POLÍTICA DE SEGURANÇA CIBERNÉTICA

Afinal, o que é Segurança Cibernética?

Trata-se de um conjunto de normas e diretrizes norteadoras, criadas para garantir a proteção e a manutenção da privacidade, a integridade, a disponibilidade e a confidencialidade das informações de sua propriedade e/ou sob sua guarda.

Queremos que você conheça o que a POSSO PARCELAR oferece e espera dos seus USUÁRIOS. A partir de então, criamos uma relação de confiança um no outro… abaixo você encontra os detalhes. 😉

POLÍTICA DE SEGURANÇA CIBERNÉTICA

1. OBJETIVO

1.1. A Política de Segurança Cibernética da POSSO PARCELAR visa garantir a proteção e a manutenção da privacidade, a integridade, a disponibilidade e a confidencialidade das informações de sua propriedade e/ou sob sua guarda, além atuar na prevenção, detecção e redução da vulnerabilidade de incidentes relativos ao ambiente cibernético, determinando as diretrizes que simbolizam, em nível estratégico, os princípios adotados para o alcance dos objetivos de segurança da informação.

1.2. Esta Política expõe o pacto da POSSO PARCELAR no zêlo e tratamento das informações de seus clientes, ao proporcionar plena satisfação quanto à segurança e privacidade de suas informações. Comprometemo-nos, ainda, com os aspectos regulatórios e legais que se associam à nossa atuação.

2. VIGÊNCIA

2.1. Esta Política é revisada anualmente, minimamente; ou quando necessário em casos de alteração nas normas e regulações, mudança de diretrizes de segurança ou modificação nas estratégias da POSSO PARCELAR.

3. PRINCÍPIO DE SEGURANÇA DA INFORMAÇÃO

3.1. Os ativos de informação são os bens mais importantes no mercado financeiro; portanto, comprometemo-nos com responsabilidade durante o seu tratamento. Neste sentido, fundamentamo-nos nos princípios de segurança da informação, cujos propósitos

fundamentam a conservação da propriedade da informação. Notadamente, zelamos pela confidencialidade, integridade e disponibilidade, assentindo ao uso e compartilhamento de forma controlada, monitorando e coibindo incidentes provenientes de ataques cibernéticos.

3.2. Princípio da Confidencialidade: garantimos que os dados tratados tenham intervenção limitada às pessoas especificamente autorizadas.

3.3. Princípio da Integridade: certificamos para que as informações sejam mantidas íntegras, sem modificações indevidas, sejam acidentais ou propositais.

3.4. Princípio da Disponibilidade: atestamos para que as informações estejam disponíveis ao acesso por todas as pessoas autorizadas.

4. INFORMAÇÕES CONFIDENCIAIS

4.1. O acesso às informações confidenciais coletadas e armazenadas pela POSSO PARCELAR, incluindo dados pessoais, é restrito aos profissionais autorizados ao uso direto dessas informações, é necessário à prestação de seus serviços, sendo limitado o uso para outras tarefas. Prezamos, ainda, pela privacidade das informações no âmbito da Lei Geral de Proteção de Dados (“LGPD”) e da Política de Privacidade. Poder-se-á revelar as informações confidenciais nas seguintes hipóteses:

4.1.1. Sempre que estiver obrigado a revelá-las, seja em virtude de dispositivo legal, ato de autoridade competente, ordem ou mandado judicial;

4.1.2. Mediante solicitação dos órgãos de proteção e defesa de crédito e prestadores de serviços autorizados a defender seus direitos e créditos;

4.1.3. Mediante solicitação dos órgãos reguladores do mercado financeiro; e/ou

4.1.4. Para outras instituições financeiras, desde que dentro dos parâmetros legais estabelecidos para tanto, podendo, nesta hipótese, o usuário, a qualquer tempo, cancelar sua autorização.

5. ESTRUTURA DE GERENCIAMENTO DE SEGURANÇA CIBERNÉTICA

5.1. A gestão de segurança objetiva assegurar que os procedimentos operacionais sejam desenvolvidos, implantados e mantidos ou modificados de acordo com os objetivos estabelecidos nesta Política.

5.2. Os acessos às informações são controlados, monitorados, restringidos e revistos periodicamente, sendo cancelados tempestivamente ao término do contrato de trabalho do colaborador ou do prestador de serviço.

5.3. As instalações e os equipamentos de processamento de informação crítica ou sensível são preservados em áreas seguras, com níveis de controle de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

5.4. Os colaboradores e terceiros prestadores de serviços são treinados constantemente através de um programa efetivo de conscientização e disseminação da cultura de segurança cibernética.

5.5. São constituídos controles e responsabilidades pela gestão e operação dos recursos de processamento das informações, visando garantir a segurança na infraestrutura tecnológica por meio de um gerenciamento efetivo no monitoramento, tratamento e na resposta aos incidentes, com o intuito de minimizar o risco de falhas e a administração segura de redes de comunicações.

5.5.1 Autenticação: o acesso às informações e aos ambientes tecnológicos devem ser permitidos apenas às pessoas autorizadas pelo titular da informação, levando em consideração o princípio do menor privilégio, a segregação de funções conflitantes e a classificação da informação.

5.5.2. O controle de acesso aos sistemas deve ser formalizado e contemplar, minimamente, os seguintes controles:

I. Utilização de identificadores individualizados (credencial de acesso), monitorados e passíveis de bloqueios e restrições (automatizados e manuais);

II. Remoção de autorizações dadas a usuários afastados ou desligados, ou que tenham mudado de função; e

III. Revisão periódica das autorizações concedidas.

5.5.3. Gestão de Incidentes de Segurança da Informação: o comportamento de possíveis ataques é identificado por meio de controles de detecção implantados no ambiente, como filtro de conteúdo, ferramenta de detecção de comportamentos maliciosos, Antivírus, Antispam, entre outros.

5.5.4. Prevenção a Vazamento de Informações: a utilização de controles para prevenção de perda de dados deve garantir que dados confidenciais não sejam

perdidos, roubados, mal utilizados ou disponibilizados na web por usuários não autorizados.

5.5.5. Testes de Intrusão: testes internos e externos nas camadas de rede e aplicação devem ser realizados anualmente, minimamente.

5.5.6. Varredura de Vulnerabilidades: as varreduras das redes internas e externas devem ser constantemente efetuadas. As vulnerabilidades descobertas devem ser sanadas e priorizadas de acordo com seu nível de criticidade.

5.5.7. Controle Contra Software Malicioso: todos os equipamentos que estejam conectados à rede corporativa, ou que façam uso de informações da POSSO PARCELAR, devem, sempre que compatível, ser protegidos com uma solução anti-malware determinada pela área de segurança da informação.

5.5.8. Criptografia: todo recurso de criptografia utilizado deve seguir as regras de segurança da informação e os padrões dos órgãos reguladores.

5.5.9. Rastreabilidade: auditorias devem ser implantadas para todos os componentes de sistema a fim de reconstruir e analisar os seguintes eventos:

I. Autenticação de usuários (tentativas válidas e inválidas);

II. Acesso a informações; e

III. Ações efetivadas pelos usuários, incluindo criações ou remoções do sistema.

5.5.10. Segmentação de Rede: computadores conectados à rede corporativa não devem ser acessíveis diretamente pela internet; não pode ser permitida a conexão direta de rede de terceiros, utilizando-se protocolos de controle remoto aos servidores conectados diretamente na rede corporativa; e para solicitação de criação, alteração e exclusão de regras nos firewalls e ativos de rede, o requisitante deve encaminhar pedido à área de segurança da informação, que fará a análise e aprovação, enviando para que seja executada pela área de tecnologia da informação.

5.5.11. Desenvolvimento Seguro: mantemos uma série de princípios para desenvolver sistemas de forma segura, certificando que a segurança cibernética seja projetada e implementada durante o ciclo de vida de desenvolvimento.

5.5.12. Cópias de Segurança (Backup): o procedimento de backup é realizado nos ativos de informação com periodicidade, a fim de evitar ou minimizar a perda de dados diante da ocorrência de incidentes.

5.6. O processo de continuidade de negócios é adotado visando reduzir os impactos e perdas de ativos da informação durante ou após um incidente crítico. Através do mapeamento de processos, análise de impacto e testes periódicos de recuperação de desastres, executa-se a continuidade de negócios; incluindo, ainda, a proteção dos serviços contratados na nuvem e os testes previstos para os cenários de ataques cibernéticos.

5.7. Conforme a Resolução BACEN n° 4.893/2021, corroborada pela Circular SUSEP n° 638/21 do Conselho Monetário Nacional, para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a POSSO PARCELAR se ampara em um procedimento efetivo para aquiescência às regras previstas na regulamentação em vigor.

6. PRINCIPAIS RECOMENDAÇÕES DE SEGURANÇA AOS CLIENTES E USUÁRIOS

6.1. O cliente é responsável pelo seu identificador (login / senha), que é único e acompanhado de senha exclusiva, pessoal e intransferível, para identificação e autenticação individual no acesso à informação e aos recursos de tecnologia. Recomendamos que o USUÁRIO:

6.1.1. Mantenha a confidencialidade, memorize e não registre a senha em lugar algum. Ou seja, não contar a ninguém e não anotar em papel;

6.1.2. Altere a senha sempre que suspeitar do comprometimento dela;

6.1.3. Elabore senhas de qualidade e complexidade que tornem difícil a adivinhação;

6.1.4. Impeça o uso do seu equipamento por outras pessoas, enquanto este estiver conectado/ “logado” com a sua identificação;

6.1.5. Bloqueie sempre o equipamento ao se ausentar; e

6.1.6. Sempre que possível, habilite um segundo fator de autenticação (SMS, Token ou outros).

6.2. Recomenda-se que o cliente mantenha uma solução de antivírus atualizada e instalada no computador utilizado para acesso aos serviços oferecidos pela POSSO PARCELAR. Além disso, sugere-se manter o sistema operacional atualizado.

6.3. A engenharia social, no contexto de segurança da informação, refere-se à técnica pela qual um indivíduo busca persuadir outro, abusando da ingenuidade ou confiança do usuário, objetivando ludibriar, aplicar golpes ou obter informações sigilosas.

6.3.1. Phishing: técnica utilizada por cibercriminosos para fraudar usuários por meio do envio de e-mails maliciosos, visando obter informações pessoais (senhas, número do cartão de crédito, CPF, número de contas bancárias, entre outros). As abordagens dos e-mails de phishing podem ocorrer das seguintes maneiras:

I. Atraem a atenção dos usuários pela possibilidade de obter alguma vantagem financeira, por curiosidade ou por caridade;

II. Simulam representar a comunicação oficial de instituições conhecidas como Bancos, Lojas de comércio eletrônico, entre outros sites populares;

III. Induzem os usuários a preencher formulários com os seus dados pessoais e/ou financeiros, ou até mesmo à instalação de softwares maliciosos que possuem o objetivo de coletar informações sensíveis;

6.3.2. Spam: tratam-se de e-mails não solicitados, que geralmente são enviados para muitas pessoas, tipicamente com fins publicitários. Além disso, os Spams estão diretamente conectados aos ataques de segurança, sendo eles um dos principais causadores da propagação de códigos maliciosos, da venda ilegal de produtos e da disseminação de golpes.

6.3.3. Falso Contato Telefônico: são técnicas utilizadas pelos golpistas para obter informações como dados pessoais, senhas, token, código de identificação do aparelho celular (IMEI) ou qualquer outro tipo de informação para a prática da fraude.

7. COMUNICAÇÃO

7.1. Quaisquer suspeitas de irregularidades no cumprimento das determinações desta Política serão alvo de averiguação interna e precisam ser comunicadas imediatamente aos nossos canais de atendimento e comunicação.

ENTRE EM CONTATO CONOSCO

Em caso de dúvidas sobre nossas práticas, ou caso deseje entrar em contato com a POSSO PARCELAR para atualizar ou corrigir qualquer uma de suas informações cadastradas, ou exercer seus direitos, nós estaremos disponíveis através do nosso endereço, telefone e chat disponíveis no site e do nosso e-mail contato@possoparcelar.com.br, por meio do nosso encarregado no tratamento de dados (DPO – Data Protection Officer).

Você entende e concorda que deve manter o seu cadastro na plataforma atualizado, com informações precisas de contato (tais como endereço de e-mail e telefone), para que possamos entrar em contato com você quando necessário e para enviar informações importantes sobre os produtos e serviços oferecidos.

Esta Política de Segurança Cibernética passa a ter validade a partir de sua publicação.

Atualizado em agosto de 2023.