1. OBJETIVO

Estabelecer as diretrizes que compõem o programa de segurança da informação e riscos cibernéticos das empresas do Grupo, bem como definir os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil conforme definido na Resolução no. 4.658 do BACEN.

2. APLICAÇÃO / PÚBLICO

Todos os colaboradores de todas as empresas do Grupo, prestadores de serviços ou terceiros, por meio do contrato firmado com a empresa prestadora de serviço, devem seguir esta política, bem como qualquer pessoa que tenha contato com informações desta empresa.
Todas as Empresas do Grupo: Pernambucanas (operações de Varejo), fintech Pefisa e a incorporadora Alinc.

3. RESPONSABILIDADES

As políticas, estratégias e processos corporativos de Segurança da Cibernética são supervisionados pela Diretoria de Tecnologia da Informação e discutidos nos fóruns específicos das áreas de negócio, e nos diversos Comitês Executivos do Grupo.

4. REGRAS GERAIS

A Segurança Cibernética define regras e procedimentos para a preservação das propriedades da informação (confidencialidade, integridade e disponibilidade), permitindo seu uso e compartilhamento de forma controlada, bem como o monitoramento e tratamento de incidentes provenientes de ataques cibernéticos oriundos de malwares, técnicas de engenharia social, invasões, ataques de rede, fraudes externas, etc, que podem causar danos financeiros e de reputação consideráveis.
A proteção e privacidade de dados dos clientes refletem os valores de todas as empresas do Grupo e reafirmam o seu compromisso com a melhoria contínua da eficácia do processo de Proteção de Dados.

5. A GOVERNANÇA DA SEGURANÇA CIBERNÉTICA

A governança da segurança cibernética no Grupo está estabelecida sobre nove (09) disciplinas, que englobam os principais **processos** e controles, as **tecnologias** aplicadas ao negócio e a capacitação e conscientização das **pessoas** envolvidas, a saber:

5.1. Segurança em Operações - Proteção do Ambiente e Segurança Física e Lógica

São constituídos controles e responsabilidades pela gestão e operação dos recursos de processamento das informações que garantem a segurança na infraestrutura tecnológica de redes locais e internet, através de um gerenciamento efetivo no monitoramento, tratamento e respostas aos incidentes, para minimizar o risco de falhas e a administração segura de redes de comunicações, incluindo a gestão de serviços contratados de processamento e armazenamento de dados e informações em nuvem.

Destacam-se as principais práticas de gestão da Segurança em Operações nos tópicos mencionados abaixo, a saber:

- *Práticas Seguras de Operação, Desenvolvimento de Sistemas e Atualização de Software*
- *Configuração de Sistema e Critérios de Segurança para Acesso aos Sistemas*
- *Boas Práticas de Atualização de Software*
- *Conexão Remota*
- *Gestão de Antivírus, Firewalls, Equipamentos e Aplicativos*
- *Transmissão de Arquivos*

- *Gestão e Testes de Vulnerabilidade*
- *Controle de Criptografia*
- *Utilização de Ativos e Recursos de TI*
- *Controle de Mídias Removíveis*
- *Segurança da Comunicação*
- *Monitoramento dos Recursos de TI*

5.2. Gestão da Classificação e Retenção da Informação

O gerenciamento da classificação da informação é realizado de acordo com a confidencialidade e as proteções necessárias são realizadas nos seguintes níveis: **Restrita**, **Confidencial**, **Interna** e **Pública**.

Na política de Gestão da Classificação e Retenção da Informação são detalhados os seguintes tópicos: Classificação e Reclassificação da Informação, Armazenamento e Backup de Informações, Transmissão, Troca e Transporte de Informações e Impressão e Descarte.

5.3. Gestão de Acesso

Os acessos às informações são controlados, monitorados, restringidos à menor permissão e privilégios possíveis, sendo que os acessos são rastreáveis, a fim de garantir que todas as ações sejam passíveis de auditoria.

Na política de Gestão de Acesso estão detalhados critérios para: acesso a sistemas; dispositivos móveis; registos de acessos; credenciais de acesso; gerenciamento de privilégios; comunicação remota à rede; transferência de colaboradores e penalidades.

5.4. Gestão da Contratação de Serviços de Processamento e Armazenamento de Dados e de Computação em Nuvem

Os fornecedores de serviços devem comprovar uma boa prática de governança corporativa no fornecimento dos serviços, tendo uma adequada estrutura organizacional de atendimento, rituais de gestão dos níveis de serviços, matriz de responsabilidades entre as partes, processo de escalação, certificações comprovadas dos profissionais e robusta arquitetura técnica da solução detalhada, bem como apoiar na inclusão de cláusulas contratuais, que atendem aos requerimentos solicitados na Resolução no. 4.568 do Bacen.

5.5. Programa de Continuidade de Negócios e TI e Continuidade de Serviços de TI

O Programa de Continuidade de Negócios foi estabelecido para que a Empresa tenha capacidade de reagir em eventuais interrupções operacionais.

Em paralelo, os processos de continuidade de TI foram estruturados para alcançar o maior nível de disponibilidade possível do ambiente tecnológico, estando preparado para diversos cenários que possam impactar a continuidade dos negócios.

5.6. Gestão e Reporte de Incidentes de Segurança

Na política de Tratamento a Incidentes de Segurança da Informação são detalhadas as seguintes diretrizes, a saber: identificação, notificação e reporte de incidentes; classificação da gravidade de incidentes; critérios de respostas a incidentes; análise de causa raiz e lições aprendidas; testes e treinamento do plano; notificações automáticas de segurança e estratégia de recuperação de sistemas críticos.

5.7. Gerenciamento de Riscos de TI

A Pernambucanas possui um Comitê de Riscos, atuante, principalmente, na eficiência do processo de gerenciamento dos riscos inerentes às atividades, bem como na compreensão e no engajamento dos colaboradores de todas as unidades do Grupo em relação aos seus papéis e

responsabilidades profissionais. Esse Comitê conta com a participação da alta liderança da empresa.

5.8. Controles e Avaliação Independente da Auditoria

A efetividade das políticas do Grupo é verificada por meio de avaliações externas semestralmente e periodicamente por Auditoria Interna.

5.9. Conscientização e Treinamento de Segurança

O Grupo possui uma Universidade Digital estruturada com diversos processos de capacitação dos profissionais com relação a cursos técnicos, legislações e boas práticas em segurança cibernética.

6. COMUNICAÇÃO

Caso ocorram situações em desacordo com as políticas da empresa ou regulamentações vigentes, cabe aos colaboradores, fornecedores e prestadores de serviços, prontamente, alertar a área de Compliance, de forma pessoal ou por meio do nosso Canal de Ética, conforme informado abaixo.

- Website: https://www.linhaetica.com.br/etica/pernambucanas
- Telefone: 0800 941 5360

7. RESPONSABILIDADE E COMPROMETIMENTO DA ALTA LIDERANÇA

A alta liderança de todas as empresas do Grupo se compromete com a melhoria contínua dos procedimentos e controles relacionados nesta Política, os quais são pautas recorrentes em Comitês Executivos internos da empresa.

8. MONITORAMENTO CONTÍNUO

Existem uma série de políticas, que estão integradas e conectas a política de Segurança Cibernética detalhada neste documento, a saber: Segurança da Informação; Segurança em Operação; Tratamento de Incidentes de Segurança da Informação; Segurança da Comunicação; Continuidade de Negócios e TI; Gestão de Acessos e Gestão da Classificação da Informação.

Fim do Resumo da Política de Segurança Cibernética.