Pincred
SOLUÇÕES FINANCEIRAS

POLÍTICA CIBERNÉTICA E DE SEGURANÇA DA INFORMAÇÃO

Sumário

Esta Política Cibernética e de Segurança da Informação tem caráter permanente. O conteúdo presente neste documento poderá ser modificado a qualquer momento de acordo com as necessidades vigentes. Os profissionais da Pintos S.A. – Crédito, Financiamento e Investimento e seus prestadores de serviço deverão, sempre que necessário, consultar a última versão disponível.

Esta Política Cibernética e de Segurança da Informação tem caráter permanente. O conteúdo presente neste documento poderá ser modificado a qualquer momento de acordo com as necessidades vigentes. Os profissionais da Pintos S.A. – Crédito, Financiamento e Investimento e seus prestadores de serviço deverão, sempre que necessário, consultar a última versão disponível.

1. OBJETIVO

A Pintos S.A. Crédito, Financiamento e Investimento estabelece a presente Política Cibernética e de Segurança da Informação com o objetivo de aplicar os princípios e diretrizes de proteção das informações consideradas sensíveis da instituição e de seus clientes.

A Diretoria compromete-se, por meio dessa Política, a oferecer os recursos necessários à melhoria contínua dos procedimentos relacionados à segurança cibernética e da Informação, mantendo, com o menor risco possível, um ambiente computacional seguro para a proteção de dados e informações sensíveis.

2. PÚBLICO-ALVO

Esta Política tem o caráter público e torna-se pública por meio do sítio da Pintos S.A. Crédito, Financiamento e Investimento.

3. RESPONSABILIDADES

A referida Política, as estratégias vinculadas e a execução de planos de revisão e melhorias do ambiente corporativo da Pintos S.A. Crédito, Financiamento e Investimento são de responsabilidade do Diretor de Riscos.

4. DIRETRIZES E OBJETIVOS GERAIS

1) As informações devem ser tratadas de forma ética e sigilosa e de acordo com regulamentação e legislação vigentes.
2) A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada.

Esta Política Cibernética e de Segurança da Informação tem caráter permanente. O conteúdo presente neste documento poderá ser modificado a qualquer momento de acordo com as necessidades vigentes. Os profissionais da Pintos S.A. – Crédito, Financiamento e Investimento e seus prestadores de serviço deverão, sempre que necessário, consultar a última versão disponível.

3) O acesso às informações deve ser feito mediante prévia autorização, e o acesso deverá ser realizado por meio de credencial única, pessoal, intransferível e identificável.
4) Quaisquer riscos às informações dos clientes da Pintos S.A. Crédito, Financiamento e Investimento devem ser comunicados diretamente à Diretoria de Riscos;
5) A Política é orientada como parte essencial e integrada aos processos de negócios, com o objetivo primordial da consecução dos objetivos e metas empresariais.
6) Como forma de reduzir as vulnerabilidades dos ativos de informação, a Pintos S.A. Crédito, Financiamento e Investimento adota procedimentos e controles baseados em autenticação, criptografia, prevenção e detecção de intrusão, prevenção de vazamento de informações, proteção contra software malicioso, mecanismos de rastreabilidade, controles de acesso e segmentação de rede de computadores e manutenção de cópias de segurança dos dados e das informações.
7) Prestadores de serviço, fornecedores e empresas conveniadas devem adotar procedimentos e controles compatíveis com os riscos envolvidos no manuseio de dados ou informações sensíveis, preservando, inclusive, a continuidade das operações e negócios do Banco.
8) As informações são devidamente classificadas de acordo com a confidencialidade e as proteções necessárias.
9) A Pintos S.A. Crédito, Financiamento e Investimento atua na disseminação da cultura de segurança cibernética, promovendo programas internos de capacitação e de prestação de informações a clientes e usuários, quanto ao uso de produtos e serviços.

Esta Política Cibernética e de Segurança da Informação tem caráter permanente. O conteúdo presente neste documento poderá ser modificado a qualquer momento de acordo com as necessidades vigentes. Os profissionais da Pintos S.A. – Crédito, Financiamento e Investimento e seus prestadores de serviço deverão, sempre que necessário, consultar a última versão disponível.

10) A efetividade da Política Cibernética e de Segurança da Informação é verificada por meio de avaliações independentes periódicas de auditoria interna e externa, incluindo órgãos de controle e reguladores.

5. SEGURANÇA CIBERNÉTICA

É responsabilidade da área de TI em conjunto com a área de Risco determinar as possíveis ameaças, definir e adotar medidas de proteção tais como a contratação de links seguros, serviços de gestão de conteúdo etc.

6. PROPRIEDADE INTELECTUAL

A propriedade intelectual é formada por bens imateriais, tais como: marcas, sinais distintivos, slogans publicitários, nomes de domínio, nomes empresariais, indicações geográficas, desenhos industriais, patentes de invenção e de modelo de utilidade, obras intelectuais (tais como obras literárias, artísticas e científicas, base de dados, fotografias, desenhos, ilustrações, projetos de arquitetura, obras musicais, obras audiovisuais, textos etc.), programas de computador e segredos empresariais (inclusive segredos de indústria e comércio). Quaisquer informações e propriedade intelectual que pertençam à Pintos S.A. Crédito, Financiamento e Investimento, ou por ele disponibilizadas, não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas, inferidas ou desenvolvidas pelo próprio colaborador em seu ambiente de trabalho.

7. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

Os colaboradores e prestadores de serviços diretamente contratados pela Pintos S.A. Crédito, Financiamento e Investimento devem aderir e praticar a Política Cibernética e de Segurança da Informação, comprometendo-se a agir de acordo

com as diretrizes descritas na mesma. Os contratos firmados com a Pintos S.A. Crédito, Financiamento e Investimento devem possuir cláusula que assegure a confidencialidade das informações protegidas por sigilo e pela legislação e regulamentação vigentes.

8. PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA CIBERNÉTICA

8.1. Equipe de Resposta a Incidentes

A Equipe de Resposta a Incidentes de Segurança Cibernética é formada por profissionais da Instituição com sólida experiência e, ocupantes de cargos de liderança: Diretora de Riscos, Gerente de TI e Compliance.

8.2. Identificação do Incidente

A identificação de um incidente ocorre a partir da detecção de anomalias ou violações aos parâmetros definidos na Política de Segurança Cibernética. A equipe deve estar apta a reconhecer sinais oriundos de sistemas de monitoramento, bem como relatos de usuários, terceiros ou quaisquer partes interessadas. Todo indício deve ser tratado com a devida diligência, considerando seu potencial de impacto.

8.3. Triagem do Incidente

Nesta fase, realiza-se uma análise preliminar para confirmar a existência do incidente, classificá-lo e determinar sua relevância para as operações institucionais. As evidências iniciais e possíveis danos devem ser registrados com precisão. A ação só será iniciada após validação técnica da ocorrência, evitando esforços indevidos sobre falsos positivos.

8.4. Análise do Incidente

Confirmado o incidente, a equipe procederá à investigação detalhada, com coleta e análise de logs, trilhas de auditoria, registros de rede, e outras evidências. A

identificação precisa dos ativos afetados: como endereços IP, MACs, nomes de hosts e switches. É fundamental para traçar a origem, o vetor e a extensão do incidente.

8.5. Categorização e Priorização do Incidente

Cada incidente será classificado com base no seu impacto operacional, no tempo de recuperação e na criticidade dos ativos envolvidos. Incidentes classificados como críticos devem ser reportados imediatamente ao Diretor de Riscos, que poderá escalar o evento e mobilizar recursos adicionais. Havendo indícios de envolvimento de dados pessoais, o Encarregado pelo Tratamento de Dados (DPO) será notificado e, se confirmada a violação, passará a integrar a equipe de resposta.

8.6. Mitigação do Incidente

A mitigação consiste em um ciclo estruturado:

(i) análise aprofundada do incidente,
(ii) pesquisa de soluções disponíveis,
(iii) execução de medidas de contenção,
(iv) comunicação com as partes interessadas,
(v) aplicação da solução definitiva ou paliativa, e
(vi) restauração do ambiente com segurança.

8.7. Contenção do Incidente

A contenção visa interromper o avanço do incidente e estabilizar os ativos afetados, ainda que temporariamente. O objetivo é proteger o ambiente até que a solução definitiva seja implementada.

Esta Política Cibernética e de Segurança da Informação tem caráter permanente. O conteúdo presente neste documento poderá ser modificado a qualquer momento de acordo com as necessidades vigentes. Os profissionais da Pintos S.A. – Crédito, Financiamento e Investimento e seus prestadores de serviço deverão, sempre que necessário, consultar a última versão disponível.

8.8. Identificação de Causa e Solução

Nesta etapa, busca-se eliminar a causa fundamental do incidente. A equipe poderá contar com o suporte das áreas impactadas para resolver falhas estruturais e garantir que a recuperação ocorra de forma ordenada. A restauração de sistemas críticos será priorizada e realizada com base em dados de backup seguros e atualizações pertinentes. Testes serão conduzidos para validar a integridade e a segurança do ambiente antes de sua liberação definitiva.

8.9. Resposta ao Incidente

Toda a resposta ao incidente deve ser rigorosamente documentada, contemplando:

- Descrição completa do incidente e sua origem;
- Forma de detecção (relato humano ou sistema automatizado);
- Etapas executadas pela equipe;
- Status e evolução do incidente durante o processo;
- Evidências coletadas;
- Classificação final do evento;
- Recomendações.

8.10. Ações Pós-Incidente

Após a contenção e recuperação, inicia-se a fase de análise crítica, onde são revisadas as causas do incidente, os pontos de falha e as oportunidades de melhoria nos controles existentes. A equipe deve elaborar um plano de ação contendo:

- Responsáveis designados;
- Prazos de execução;
- Entregas previstas;
- Medidas de curto e longo prazo.

As conclusões devem ser compartilhadas com as partes interessadas. O objetivo é promover resiliência institucional e prevenir a reincidência.

9. RELATÓRIO ANUAL

Anualmente, a instituição elaborará relatório sobre a implementação do Plano de Ação e de Resposta a Incidentes, tendo como data-base o dia 31 de dezembro de cada ano.

O relatório deverá ser apresentado ao conselho de administração ou, na sua inexistência, à diretoria da instituição até 31 de março do ano seguinte ao da data-base, devendo abordar:

- A efetividade da implementação das ações desenvolvidas pela instituição para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes desta política (Item 8);
- O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizadas na prevenção e na resposta a incidentes;
- Os incidentes relevantes relacionados com o ambiente cibernético, ocorridos no período;

- Os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes de segurança.

10. REVISÃO

A Política será revisada anualmente e sua aprovação caberá a Diretoria da Pintos S.A. Crédito, Financiamento e Investimento.

11. ÓRGÃO RESPONSÁVEL

O Diretor de Risco é responsável por manter e atualizar esta política.

12. APROVAÇÃO E REVISÃO DA POLÍTICA

A aprovação e atualização desta política é evidenciada através de ata de reunião de diretoria.

13. HISTÓRICOS DAS ALTERAÇÕES E REVISÕES

HISTÓRICO	Nº REVISÃO	ELABORAÇÃO	DATA DE APROVAÇÃO
Elaboração da Primeira Versão	1.0	10/2019	13/12/2019
Elaboração da Segunda Versão	2.0	11/2023	02/02/2024
Elaboração da Terceira Versão	3.0	02/2025	27/03/2025

Esta Política Cibernética e de Segurança da Informação tem caráter permanente. O conteúdo presente neste documento poderá ser modificado a qualquer momento de acordo com as necessidades vigentes. Os profissionais da Pintos S.A. – Crédito, Financiamento e Investimento e seus prestadores de serviço deverão, sempre que necessário, consultar a última versão disponível.