ASSUNTO	PUBLICAÇÃO	NÚMERO-VERSÃO
Segurança Cibernética	**28/10/2022**	**0500-001**

1. Visão Geral

Este documento e seus anexos demonstram o compromisso do Pinbank e de sua Alta Administração em zelar e tratar as informações de seus clientes, de forma a proporcionar plena satisfação quanto à segurança e privacidade de suas informações. Demonstramos também o nosso compromisso com os aspectos regulatórios e estratégicos do Pinbank, estando assim, em conformidade com as principais regulamentações vigentes.

2. Objetivo

A Política de segurança cibernética do Pinbank visa garantir a proteção, a manutenção da privacidade, integridade, disponibilidade e confidencialidade das informações de sua propriedade e/ou sob sua guarda, além de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, definindo as regras que representam, em nível estratégico, os princípios fundamentais incorporados pelo Pinbank para o alcance dos objetivos de segurança da informação.

3. Escopo

Por integrar o instrumento normativo 00.01.02 – Política de Segurança da Informação do Pinbank, este documento tem a mesma abrangência contemplando todas as suas áreas de negócio, empresas que compõe o Conglomerado, escritórios e demais operações no que se refere a ocorrência de incidentes de segurança cibernética.

4. Vigência

Esta política tem vigência a partir da data de sua publicação (“Publicado em”) e vigorará por prazo indeterminado, devendo ser revisada anualmente ou sempre que necessário.

5. Aspectos Regulatórios e Normativos

Órgão Regulador	Número do Requerimento	Título
BACEN	Resolução nº 4983/21	Define sobre a Política de Segurança Cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.

PINBANK	00.01.02	Política de segurança da informação que define o Sistema de Gestão de Segurança da Informação (SGSI) do Pinbank. Onde é definida a abordagem organizacional usada para proteger a informação empresarial e seus critérios de confidencialidade, integridade, disponibilidade e autenticidade.

6. Conceituação

Ameaça – Qualquer causa potencial de um incidente indesejado que possa resultar em impacto nos objetivos do negócio. As ameaças podem ser internas ou externas, intencionais ou não intencionais.

Baselines – Requisitos, recomendações e melhores práticas de configurações de segurança da informação para os ativos.

Boas Práticas de Segurança da Informação – São consideradas boas práticas de segurança da informação as recomendações contidas em normas e instituições como: ISO/IEC 27001, ISO/IEC 31000, OWASP (www.owasp.org), NIST (www.nist.gov), ISACA (www.isaca.com.br), SANS (www.sans.org) e outras internacionalmente reconhecidas.

Colaborador – Entende-se como colaborador qualquer pessoa que trabalhe para o Pinbank, quer seja: funcionário com registro em carteira de trabalho, terceiro, estagiário, aprendiz ou trainee.

Controle – Qualquer recurso ou medida que assegure formas de tratamento de riscos, incluindo a redução, eliminação ou transferência. A implantação e manutenção adequada de controles materializa a segurança das informações. Podem ser interpretados como controles: políticas, processos, estruturas organizacionais, técnicas padrões, software, hardware e outros.

Gestor – Colaborador que exerce cargo de liderança, como: presidente, vice-presidente, diretor, gerente, coordenador, líder ou chefe de seção.

Informação – Qualquer conjunto organizado de dados que possua algum propósito e valor para o Pinbank, seus clientes, parceiros e colaboradores. A informação pode ser de propriedade da empresa, estar sob sua custódia ou sob custódia de terceiros.

Nuvem (Cloud) – infraestrutura, plataforma, aplicação ou serviço localizado na internet. A nuvem pode ser pública com acesso a todos, privada, com acesso restrito ou híbrido, com parte restrita e parte irrestrita.

Política de Segurança da Informação – Estrutura de documentos formada pela política, normas e padrões de segurança cibernética e segurança da informação.

Princípios de "Least Privilege" e "Need do Know" – Estes princípios devem reger a autorização de qualquer acesso a sistemas e informações. Segundo eles, deve ser concedido apenas o nível mínimo de acesso (Least Privilege) a quem realmente tenha a necessidade de acesso (Need to Know).

Recursos Críticos – Recursos essenciais para o funcionamento da operação do Pinbank e que possuem informações críticas ou sensíveis.

Risco – Qualquer evento que possa afetar a capacidade da companhia de atingir seus objetivos e sua estratégia de negócios ou conforme a ISO 31000, o efeito da incerteza nos objetivos.

Segurança Cibernética – Conjunto de tecnologias, processos e práticas projetados para proteger redes, computadores, sistemas e dados de ataques, danos ou acesso não autorizado. Também conhecida como Segurança de TI, visa proteger somente assuntos relacionados ao digital.

7. Papéis e Responsabilidades

7.1. Da Alta Administração

A Alta Administração deve prover comprometimento e apoio à aderência da política de segurança cibernética de acordo com os objetivos e estratégias do negócio do Pinbank.

7.2. Gerencia de segurança da informação e o Comitê de Segurança da Informação

A gerência de segurança da informação e o comitê de segurança da informação são responsáveis por elaborar, custodiar, manter e divulgar esta política, bem como assegurar que todos os assuntos relacionados com a segurança da informação e segurança cibernética sejam tratados de uma maneira consistente e efetiva.

7.3. Gestores

Todo gestor é responsável por assegurar o cumprimento da política pelos funcionários de sua área, atuando de forma coordenada com a gerência de segurança da informação, bem como assegurar que os contratos e serviços sob sua responsabilidade estejam aderentes à esta política e demais normais e procedimentos de segurança.

7.4. Colaboradores

Todo colaborador é responsável por proteger as informações da empresa e relatar qualquer situação que represente desvio ou violação da segurança destas, bem como atender as recomendações pertinentes, constantes nas normas e procedimentos de segurança da empresa.

É responsabilidade de cada colaborador tomar conhecimento de todo o conteúdo das políticas e normas vigentes disponíveis por meio da Intranet.

8. Disposições Gerais

Esta política será atualizada sempre que necessário, de modo a refletir as necessidades do Pinbank.

As alterações nesta política poderão ser feitas por determinação do comitê gestor de segurança da informação do Pinbank.

Anexo I – Aspectos da Segurança Cibernética

1. Visão geral

Consoante dispõe a Política de Segurança da informação, cada tema da segurança cibernética é tratado por uma política própria. Onde são detalhados todos os controles, processos e procedimentos a serem seguidos de acordo com o tema abordado.

2. Objetivo

Expor de forma clara e objetiva os aspectos gerais dos principais tópicos da segurança cibernética, bem como indicar o instrumento normativo que compõe a política de segurança da informação do Pinbank que detalha seus respectivos controles, processos e procedimentos de acordo com o tópico.

3. Disposições gerais

A informação é um ativo essencial para os negócios do Pinbank e sendo assim deve ser adequadamente protegida.

A segurança cibernética e da informação visa proteger as informações contra diversos tipos de ameaças, para minimizar a exposição da empresa a riscos, garantindo que as características fundamentais da informação sejam preservadas, sendo elas: confidencialidade, integridade, disponibilidade e conformidade.

O Pinbank alinhado com os objetivos e requisitos do negócio, estabelece na política de segurança da Informação, regras e direcionamentos a serem seguidos e aplicados a pessoas, processos e tecnologia, de forma a proteger as informações do Pinbank, de seus clientes, fornecedores e parceiros de negócios.

Seguir as diretrizes desta política, significa proteger a empresa contra o vazamento de informações, contra fraudes, zelar pela privacidade, garantir que sistemas e informações estejam disponíveis quando necessário e zelar pela proteção da imagem e das marcas do Pinbank.

4. Diretrizes para tratamento das informações

Toda informação deve ter regras claramente definidas pelo seu proprietário para proteção contra perda, alteração e acesso, seja ela armazenada em meio eletrônico (computador central, servidores de rede, microcomputadores, pen drive), em papel (correspondências, atas, relatórios, manuscritos etc.) ou outros meios.

Toda informação deve ter usuários explicitamente definidos (instituições, áreas, pessoas) e os tipos de direitos que cada um terá para acessá-la.

Toda informação deverá ter procedimentos para protegê-la do acesso de pessoas não autorizadas.

Toda informação que garanta a continuidade das atividades do Pinbank, deverá ter cópia de segurança em local físico distinto, devidamente protegido para essa finalidade ou outro meio eficiente para permitir sua pronta recuperação em caso de perda ou danos.

As informações contidas em material que se tornar disponível para descarte (papel, pendrives, cd, etc.) deverão ser destruídas ou mantidas em locais fechados, protegidas do acesso de pessoas não autorizadas.

Todo colaborador do Pinbank é responsável pela segurança da informação a que tem acesso.

Toda informação encontrada extraviada deverá ser, imediatamente, devolvida a sua origem.

Os equipamentos que contiverem informações dos integrantes do Pinabnk, somente poderão ser deslocados para outro destino que o previamente estabelecido, quando certificado de que as informações neles contidos estejam formatadas.

Os colaboradores não devem efetuar tentativas de obter acesso às informações que não lhe são permitidos, devendo solicitá-las ao respectivo proprietário da informação, pasta ou arquivo.

A elaboração das normas e procedimentos de acesso deverá levar em consideração os riscos do acesso e alteração não autorizados, divulgação indevida e indisponibilidade dos dados, que tem por consequência às fraudes, problemas legais, perdas de negócios, danos à imagem e dificuldade na recuperação da informação.

5. Objetivos e diretrizes para a classificação da informação

A classificação da Informação tem o objetivo de proporcionar ao usuário a possibilidade de analisar suas informações, facilitando a definição do seu nível de acesso e condições de armazenamento, considerando sua confidencialidade, integridade e disponibilidade.

Todas as informações devem ser classificadas.

Toda a informação deverá ser considerada sigilosa e de alto risco até que se tenha estabelecido sua classificação.

A proteção proporcionada à informação, tanto em termos de acesso quanto de conservação, deve estar de acordo com sua classificação.

Quando em um mesmo meio físico existirem informações classificadas de formas diferentes, deve-se adotar, para fins de segurança, a classificação mais restrita.

Sempre que forem efetuadas alterações significativas em um sistema informatizado, ou nas características de uma informação, deverá ser comunicado aos usuários com antecedência e efetuada uma revisão de classificação.

6. Conceitos de confidencialidade

Os tipos de informações podem ser:

- Informações Sigilosas: Informações extremamente restritas quanto a sua divulgação. São de alto valor por motivos estratégicos e/ou com grande possibilidade de provocar prejuízos, razão pela qual seu nível de proteção deve ser o mais alto possível;
- Informações Confidenciais: Informações de caráter setorial e para divulgação a um reduzido grupo de pessoas de uma área ou setor de atividade;
- Informações Internas: São aquelas que têm sua circulação restrita ao âmbito interno do Pinbank;
- Informações Públicas: São aquelas que circulam livremente, interna e externamente, em relação ao Pinbank e a seus parceiros comerciais não havendo interesse em controlar sua divulgação e acesso.

7. Conceitos de restrição ao acesso

As restrições ao acesso podem ser:

- Controlado: O acesso às informações sigilosas, confidenciais e internas, deverá ser determinado pelo comitê de segurança da informação, que estabelecerá as áreas, pessoas e o nível desse acesso;
- Não Controlado: As informações públicas não estarão sujeitas ao controle de acesso

8. Conceitos de níveis de acesso

Os níveis de acesso podem ser:

- Somente para consulta: Nível de acesso do usuário permite somente a leitura das informações.
- Consulta e alteração: Nível de acesso do usuário permite efetuar mudanças nas informações disponibilizadas, como inclusão de pareceres, informações complementares, valores, etc.

9. Conceitos de integridade e disponibilidade

A integridade e disponibilidade podem ser:

- De Alto Risco: Informações cuja indisponibilidade e/ou inexatidão poderão causar prejuízos à continuidade dos negócios.
- De Médio Risco: Informações que impõem ao negócio problemas de disponibilidade e dificuldade na recuperação. O proprietário da informação e os usuários aceitam a disponibilidade limitada e a existência de um determinado tempo para recuperação.
- De Baixo Risco: Informações cuja exatidão e acessibilidade apresentam pouco ou nenhum risco ao negócio. Os usuários aceitam eventuais indisponibilidades e longos períodos para recuperação das informações.

10. Administração de acesso de usuários

A área responsável pelo controle de acesso aos sistemas deverá manter procedimentos formais que contemplem desde o registro inicial para um novo usuário à administração de privilégios e senhas e o cancelamento de autorizações.

A área responsável pelo controle de acesso deverá prover a prevenção de acessos não autorizados.

Cada usuário deverá gravar os arquivos de sua competência em pasta própria, ficando assim, responsável pelo conteúdo de sua pasta.

Cada usuário terá acesso apenas ao seu núcleo de informações concernentes à sua alçada. Em caso de necessidade de informações que fogem da mesma, deverá ser autorizado pela gerência o acesso a tais informações.

Todos os acessos, alterações, exclusões, efetuados pelos usuários nos diretórios compartilhados será gravado em um Log para fins de auditoria.

11. Controle de acesso a computadores e rede

O controle de acesso deverá assegurar que os usuários de computadores, conectados à rede corporativa do Pinbank, não comprometam a segurança de qualquer sistema operacional ou produto. Para isso, deverá ser disponibilizado um servidor de controlador de domínio que garanta que o usuário não efetue alterações indevidas na estação de trabalho. Além disso, todos os computadores/notebooks devem estar com antivírus corporativo devidamente instalados.

A inserção de qualquer nova informação, realizada por meio de dispositivos removíveis só será liberada mediante autorização do gerente ou gestor do setor responsável. Antes de efetuar a liberação, deverá ser verificado se a estação de trabalho realmente possui antivírus instalado e atualizado.

O acesso a serviços computacionais deverá sempre ocorrer através de um procedimento seguro no qual o usuário conecta-se a um sistema de controle utilizando seu usuário e senha, devendo ser planejado para minimizar os riscos de acesso não autorizados.

O acesso às estações de trabalho de forma remota só deverá ocorrer mediante autorização do usuário da estação de trabalho.

O acesso ocorrerá através de programa adquirido e licenciado pela área de infraestrutura para atendimento/suporte aos colaboradores do Pinbank. Para isso, o setor de infraestrutura deverá instalar o programa cliente nas estações de trabalho de cada colaborador, proporcionando assim o acesso remoto seguro.

Redes Wi-Fi só serão permitidas com uma internet exclusiva para tal serviço.

12. Aspectos gerais da segurança física de computadores e de servidores

Todos os equipamentos deverão ser configurados conforme padrões estipulados pela política de segurança da informação do Pinbank, mais especificamente pelo setor de Infraestrutura, tanto para computadores, como para os servidores.

A estrutura para manter a segurança física dos equipamentos de rede e computadores, devem obedecer aos padrões de segurança gerais do Pinbank e adequar-se, no mínimo, às especificações dispostas nos instrumentos normativos relacionados.

Em relação ao centro de processamento de dados (CPD):

- A sala deve ser fechada com uso de chaves, ou outro controle de acesso, restringindo o acesso ao ambiente.
- A disposição dos cabos lógicos e de energia devem ser instalados em canaletas específicas para que não haja interferência na rede e deve ser adequada para que as pessoas possam transitar livremente.

13. Precauções Quanto a Disponibilização dos Equipamentos que Armazenam Dados e Informações

Quando os equipamentos que armazenam dados e informações forem descartados, devolvidos ao fabricante, enviados para manutenção ou doados para instituições e outras finalidades do tipo, as informações neles contidas devem ser destruídas antes de deixar as dependências do Pinbank.

É importante ressaltar que esse equipamento não é suficiente apenas apagar os dados. Deve-se executar um programa de formatação que realmente os destrua.

As manutenções dos equipamentos que armazenam dados e informações realizadas no próprio local, devem ser autorizadas pelo responsável da área a qual o equipamento pertence. Caso haja dúvidas quanto à manutenção, solicitar antecipadamente o acompanhamento de um colaborador do setor de infraestrutura do Pinbank.