.3 Rastreamento

Todas as tecnologias ou dispositivos exigem uma lista de todo o pessoal autorizado a usar os dispositivos, conforme princípios de *need to know*.

6.1.4 Marcação

Todas as tecnologias ou dispositivos exigem rotulagem de dispositivos com proprietário, informações de contato e finalidade.

6.1.5 Classificação e acesso à informação

As informações devem ser classificadas e acessadas de acordo com esta Política.

6.1.6 Laptops

Como as informações contidas em *notebooks* são especialmente vulneráveis, deve-se ter cuidado especial, dessa forma o uso dos mesmos deve ser realizado conforme o presente documento.

6.1.7 *Software* antimalware

O uso de *software* de proteção contra *malware* deve estar em conformidade com o presente instrumento.

6.1.8 E-mail

A comunicação via e-mail e utilização dessas ferramentas deve estar em conformidade com o presente instrumento.

6.1.9 Usos proibidos

Os ativos, sistemas e bens da Greenn em nenhuma circunstância poderão ser utilizados para atividades ilícitas ou que vão em encontro com os objetivos, missão e cultura da empresa, assim como suas Políticas internas.

A lista, a seguir, de condutas proibidas, é exemplificativa. São terminantemente proibidos(as):

- A distribuição ou acesso de informações confidenciais, restritas por pessoas que não possuam a devida autorização de segurança;
- Violações dos direitos de qualquer pessoa ou empresa protegida por direitos autorais, segredo comercial, patente ou outra propriedade intelectual, ou leis ou regulamentos semelhantes, incluindo, mas não limitado à instalação ou distribuição de produtos de *software* "pirateados" ou outros que não sejam devidamente licenciados para uso pela Greenn;
- Realização ou uso de cópia não autorizada de material protegido por direitos autorais, incluindo, mas não limitado a digitalização e distribuição de fotografias de revistas, livros ou outras fontes protegidas por direitos autorais, música protegida por direitos autorais e a instalação de qualquer software protegido por direitos autorais para o qual a Greenn ou o usuário final não tenha uma licença ativa;
- A exportação de software, informações técnicas, *software* ou tecnologia de criptografia, em violação às leis internacionais ou regionais de controle de exportação, sem a devida autorização;
- A introdução de programas maliciosos na rede ou servidor da Greenn ou de Terceiros (por exemplo, vírus, *worms*, cavalos de Tróia, bombas de e-mail, etc.);
- A revelação da senha de contas de acesso para outras pessoas ou permissão do uso de contas de acesso por outras pessoas. Isso inclui familiares e outros membros da família quando o trabalho está sendo feito em casa;

- O uso de um ativo de computação da Greenn para se envolver ativamente na aquisição ou transmissão de material que viole as leis de assédio sexual ou locais de trabalho hostis na jurisdição local do usuário;
- A feitura de ofertas fraudulentas de produtos, itens ou serviços provenientes de qualquer conta da Greenn;
- Efetuar violações de segurança ou interrupções de comunicação de rede. As violações de segurança incluem, mas não se limitam, a acessar dados dos quais o colaborador não é um destinatário pretendido ou fazer login em um servidor ou conta que os Colaboradores que fazem parte do escopo PCI não estão expressamente autorizados a acessar, a menos que essas funções estejam dentro do escopo das funções normais. Para os propósitos desta seção, "interrupção" inclui, mas não se limita a: detecção de rede, inundações de *ping*, falsificação de pacotes, negação de serviço e informações de roteamento forjadas para fins maliciosos;
- A varredura de portas ou varredura de segurança de forma independente é expressamente proibida, a menos que seja feita uma notificação prévia ao Gestor responsável;
- Executar qualquer forma de monitoramento de rede que intercepte dados, a menos que essa atividade faça parte do trabalho/dever normal dos Colaboradores que fazem parte do escopo PCI;
- Contornar a autenticação do usuário ou a segurança de qualquer *host*, rede ou conta;
- Usar qualquer programa, script e/ou comando ou enviar mensagens de qualquer tipo com a intenção de interferir ou desabilitar a sessão do terminal de um usuário, por qualquer meio, localmente ou via Internet, Intranet e/ou Extranet;
- Revelar informações ou listas de colaboradores da Greenn para terceiros;
- Enviar e-mail não solicitado, realizar o envio de mensagens de e-mail não solicitadas, incluindo o envio de “lixo eletrônico” ou outro material publicitário para indivíduos que não solicitaram especificamente esse material (*spam* de e-mail);
- Envio de PANs (números de cartão de crédito) não criptografados por qualquer tecnologia de mensagens do usuário final (e-mail, mensagens instantâneas, bate-papo);
- Realizar qualquer forma de assédio via qualquer canal de comunicação;

- Realizar o uso não autorizado ou falsificação de informações de cabeçalho de e-mail;
- Criação ou encaminhamento de "correntes", "Ponzi" ou outros esquemas de "pirâmide" de qualquer tipo;
- Publicar mensagens não relacionadas a negócios iguais ou semelhantes em muitos grupos de notícias *Usenet* (spam de grupo de notícias).

7 PROCEDIMENTOS E CONTROLES

7.1 Classificação de Informações e Dados Pessoais

As informações, dados e documentos operados pela Greenn serão classificados de acordo com as categorias abaixo indicadas, considerando a sensibilidade e a relevância do seu conteúdo para a Greenn e para os seus Clientes:

- **Nível 01 - Documentos Públicos**: Informações aprovadas pela Alta Administração para uso público (interno e externo), por exemplo: relatórios anuais, indicações para a imprensa etc.;
- **Nível 02 - Somente Uso Interno**: Informação não aprovada para circulação fora da Greenn como, por exemplo: políticas classificadas como de uso interno e restrito, memorandos internos, minutas e atas de reuniões, procedimentos, rotinas operacionais e relatórios de projetos internos;
- **Nível 03 – Confidencial**: Informações cuja circulação interna é controlada, por questões estratégicas e de gestão, e cuja circulação externa é vedada, pois se tornadas públicas ou compartilhadas causarão impacto e prejuízos aos negócios, podendo ser: documentos do escopo PCI ou ambiente CDE, planos estratégicos e especificações que definem a forma que a organização opera, informações contábeis, planos de negócio, informações sobre clientes ou acionistas, políticas classificadas como confidencial, entre outros. Este nível envolve todas as informações e dados referentes aos Clientes da Greenn, inclusive dados pessoais.
- **Nível 04 - Informações Sensíveis**: Informações internas ou confidenciais críticas ao desenvolvimento das atividades da Greenn, que: (i) são referentes a dados pessoais sensíveis e de crianças e adolescentes (ii) são acobertadas por sigilo bancário, nos termos da legislação aplicável; e/ou (iii) cuja perda ou

indisponibilidade pode prejudicar ou impedir a adequada prestação de serviços pela Greenn aos clientes, a realização de operações da Greenn e/ou o cumprimento de suas obrigações legais e/ou normativas.

7.1.1 Restrição de Acessos

Apenas poderão ter acesso a informações aqueles indivíduos que realmente precisam saber sobre elas para desempenhar suas atividades. O acesso às informações se dará conforme os seguintes requisitos:

- **Nível 01:** Livre acesso;
- **Nível 02:** Colaboradores, Parceiros e Terceiros relacionados à Greenn com acordos de confidencialidade assinados que têm uma necessidade comercial de saber;
- **Nível 03:** Colaboradores, Parceiros e Terceiros designados com acesso aprovado e acordos de confidencialidade assinados;
- **Nível 04:** Somente os indivíduos designados com acesso aprovado e acordos de confidencialidade assinados. O acesso deve ser restrito a poucos colaboradores, de preferência gestores.

7.2 Da Auditoria

A Greenn se reserva o direito de auditar qualquer dispositivo utilizado pelos indivíduos sujeitos a esta Política durante o desempenho das atividades comerciais ou funções, para este fim serão solicitados os acessos, que podem incluir (rol exemplificativo):

- Nível de usuário e/ou acesso em nível de sistema a qualquer computação ou comunicação;
- Acesso às informações (eletrônicas, impressas, etc.) que possam ser produzidas, transmitidas ou armazenadas em equipamentos ou instalações da Greenn;
- Acesso às áreas de trabalho (escritórios, cubículos, áreas de armazenamento, data centers, centros de operações, etc.);
- Acesso para monitorar e registrar interativamente o tráfego nas redes da Greenn.

Além disso, estabelece auditoria planejada com periodicidade mensal.

Esta auditoria deve observar as regras da Lei Geral de Proteção de Dados e sua possibilidade informada na Comunicação Interna de Privacidade aos Colaboradores da Greenn, principalmente dos que fazem parte do escopo PCI.

7.2.1 Uso de equipamentos corporativos, responsabilidade com os dados de acesso e restrições de acesso

A Greenn fornecerá os equipamentos eletrônicos que sejam necessários à execução das atividades pelos Colaboradores que fazem parte do escopo PCI, tais como: *laptops, pen-drives, tablets*, celulares, dentre outros, podendo assim realizar varreduras e investigações internas nos equipamentos corporativos. Além disso, a Greenn se propõe a implementar em seus equipamentos e sistemas um controle de acesso aplicável a todos os usuários, com níveis de permissão na proporção da necessidade de trabalhar com o sistema e de acessar dados pessoais, conforme determinado nesta Política.

Os Colaboradores, inclusive que fazem parte do escopo PCI, são responsáveis por todos os atos executados com seu identificador (*login*), que é único e acompanhado de senha exclusiva para identificação/autenticação individual no acesso à informação e aos recursos de tecnologia, estando proibido de ceder ou facilitar o uso do seu identificador ou o uso de equipamentos por outras pessoas, ainda, enquanto estiver ausente deverá bloqueá-los, outros detalhes constam na Política de Segurança da Informação e Segurança Cibernética.

7.3 Prevenção à Indisponibilidade do Sistema e Ambientes Virtuais da Greenn

A Greenn dedicará equipe interna específica para a implementação de melhorias e monitoramento da integridade do sistema e ambientes virtuais, ademais, para reduzir as chances de indisponibilidade tem como medidas de controle:

- Redundância de *links* de internet e de servidores;
- *Load balance*;
- Assistência externa com o provedor de internet com SLA máximo de 24h (vinte e quatro horas) para a solução, quando estiver sem acesso à rede.

7.3.1 Manutenção e cópias de segurança

A Greenn realizará cópias de Segurança (*Backup*) e recuperação (*Restore*) de dados e informações, inclusive das informações e dados que, porventura, estejam sendo processados e armazenados por prestadores de serviços localizados no Brasil ou no exterior, devendo adotar medidas administrativas que visem a sua integridade e inviolabilidade.

7.3.2 Informações e proteção aos clientes

A Greenn, em seu *website* disponibiliza os Termos de Uso e Política de Privacidade, pelos quais será possível verificar as condições gerais dos serviços disponíveis e de utilização da plataforma, além de informar as empresas terceiras que terão acesso aos dados pessoais, para fins de prestação dos serviços.

7.4 Segurança das Comunicações

Para garantir a segurança das Comunicações a Greenn deverá sempre:

- Utilizar conexões cifradas (TLS/HTTPS) ou aplicativos com criptografia fim - a fim para serviços de comunicação;
- Instalar e manter um sistema de firewall e/ou utilizar um *Web Application Firewall* (WAF – Filtro de Aplicação);
- Proteger e-mails via adoção de ferramentas *AntiSpam*, filtros de e-mail e integrar o antivírus ao sistema de e-mail;
- Remover quaisquer dados sensíveis e outros dados pessoais que estejam desnecessariamente disponibilizados em redes públicas.

7.5 Da contratação de serviços de processamento, armazenamento de dados e de computação em nuvem

A Greenn realizará avaliações prévias (*Due Diligence*) para efetivar a contratação de terceiros prestadores de serviços de processamento, armazenamento de dados e de computação em nuvem, seja no Brasil ou no exterior, de forma que as práticas de verificação a serem adotadas consideram a (i) criticidade do serviço, (ii) sensibilidade dos dados e informações a serem processados, armazenados e gerenciados, levando em conta ainda a classificação prevista nesta Política.

A Greenn poderá adotar as seguintes práticas:

- Necessidade de ter obtido e estar válida certificação de segurança da informação, tais como: PCI DSS e ISO 270001, dentre outras certificações aplicáveis;
- Pesquisa prévia utilizando banco de dados público ou privado;
- Solicitação de preenchimento de formulário e envio de documentos e informações;
- Visitas técnicas;
- Auditoria realizada por empresa externa independente especializada;
- Solicitação de contratação de seguro contra vazamento de dados;
- Previsão contratual de responsabilidade por incidente de dados pessoais ocasionados por sua culpa ou dolo;
- Realizar contrato de acordo de nível de serviço com o provedor de serviços em nuvem, contemplando a segurança dos dados armazenados;
- Avaliar se o serviço oferecido pelo provedor do serviço em nuvem atende os demais requisitos de segurança da informação estabelecidos;
- Analisar os requisitos para o acesso do usuário a cada serviço em nuvem utilizado;
- Utilizar técnicas de autenticação multi-fator para acesso aos serviços em nuvem relacionados a dados pessoais;
- O Contratado deverá cumprir com o Guia da ANPD de Segurança da Informação e os padrões PCI DSS se for de seu escopo.

Ainda, no momento de extinção contratual o prestador de serviços deverá:

- Transferir os dados ao novo prestador ou a Greenn;
- Confirmar a integridade e disponibilidade dos dados transferidos e, após isso, excluí-los de sua base.

7.6 Da Análise de Riscos

A execução, desenvolvimento e implementação de programas de análises de riscos são de responsabilidade do Gerente de Tecnologia da Informação. Espera-se que os Colaboradores que fazem parte do escopo PCI cooperem totalmente com qualquer análise conduzida em sistemas pelos quais são responsáveis. Espera-se também que os Colaboradores que fazem parte do escopo PCI trabalhem

conjuntamente no desenvolvimento de um plano de gestão de risco e remediação. Avaliações preliminares de risco serão sempre realizadas quando ocorrerem:

- Grandes Pedidos de Alteração.
- Grandes mudanças nos sistemas e redes responsáveis pelo transporte ou processamento de informações confidenciais ou restritas, incluindo novos equipamentos de rede, novos sistemas operacionais e novos servidores de correio.
- Novas interfaces para processadores de terceiros ou integradores de sistemas.

7.6.1 Processo de Avaliação de Risco

As análises de risco devem conter ao menos os seguintes componentes:

- Atribuir um nível de risco;
- Atribuir valores para probabilidade e impacto do evento negativo, conforme matriz previamente aprovada;
- Determinar qual nível de segurança existe no momento;
- Verificar possibilidade de Risco inerente;
- Estabelecer medidas complementares e realizar a gestão do risco.

O risco é definido como uma função da probabilidade de um evento negativo se concretizar e da magnitude da perda se ocorrer. Os seguintes níveis de risco são usados no processo de avaliação:

- Risco mínimo;
- Baixo risco;
- Risco moderado;
- Alto risco;
- Risco máximo.

Para mais detalhes, ver nosso Manual de Procedimentos de Avaliação Interna de Risco (AIR).

7.7 Controles e Processos de Segurança

Controles de Segurança são medidas ou contramedidas de segurança para evitar, impedir, detectar, neutralizar ou minimizar os riscos de segurança para

pessoas, propriedades físicas, informações, sistemas de computador ou outros ativos. Fazem parte da estratégia de segurança da Greenn, e são voltados para mitigar riscos e manter a conformidade com requisitos legais, normativos, contratuais e internamente desenvolvidos.

8 CAPACITAÇÃO DE COLABORADORES, PARCEIROS E TERCEIROS QUE FAZEM PARTE DO ESCOPO PCI

A equipe da Greenn manterá comunicação ativa e periódica sobre os termos desta Política, de modo que os Colaboradores, Parceiros e Terceiros que fazem parte do escopo PCI passarão periodicamente por capacitações, com objetivo de esclarecer a interpretação e aplicação desta Política, bem como serão informá-los sobre temas atrelados a esta Política.

Além disso, a equipe da Greenn será responsável por orientar os Colaboradores que fazem parte do escopo PCI para não desativar ou ignorar as configurações de segurança de estações de trabalho, realizar *backups offline*, periódicos e armazená-los de forma segura e inventariar e cifrar dados de dispositivos externos.

Os treinamentos devem conter no mínimo:

- Como utilizar controles de segurança dos sistemas de TI relacionados ao trabalho diário;
- Como evitar de se tornarem vítimas de incidentes de segurança corriqueiros, tais como contaminação por vírus ou ataques de *phishing*, que podem ocorrer, por exemplo, ao clicar em links recebidos na forma de *pop-up* de ofertas promocionais ou em links desconhecidos que chegam por e-mail;
- Manter documentos físicos que contenham dados pessoais dentro de gavetas, e não sobre as mesas;
- Não compartilhar logins e senhas de acesso das estações de trabalho;
- Bloquear os computadores quando se afastar das estações de trabalho, para evitar o acesso indevido de terceiros;
- Seguir as orientações da política de segurança da informação e segurança cibernética.

9 POLÍTICAS ESCOPO PCI DSS

Visando maior clareza, manutenção e aplicabilidade das políticas, foi necessário separar as políticas específicas do *framework* do PCI-DSS. Elas foram desenvolvidas de forma mais detalhada e específica, abrangendo áreas como segurança da informação em dados de cartão, gerenciamento de riscos direcionado, conformidade regulatória e diretrizes adequadas para cada requisito.

Essa abordagem não apenas promoverá melhor compreensão das diretrizes específicas, mas também facilitará a implementação eficaz das Políticas, fortalecendo a governança e a gestão eficiente dentro da organização, quais sejam, mas não se limitando a:

I. Criptografia;
II. *Antimalware*;
III. Monitoramento e Gestão de *Logs*;
IV. Proteção e Retenção de Dados de Cartão;
V. Administração de Dispositivos de Rede;
VI. Controles Criptográficos;
VII. Gestão de Acessos e Usuários;
VIII. Gerenciamento de Vulnerabilidades
IX. Segurança para Fornecedores e Terceirizados;
X. Tecnologias Críticas;
XI. Uso Aceitável para Tecnologia de Usuário Final.

10 VIGÊNCIA

A presente Política foi aprovada pela Diretoria Executiva, de forma que o presente documento entra em vigor em sua versão 1.1 em 08 de julho de 2024 e será revisado pelo menos uma vez a cada 12 meses e atualizada conforme necessário para refletir mudanças nos objetivos de negócios ou riscos ao ambiente.

Em caso de dúvidas acerca desta Política, entre em contato por meio do e-mail compliance@greenn.com.br.

11 INFORMAÇÕES DE CONTROLE

Elaboração	Everton Duarte, *Legal Operations Officer (LOO)*
Revisão	Valéria Medeiros, *Chief Compliance Officer* (CCO) Allan Godoy, *Chief Technology Officer* (CTO)
Aprovação	Rafael Wisch, *Chief Executive Officer* (CEO)

Identificação	POL-TI-001
Sigla	PSI

Classificação da Informação	Público
Área de aplicação	Brasil
Periodicidade de Revisão	Anual

Versão	Aprovação	Data	Alterações
1.0	Rafael Wisch *Chief Executive Officer (CEO)*	22/03/2023	Original.
1.1	Rafael Wisch *Chief Executive Officer (CEO)*	16/07/2024	Mudanças em todos os itens para atualização com as normas PCI DSS v.4.0.1.
1.2	Allan Godoy *Chief Technology Officer (CTO)*	06/01/2025	Modificação da área “Informações do declarante” no Anexo I; Acréscimo de Anexo II “Termo de Responsabilidade pela Guarda e Uso de Equipamentos”; Acréscimo Anexo III “Termo de Devolução de Equipamentos”.

ANEXO I

TERMO DE COMPROMISSO

POL-TI-001 Política de Segurança da Informação e Cibernética

DECLARO:

- Ter acesso, que li e entendi a Política de Segurança da Informação e Cibernética da Greenn;
- Ter conhecimento integral de todas as regras e procedimentos constantes na Política e normas vinculadas a esta;
- Estar ciente de minhas obrigações quanto à salvaguarda das informações e dados pessoais por mim acessadas em virtude de minhas atribuições profissionais na Greenn;
- Estar em concordância em cumprir as normas internas apresentadas, ciente de que o seu não cumprimento poderá acarretar a aplicação de sanções administrativas, civis e penais, na forma da Lei;
- Estar ciente de que não devo criar expectativa de privacidade em relação a minhas atividades no ambiente computacional corporativo e que meus acessos poderão ser registrados, auditados ou investigados pelo Compliance da Greenn, em caso de incidentes de segurança da informação;
- Reportar imediatamente a ocorrência de incidentes de segurança;
- Estar ciente que devo comunicar imediatamente à ao Compliance qualquer descumprimento da Política e normas de Segurança da Informação de que tenha ciência ou suspeita.

Informações do declarante:

Assinatura

ANEXO II

TERMO DE RESPONSABILIDADE PELA GUARDA E USO DE EQUIPAMENTOS

POL-TI-001 Política de Segurança da Informação e Cibernética

GREENN PAGAMENTOS E TECNOLOGIA LTDA, pessoa jurídica, inscrita no CNPJ 31.975.959/0001-76, com sede na Av. Brasil, nº 2379, Andar 2, Centro, Rondon – PR, CEP 87.800-000, neste ato representada por Danilo Macedo Paulo, *DevOps*, CPF 012.403.679-10, E-mail: danilo@greenn.com.br, doravante denominado simplesmente como "GREENN", e de outro lado;

NOME COMPLETO, inscrito no CPF sob o nº [número do CPF separado por ponto], residente e domiciliado à [endereço residencial completo com CEP]. ora em diante denominado "INTERESSADO".

Na data de assinatura deste instrumento, o GREENN entregou ao INTERESSADO, a título de empréstimo, para fins de desempenho de seus serviços, os equipamentos descritos:

Dispositivo	Marca	Modelo	Carregador	Número	Sistema operacional	Condições

Dessa forma, o INTERESSADO compromete-se a mantê-los em perfeito estado de conservação, ficando **CIENTE** de que:

1) Os equipamentos descritos acima, emprestados ao INTERESSADO, devem ser utilizados com a exclusiva finalidade de possibilitar a execução do contrato vigente e celebrado entre as partes na [data].

2) Se os equipamentos forem danificados ou inutilizados por mau uso, negligência ou extravio, é responsabilidade do INTERESSADO ressarcir o GREENN pelos danos causados, desde que comprovada culpa ou dolo do INTERESSADO.

3) Em caso de dano ou inutilização dos equipamentos o INTERESSADO deverá comunicar imediatamente ao GREENN.

4) O INTERESSADO se responsabiliza por qualquer dano causado a si, ao GREENN e a terceiros em razão da má utilização dos equipamentos, assim como pelas páginas acessadas, conversas participadas, entre outros, desde que comprovada culpa ou dolo do INTERESSADO nos mesmos termos do item 1 deste termo.

5) Ao realizar as atividades, o INTERESSADO se compromete a utilizar os equipamentos em rede de internet confiável, com garantia de segurança, independentemente da localização em que se encontrar, bem como utilizar mecanismos de proteção como antivírus, firewall, entre outros recursos que possam evitar quaisquer invasões e/ou danificações nos equipamentos que estão

sob sua responsabilidade. Ainda, se compromete em seguir com as recomendações da Política de Segurança da Informação, principalmente no que diz respeito às regras de uso de laptops.

6) O INTERESSADO poderá solicitar o uso de equipamentos da empresa fora das dependências, exclusivamente para fins de estudo e capacitação, mediante solicitação formal por e-mail. A solicitação deverá ser enviada para o departamento responsável e estará sujeita à análise e aprovação, considerando as necessidades operacionais e a disponibilidade do equipamento. Caso aprovada, o INTERESSADO se compromete a seguir todas as diretrizes de uso e guarda especificadas no presente termo, bem como a garantir a segurança e a integridade do equipamento durante o período em que estiver fora das dependências da empresa.

7) Terminando os serviços, no caso de rescisão da relação entre as partes, o INTERESSADO deverá devolver os equipamentos em perfeito estado de conservação, considerando-se o tempo de uso deles.

8) A tolerância de uma das partes para com a outra, relativamente ao descumprimento de qualquer uma das obrigações assumidas neste termo, será mera liberalidade, não implicando novação ou renúncia a qualquer direito. A parte tolerante poderá, a qualquer tempo, exigir da outra parte o fiel e cabal cumprimento de suas obrigações.

9) As Partes afirmam e declaram que o presente Termo poderá ser assinado por meio eletrônico, sendo consideradas válidas as referidas assinaturas feitas através da plataforma “Clicksign” (assinatura@greenn.com.br), quando enviadas para os endereços de e-mail citados nas suas qualificações do presente Instrumento, nos termos do Art. 10º §2º da MP 2200-2/2001 e da Lei nº 14.063/20.

E, por estarem cientes, assinam o presente instrumento em 02 (duas) vias, de igual teor e forma para um só fim, na presença das testemunhas abaixo arroladas, declarando anuência com o aqui exposto.

Rondon - PR, data da assinatura eletrônica.

Informações das Partes:

Assinatura Interessado	Assinatura Representante Grreenn

ANEXO III

TERMO DE DEVOLUÇÃO DE EQUIPAMENTOS

POL-TI-001 Política de Segurança da Informação e Cibernética

GREENN PAGAMENTOS E TECNOLOGIA LTDA, pessoa jurídica, inscrita no CNPJ 31.975.959/0001-76, com sede na Av. Brasil, nº 2379, Andar 2, Centro, Rondon – PR, CEP 87.800-000, neste ato representada por Danilo Macedo Paulo, *DevOps*, CPF 012.403.679-10, E-mail: danilo@greenn.com.br, doravante denominado simplesmente como "GREENN", e de outro lado;

NOME COMPLETO, inscrito no CPF sob o nº [número do CPF separado por ponto], residente e domiciliado à [endereço residencial completo com CEP], E-mail: [endereço eletrônico]. ora em diante denominado "INTERESSADO".

DECLARO que os equipamentos descritos neste termo foram devidamente devolvidos na [data].

COMPROMETO-ME a esclarecer eventuais dúvidas ou pendências relacionadas à devolução e compromisso com perfeito estado de conservação durante o período de uso.

Este termo está em entendimento com o **TERMO DE RESPONSABILIDADE PELA GUARDA E USO DE EQUIPAMENTOS**, previamente firmado.

Dispositivo	Marca	Modelo	Carregador	Número	Sistema operacional	Condições

Rondon - PR, data da assinatura eletrônica.

Informações das Partes:

Assinatura Interessado	Assinatura Representante Grreenn