POLÍTICA CORPORATIVA DE SEGURANÇA CIBERNÉTICA

1. OBJETIVO

A Política de Segurança Cibernética é o documento que estabelece as diretrizes que compõem o programa de segurança da informação e riscos cibernéticos da Pernambucanas e suas empresas controladas, bem como definir os requisitos para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, proteger redes, computadores, sistemas e dados de ataques, danos ou acesso não autorizado.

As políticas de Segurança Cibernética estabelecem um conjunto de diretrizes que regulamentam os controles necessários e a conduta adequada para prevenir impactos negativos na gestão dos negócios, possibilitando a manutenção de um ambiente estável, confiável e íntegro.

2. ABRANGÊNCIA

Todos os colaboradores da Pernambucanas e suas empresas controladas, 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 os recursos de TI e telecomunicações que transmitem, processam ou armazenam dados da Pernambucanas.

3. CONTEXO SOBRE A SEGURANÇA CIBERNÉTICA

A Segurança Cibernética é o conjunto de práticas, políticas, conceitos de segurança, abordagens de gestão de risco, treinamentos e tecnologias utilizados para proteger o ambiente cibernético, a organização, a continuidade dos negócios e os dados dos clientes, funcionários, fornecedores ou parceiros de negócios da Pernambucanas e suas empresas controladas.

Para a Política de Segurança Cibernética da Pernambucanas e suas empresas controladas, utilizará os termos abaixo possuem as seguintes definições:

- Incidente de Segurança: pode ser definido como qualquer evento que explora alguma brecha/vulnerabilidade, de processos, de soluções, de produtos, sistemas, infraestrutura de TI, entre outros, onde o resultado pode:
- Causar danos à negócio e/ou aos colaboradores da Pernambucanas e suas empresas controladas e/ou clientes, ou;
- Afetar a habilidade da Pernambucanas e suas empresas controladas de entregar serviços apropriados aos clientes, ou;
- Resultar em roubo, fraude.
- Incidente Cibernético: Também conhecido como incidente de segurança cibernética, incidente de segurança de TI e / ou um incidente de segurança da informação é definido como: Uma ocorrência que compromete a confidencialidade, integridade e/ou a disponibilidade de um sistema e/ou as informações que o sistema processa, armazena ou transmite e que portanto constitui uma violação ou ameaça iminente à informação, assim como aos regulamentos internos como às políticas, procedimentos, padrões de segurança definidos pela Pernambucanas e suas empresas controladas. Destaca-se que informações armazenadas em meio físico é parte do escopo de proteção.
- Vulnerabilidades: quaisquer condições que, quando exploradas por uma pessoa desconhecida ou não vinculada a Pernambucanas e suas empresas controladas (mas pode ser um funcionário também) mal-intencionado, possam resultar em violações de segurança, tais como falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede, desatualização ou ausência de mecanismos de segurança cibernética. Um ataque de exploração de vulnerabilidades ocorre quando um atacante tenta executar ações maliciosas, como por exemplo invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar uma aplicação ou serviço indisponível.
- Confidencialidade: informação acessível somente para pessoas autorizadas.
- Integridade: propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças.
- Disponibilidade: acesso à informação e aos ativos correspondentes aos usuários autorizados sempre que necessário.
- Riscos Cibernéticos: Riscos de ataques cibernéticos, oriundos de malwares, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, desprotegendo dados, redes e sistemas da empresa causando danos financeiros e de reputação consideráveis.
- Malwares: Malware é a abreviação de "software malicioso" (em inglês, malicious software) e se refere a um tipo de programa de computador desenvolvido para infectar o computador de um usuário legítimo e prejudicá-lo através das seguintes formas:

a) Vírus: software que causa danos a máquina, rede, softwares e banco de dados;

b) Cavalo de Tróia: aparece dentro de outro software e cria uma porta para a invasão do computador;

c) Spyware: software malicioso para coletar e monitorar o uso de informações;

d) Ransomware: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido;

e) Engenharia Social: é termo utilizado para descrever um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações;

f) Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento;

g) Phishing: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
h) Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
i) Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;
j) Fraudes Externas e invasões: realização de operações por fraudadores, utilizando-se de ataques em contas bancárias, conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico;
k) Ataques DDoS e Botnets: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da Grupo; no caso dos Botnets, o ataque vem de muitos computadores infectados utilizados para criar e enviar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços;
l) Infraestrutura na Nuvem: de acordo com o NIST (National Institute of Standards and Technology), a computação em nuvem é definida como m modelo de serviços fornecido por terceiros que permite acesso, de modo conveniente e sob demanda, a um conjunto de recursos computacionais configuráveis e compartilhado (por exemplo, redes, servidores, armazenamento, aplicações e serviços) que podem ser rapidamente provisionados e liberados com o mínimo de esforço de gerenciamento ou interação com o provedor de serviços.
m) Exploits: são execuções de sequências de comandos, dados ou uma parte de um software elaborados por hackers que conseguem tirar proveito de um defeito ou vulnerabilidade. Os exploits fazem parte de um conjunto de malwares, ou softwares modificados, que tem o objetivo de invadir sistemas, roubar dados e danificar os programas. Na maioria das vezes, eles entram em ação no formato de programas com códigos e dados maliciosos e/ou danificados.

4. ESCOPO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

A Política de Segurança Cibernética da Pernambucanas e suas empresas controladas, é revisada periodicamente, abrange a confidencialidade, a integridade e a disponibilidade das informações, assim como promover a implantação de medidas preventivas, detectivas e corretivas, voltadas ao controle do ambiente cibernético, mitigação de potenciais incidentes de segurança cibernética e redução de vulnerabilidades.

5. DIRETRIZES BÁSICAS

Visamos atingir um alto padrão de Segurança da Informação. Por isso, a Pernambucanas é comprometido com a confidencialidade, integridade e disponibilidade de todos os ativos físicos e lógicos de informação da empresa, garantindo que os requisitos legais, operacionais e contratuais sejam cumpridos. A preocupação com a Segurança da Informação e Cibersegurança é comum aos diversos níveis de gestão e um compromisso individual de todos, garantindo assim a Identificação, Proteção, Detecção, Resposta e Recuperação de eventos e/ou incidentes de segurança.

Portanto, o cumprimento da Política Corporativa de Segurança Cibernética é de responsabilidade de todos os colaboradores e dos prestadores de serviços, os quais devem obedecer às seguintes diretrizes:

- Proteger as informações contra acesso, modificações, destruição ou divulgação não autorizada;
- Prover a adequada classificação da informação, sob os critérios de confidencialidade, disponibilidade e integridade;
- Assegurar que os recursos utilizados para o desempenho de sua função sejam utilizados apenas para as finalidades aprovadas pela Pernambucanas e suas empresas controladas;
- Garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos;
- Garantir a continuidade do processamento das informações críticas de negócios;
- Atender às leis que regulamentam as atividades de toda a Pernambucanas e suas empresas controladas e seu mercado de atuação;
- Selecionar os mecanismos de segurança da informação, balanceando fatores de riscos, tecnologia e custo.

5.1. Proteção de Dados dos Clientes

A proteção e privacidade de dados dos clientes refletem os valores da Pernambucanas e suas empresas controladas e reafirmam o seu compromisso com a melhoria contínua da eficácia do processo de proteção de dados.

Quanto às informações de nossos clientes, são obedecidas as seguintes determinações:

- São coletadas de forma legal, para propósitos específicos e devidamente informados;
- Somente são acessadas por pessoas autorizadas e capacitadas para o seu uso adequado;
- Poderão ser disponibilizadas a empresas contratadas para prestação de serviços, sendo exigido de tais organizações o cumprimento de nossas diretrizes de segurança e privacidade de dados;
- As informações constantes de nossos cadastros, bem como outras solicitações que venham garantir direitos legais ou contratuais, somente são fornecidas aos próprios interessados, mediante a solicitação formal, seguindo os requisitos legais vigentes.

5.2. Princípios

Os princípios da Política Corporativa de Segurança Cibernética são:

- Proteger a reputação da empresa;
- Garantir a confidencialidade, integridade e disponibilidade das informações da Pernambucanas e suas empresas controladas, e de informações de terceiros por ela custodiadas, contra acessos indevidos e modificações não autorizadas, assegurando ainda que as informações estarão disponíveis a todas as partes autorizadas, quando necessário;
- Identificar violações de Segurança Cibernética, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e lógicos, objetivando a mitigação dos riscos cibernéticos, dentre outros;
- Garantir a continuidade dos negócios, protegendo os processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos;
- Atender aos requisitos legais, regulamentares e às obrigações contratuais pertinentes a atividade da empresa;
- Gerenciar os incidentes referentes a Segurança Cibernética originados na Pernambucanas e suas empresas controladas, o controle e os tratamentos adotados nas empresas prestadoras de serviços a terceiros, que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da Pernambucanas e suas empresas controladas;
- Conscientizar, educar e treinar os colaboradores por meio de Política Corporativa de Segurança Cibernética, normas e procedimentos internos aplicáveis as suas atividades diárias;
- Estabelecer e melhorar continuamente um processo de Gestão de Riscos de Segurança Cibernética.

6. GOVERNANÇA DA SEGURANÇA CIBERNÉTICA

A governança da segurança cibernética da Pernambucanas e suas empresas controladas está estabelecida sobre nove (09) pilares, que englobam os principais processos e controles, as tecnologias aplicadas ao negócio e a capacitação e conscientização das pessoas envolvidas, a saber:

- Segurança em Operações - Proteção do Ambiente e Segurança Física e Lógica;
- Gestão da Classificação e Retenção da Informação;
- Gestão de Acesso;
- Gestão da Contratação de Serviços de Processamento e Armazenamento de Dados e de Computação em Nuvem;
- Plano de Continuidade de Negócios e TI e “Disaster Recovery”;
- Gestão e Reporte de Incidentes;
- Gerenciamento de Riscos de TI;
- Controles de Auditoria & Sanções por não Conformidade;
- Conscientização e Treinamento de Segurança.

6.1. 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.

Os equipamentos e instalações de processamento de informação críticas ou sensíveis são mantidos em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

6.2. Práticas Seguras para Desenvolvimento de Sistemas

Nenhum sistema, programa ou aplicativo deve ser desenvolvido diretamente no ambiente de Produção.

Durante e após a etapa de desenvolvimento devem ser realizados testes com os softwares antes de sua utilização em ambiente de produção. Softwares/Sistemas que processem, transmitam e armazenem dados de titulares de cartão (próprio ou externos a Pernambucanas e suas empresas controladas), assim como aqueles que estejam ligados diretamente a outros sistemas que tenham acesso a este tipo de informação, devem cumprir todos os requisitos aplicáveis da versão mais atual do Padrão de Segurança de Dados do Setor de Cartões de Pagamento (Payment Card Industry Data Security Standard – PCI DSS).

Os programas-fonte devem ser guardados em ambientes protegidos contra incidentes de origem física e contra acesso indevido. Sempre quando for adquirir um código, programa ou sistema que não for produzido pela Pernambucanas e suas empresas controladas, ou seja, de terceiros, OBRIGATORIAMENTE, deve ser homologado pela Diretoria de Tecnologia da Informação, bem como, a validação de licenciamento, indicando a forma adequada de uso, a propriedade do software e/ou código e o tempo de vigência de contrato, de acordo com a Lei de Direitos Autorais.

6.3. Práticas Seguras para Atualização de Software

Todos os patches de segurança críticos e pacotes de serviço identificados pela área de Segurança da Informação ou o administrador do sistema, devem estar instalados nos sistemas aplicáveis em até 90 (noventa) dias após a identificação da vulnerabilidade. Qualquer exceção deve ser previamente tratada, documentada e justificada para a área de Segurança da Informação.
Servidores que armazenam, processam ou possuam acesso aos dados de cartões de pagamento devem ter seus patches e correções instalados em um prazo máximo de 30 (trinta) dias.

A instalação do patch pode ser aplicada a equipamentos e sistemas menos críticos dentro de 90 (noventa) dias, quando aprovado pela área de Segurança da Informação e baseada em uma análise de risco anterior.

6.4. Configuração de Sistema e Critérios de Segurança para Acesso aos Sistemas

O processo de configuração de sistema prevê registro de configuração para todos os sistemas pelo implementador, procedimentos e instruções de trabalho para execução e recuperação do ambiente de desenvolvimento, como dados históricos, programas fontes e versões anteriores.

Todos os softwares desenvolvidos e implementados devem possuir um sistema de controle de acesso, com no mínimo um fator de autenticação (“aquilo que se sabe”, como usuário e senha, por exemplo).

Sistemas que representem um alto risco para a Segurança das Informações da Pernambucanas e suas empresas controladas devem contar com no mínimo dois fatores de autenticação diferentes. A saber, os fatores de autenticação possíveis são “aquilo que se sabe” (senhas, por exemplo), “aquilo que se possui” (token, por exemplo), e “aquilo que se é” (biometria). Além disso, eles devem ser submetidos a análise de segurança do código-fonte, assim como testes de invasão anualmente.
As telas que solicitem a digitação de usuários e senhas dos usuários devem utilizar protocolos seguros para transmitir essas informações do usuário ao servidor/sistema.

6.5. Conexão Remota

O acesso remoto aos recursos de TI é limitado apenas às necessidades efetivas do usuário (colaborador ou terceiro), que deve ser liberado somente após solicitação formal do usuário mediante aprovação pela área de Segurança da Informação, com definição do período e permissões de acesso.

Esta conexão remota é executada através da VPN (Virtual Private Network ou Rede Privada Virtual), que é uma conexão que permite acesso remoto aos sistemas internos de uma empresa mantendo seguro o tráfego de dados.

Colaboradores Terceiros e Empresas Parceiras só podem ter acesso remoto através de VPNs site-to-site.
Em caso de acesso a qualquer sistema remotamente, devem ser empregadas as tecnologias adequadas para garantir que o ambiente de rede não seja exposto a nenhum risco, observando:

- Tecnologias como SSH, VPN ou SSL v3.0 / TLS v1.2 ou superior devem ser empregadas para todo gerenciamento remoto;
- Todo acesso remoto à rede através de redes públicas, tais como a Internet, deve ser autenticado por um esquema de autenticação forte de dois fatores: o uso de uma senha como um dos fatores, e um token exclusivo ou certificado como segundo fator.

6.6. Gestão de Antivírus, Firewalls, Equipamentos e Aplicativos

Todos os servidores, estações de trabalho, notebooks ou dispositivos móveis que utilizarem sistemas operacionais no ambiente da Pernambucanas e suas empresas controladas devem estar configurados com software antivírus aprovado e homologado pela área de Segurança da Informação.

O software antivírus e os sistemas utilizados devem estar configurados para:

- Receber atualizações automáticas, inclusive atualização das assinaturas de vírus;
- Executar varreduras de acordo com período indicado pela área de Segurança da Informação e melhores práticas;
- Registrar eventos com vírus em uma solução central de registro;
- Não permitir que os usuários finais sejam capazes de configurar ou desabilitar o software.

A Diretoria de Tecnologia da Informação (DTI) é responsável pela divulgação de informações sobre vírus de computador. Qualquer outra informação desta natureza, enviada por outra entidade interna / externa ou colaboradores, deve ser comunicada ao DTI para análise e diagnóstico através do Service Desk e documentado no formulário “Notificação – Incidentes – Segurança-Informação”.

Todo meio de armazenamento e/ou processamento de informações deve ser verificado pelo software antivírus antes de ser acessado, assim como arquivos acessados através da internet e correio eletrônico.

Principais características que devem ser observadas para aplicativos em relação à Informação de Portadores de Cartão:

- Todos os aplicativos do Grupo relacionados ao processamento ou resgate de informações de portadores de cartão devem, onde não houver uma necessidade comercial para exibição de PAN completo, mascarar os números primários de conta (PAN), no máximo, os seis primeiros e os últimos quatro dígitos de PAN completo;
- Todos os aplicativos relacionados ao armazenamento de informações de portadores de cartão devem ser configurados de forma a não reter informações, tais como dados completos de tarjas magnéticas, códigos de validação de cartão, valores de cartão não presente, pins ou blocos de pins.

A área de Segurança da Informação deve:

- Aprovar todas as mudanças de hardware, software e regras de firewalls e roteadores sejam aprovadas pela área Segurança da Informação;
- Assegurar que as regras de segurança, aplicadas aos firewalls e roteadores, sejam suficientes para proteger as redes e ativos corporativos de ataques externos e de acesso não autorizado;
- Solicitar a equipe responsável a realização de revisões semestrais de todas as regras de firewall e roteadores expostos para a Internet e geração de relatórios, sendo que uma série de características relativas à segurança dos firewalls e roteadores são.

Firewall	Período
Revisão do conjunto de regras de firewall	Março / Setembro
Revisão de atualização de versão das caixas	Março / Setembro
Revisão de configurações de Firewall restringindo conexões entre redes e protocolos / portas não confiáveis	Março / Setembro
Lista dos usuários com liberação de acesso aos firewalls diretamente nas caixas	Março / Setembro
Revisão das configurações de todos os programas IDS/ IPS de acordo com as instruções do fornecedor	Março / Setembro

6.7. Gestão e Testes de Vulnerabilidade

A Gestão de Testes de Vulnerabilidades é uma atividade proativa e contínua para gerenciar a segurança de redes, buscando mitigar os riscos de falhas e exploits em códigos ou arquiteturas que possam comprometer endpoints ou ativos de rede, que utiliza diversas tecnologias e ferramentas para identificar riscos de Cyber Exposure em toda a Pernambucanas e suas empresas controladas, alinhá-los com seus objetivos operacionais e, então, corrigir essas vulnerabilidades em tempo hábil para proteger sua rede e suas operações.

Para a execução destes testes, a Gestão de Vulnerabilidades se baseia na adoção de práticas e processos de rotina, que visem diminuir as falhas e integrar esse trabalho à rotina da operação. Os testes de vulnerabilidades devem:

- Buscar por Vulnerabilidades: neste processo deve incluir varreduras periódicas de rede, logs de firewall, pentests ou uso de ferramentas automatizadas como um scan de vulnerabilidades das redes interna e externa;
- Identificar Vulnerabilidades: neste processo envolve a análise das varreduras de rede e pentests, essas análises podem encontrar anomalias que sugerem ataques de malware ou outras atividades maliciosas que tenham tomado vantagem sob uma vulnerabilidade;
- Verificar Vulnerabilidades: neste processo inclui verificar se as vulnerabilidades identificadas podem de fato ser exploradas em servidores, aplicações, redes e outros sistemas. Isso também inclui a classificação de severidade de uma vulnerabilidade e o nível de risco que ela apresenta à empresa;
- Mitigar as Vulnerabilidades: neste processo consiste em descobrir, de acordo com os recursos e limitações de sua empresa como prevenir essas vulnerabilidades de serem exploradas antes que um patch de correção esteja disponível, ou como aplicar o patch da forma mais rápida possível. Uma forma de contornar isso, por exemplo, é contar com uma solução de virtual patching no ambiente;
- Aplicação de Patches: é o processo para coletar os patches disponibilizados pelos fabricantes e aplicá-los em todos os sistemas presentes no ambiente em tempo hábil.

6.8. Transmissão de Arquivos

Definições aplicáveis a todos os tipos de transferência de arquivos:

- Toda transferência de arquivo deve ser realizada de forma segura, obrigatoriamente seguindo o padrão definido pelas áreas de Operação e Segurança da Informação da Diretoria de Tecnologia da Informação;
- É proibida qualquer outra forma de transferência de arquivos periódica com ambientes externos sem aprovação da área de Segurança da Informação;
- A disponibilização dos arquivos pelas empresas parceiras deve ser realizada em horário que permita o seu processamento dentro da janela de execução de processos batch;
- Toda criação de arquivos por processos batch no ambiente Unix ou disponibilizados por empresas parceiras, deve seguir o padrão de nomes de arquivos utilizados pela Pernambucanas e suas empresas controladas, de acordo com os padrões estabelecidos e homologadas pelas áreas de Segurança da Informação e Operações de TI.

6.9. Controle de Criptografia

O acesso à chave de encriptação é concedido somente àqueles que necessitarem especificamente ter acesso em decorrência de sua função.

As informações de portadores de cartão em mídia removível devem ser encriptados onde quer que sejam armazenados (encriptação de disco geralmente não pode encriptar mídia removível).

As redes sem fio que transmitam informações de portadores de cartão ou que estejam conectadas ao ambiente de informações de portadores de cartão, utilizam as melhores práticas da indústria.

6.10. Utilização de Ativos e Recursos de TI

Todos os equipamentos em posse dos colaboradores devem ser relacionados pela Diretoria de Tecnologia da Informação. Em caso de desligamento de colaboradores, todos os equipamentos que pertencem a Pernambucanas e suas empresas controladas devem ser devolvidos.

É proibido o uso de recursos TI da empresa para fins não profissionais ou de forma diversa da especificada pela DTI.

6.11. Banco de Dados

Os acessos dos usuários aos bancos de dados são controlados pela Diretoria de Tecnologia da Informação. Esse acesso deve estar restrito aos administradores e aos “DBAs” (administradores de banco de dados).

Os prestadores de serviços que acessam o ambiente da Pernambucanas e suas empresas controladas são responsáveis pela segurança dos dados do portador do cartão que possuírem, ou que os armazenam, processam ou transmitem em nome da Pernambucanas e suas empresas controladas.

6.12. Controle de Mídias Removíveis

Não é permitido nos ambientes da Pernambucanas e suas empresas controladas, o uso de mídias removíveis como drives USB, CD-R, DVD, discos rígidos, fitas, etc.

A área Segurança da Informação é responsável pela liberação e pelo controle de acesso a mídias removíveis. Ressaltamos que toda mídia removível que contém dados e informações confidenciais para o negócio, deve ser claramente identificada de acordo com a Política de Classificação da Informação.

Para minimizar os riscos e atender os usuários que necessitem da liberação do acesso, dado a necessidade do negócio, exceções a esta política somente serão permitidas se aprovadas formalmente pela área de Segurança da Informação, conforme diretrizes específicas.

6.13. Segurança da Comunicação

A Segurança da Comunicação estabelece as diretrizes necessárias para garantir a segurança e proteção das informações durante a utilização de recursos, ferramentas e mecanismos de comunicação para garantir o uso adequado dos meios de comunicação disponibilizados.

Define as regras para a segurança de comunicação durante a utilização de recursos e canais de comunicação autorizados para toda a Pernambucanas e suas empresas controladas.

- Internet;
- Microsoft OneDrive (repositório de dados homologado e disponibilizado pela Pernambucanas e suas empresas controladas);
- Download/Upload;
- Correio Eletrônico (e-Mail);
- Mensagens Instantâneas;
- Relação com Terceiros.

6.14. Monitoramento dos Recursos de TI

O monitoramento da TI é o processo contínuo de acompanhamento das atividades operadas pela infraestrutura de TI, permitindo a identificação imediata de inatividade inesperada, invasão de rede e saturação de recursos.

Este monitoramento é realizado pelos Softwares:

- Monitoramento de integridade de arquivos (FIM - File Integrity Monitoring & SIEM - Security Information and Event Management).
- Monitoração Contínua de Ameaças”, realizado por um prestador de serviços, que possui o escopo básico prover uma visão geral sobre o cenário de ameaças digitais à qual está sujeita.

7. GESTÃO DA CLASSIFICAÇÃO E RETENÇÃO DA INFORMAÇÃO

A Companhia possui uma política denominada Gestão da Classificação da Informação, que está baseada nas normas ABNT NBR ISO/IEC 27001:2013 - Código de prática para a gestão de segurança da informação, e PCI-DSS – Payment Card Industry Data Security Standard – Requirement sand Security Assessment Procedures. O gerenciamento da classificação da informação e acordo com a confidencialidade e as proteções necessárias são realizadas nos seguintes níveis: Restrita, Confidencial, Interna e Pública.

A disciplina Gestão da Classificação e Retenção da Informação é categorizada conforme os itens abaixo:

- Classificação da Informação;
- Reclassificação da Informação;
- Armazenamento e Backup de Informações;
- Transmissão, Troca e Transporte de Informações;
- Impressão e Descarte.

8. GESTÃO DE ACESSO

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

Os processos citados abaixo foram estruturados na política de gestão de acesso:

- Acesso a Sistemas;
- Dispositivos Móveis;
- Registros de Acessos;
- Credenciais de Acesso;
- Gerenciamento de Privilégios;
- Comunicação Remota à Rede;
- Transferência de Colaboradores;
- Penalidades.

9. GESTÃO DA CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

Os critérios a seguir são acordados entre as partes através de instrumento contratual. Os fornecedores de serviços devem comprovar uma prática de governança corporativa e de gestão que considere no mínimo os seguintes pontos:

- Estrutura organizacional do fornecedor que suporte a gestão do contrato, gestão dos serviços e gestão técnica da entrega;
- Rituais de gestão dos níveis de serviços diários, semanais e mensais;
- Matriz de Responsabilidades, indicando as áreas da Companhia e do Fornecedor envolvidos no serviço;
- Processo de escala formalizado e operante entre a Companhia e o Fornecedor, e procedimentos de “Call” de Crise para incidentes críticos;
- Processo de certificações das tecnologias envolvidas nos serviços.

Os fornecedores de serviços, em conjunto com a Diretoria de Tecnologia da Informação da Companhia devem garantir a capacidade da execução dos serviços através de:

- Cumprimento do processo de credenciamento do fornecedor, coletando a documentação que comprove o cumprimento da legislação e da regulamentação em vigor para execução dos serviços;
- Estabelecimento de processo e documentos que garantam a entrada e a saída de profissionais de gestores e técnicos da Companhia na instalação do fornecedor, garantido o acesso aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;
- Arquitetura técnica detalhada no anexo de contrato com recursos tecnológicos que garantam a confidencialidade, integridade, disponibilidade e a recuperação dos dados e das informações processadas ou armazenadas pelo prestador de serviço.
- Detalhamento em anexo do contrato, que garanta a aderência do fornecedor as certificações exigidas pela Companhia para a prestação do serviço a ser contratado.

a) Detalhamento em cláusula que garanta o acesso da Companhia aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;

b) Detalhamento em cláusula de ferramenta de monitoração, que permita provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

c) Detalhamento em cláusula com a indicação dos países e das regiões em cada país onde os serviços serão prestados e os dados que poderão ser armazenados. Em caso de contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior, deve ser incluído na cláusula contratual detalhes do convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados;

A contratação e alterações de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem será previamente comunicada ao Banco Central do Brasil, sessenta (60) dias antes da contratação dos serviços através do fornecimento das seguintes informações:

- A denominação da empresa a ser contratada;
- Os serviços relevantes a serem contratados;
- A indicação dos países e das regiões em cada país conforme indicado acima.

10. PROGRAMA DE CONTINUIDADE DE NEGÓCIOS E TI E “DISASTER RECOVERY”

O Programa de Continuidade de Negócios refere-se à capacidade de uma empresa continuar operando durante ou após uma interrupção inesperada. As interrupções incluem eventos como a perda de energia em um data center, a perda de dados como resultado da falha de um disco ou um ataque cibernético tornando os servidores temporariamente indisponíveis.

O “Disaster Recovery” é o processo de restaurar dados e sistemas para um estado operacional normal após uma interrupção. Requer ferramentas de software, infraestrutura de hardware e equipe técnica. Os backups de dados de rotina são essenciais para a recuperação eficiente de desastres, assim como a implementação dos processos e da infraestrutura corretos para restaurar os dados após um desastre.

10.1. Programa de Continuidade de Negócios

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

Para a execução do Programa de Continuidade de Negócio são detalhadas as seguintes etapas:

- Análise de Impacto no Negócio (BIA);
- Análise de Riscos Físicos;
- Definição de Cenários de Indisponibilidade;
- Plano de Contingência Operacional;
- Plano de Recuperação de Desastre;
- Calendário de teste de Contingência;
- Execução do resultado do teste de Contingência;
- Relatório do resultado do teste de Contingência;
- Disseminação do Programa de Continuidade de Negócios.

As referências utilizadas para o estabelecimento e execução do programa de continuidade de negócios e Disaster Recovery são:

- Norma ISO 22301/BS;
- Norma de gestão de continuidade de negócios (22301 substituiu a 15999-2);
- Práticas profissionais para continuidade de negócios pelo DRII (Disaster Recovery Institute International) – Instituto Internacional de Recuperação de Desastre;
- Práticas profissionais para continuidade de negócios pelo BCI (Business Continuity Institute) – Instituto de Continuidade de Negócios.

10.2. Programa de Continuidade de TI

O Programa de Continuidade de TI foi estruturado para alcançar o maior nível de disponibilidade possível do ambiente tecnológico, estando preparado para diversos cenários que possam impactar a continuidade dos negócios.

A Companhia mantém uma estrutura de Datacenter Primário e Datacenter Secundário em geografias distintas, e o exige em seus contratos de prestação de serviços.

11. GESTÃO E REPORTE DE INCIDENTES DE SEGURANÇA

Incidente de segurança da informação é qualquer evento relacionado a sistemas de informação que prejudique a confidencialidade, integridade ou disponibilidade das informações. Todos os processos envolvidos na gestão de incidentes, desde a detecção até a resposta, asseguram a existência de logs e documentação adequados que permitem melhores evidências forenses e conteúdo para auditoria. A documentação é armazenada em conformidade com as legislações e com a devida preservação de dados pessoais e sigilosos envolvidos.

Na política de Tratamento a Incidentes de Segurança da Informação são detalhadas as seguintes diretrizes:

- Identificação de Incidentes;
- Procedimento de Notificação e Reporte de Incidente;
- Classificação da Gravidade do Incidente;
- Resposta a Incidentes segregadas em:

a) Resposta Típica;
b) Comprometimento de Cartões de Crédito – Resposta Especial

- Análise de Causa Raiz e Lições Aprendidas;
- Testes e Treinamento do Plano;
- Notificações Automáticas de Segurança do Sistema;
- Estratégia de Recuperação de Sistemas Críticos.

12. GERENCIAMENTO DE RISCOS DE TI

A Pernambucanas e suas empresas controladas possui um Comitê de Gestão de Riscos atuante e embasado, principalmente, na compreensão e no engajamento dos colaboradores da empresa, de seus papéis e responsabilidades profissionais, na eficiência do processo de gerenciamento dos riscos inerentes às atividades à luz das diretrizes da alta administração.

Principais tipos de riscos operacionais gerenciados pela Pernambucanas e suas empresas controladas:

- Fraude Interna/Externa;
- Interrupção das Atividades da Grupo;
- Falha na Execução, Entrega ou Gestão das Atividades de Negócio;
- Práticas Trabalhistas e Ambiente de Trabalho Seguro;
- Clientes, Produtos e Práticas de Negócios Indevidas;
- Desastre;
- Falha na Infraestrutura e nos Sistemas de TI – Tecnologia da Informação.

Para todos os tópicos acima a Pernambucanas e suas empresas controladas, mantém os procedimentos, os controles internos, a avaliação de riscos, os planos de ações para a efetiva mitigação de riscos.

13. CONTROLES E AVALIAÇÃO INDEPENDENTE DA AUDITORIA

A efetividade das políticas da Pernambucanas e suas empresas controladas, são verificadas por meio de avaliações externas semestralmente, e periodicamente por Auditoria Interna.

14. CONSCIENTIZAÇÃO E TREINAMENTO DE SEGURANÇA

A Pernambucanas e suas empresas controladas, possui uma Universidade Digital estruturada com:

- Grade de treinamento em cursos técnicos, legislações e boas práticas;
- Execução do Treinamento em Apps (smartphones);
- Execução dos respectivos exames sobre a matéria do curso em Apps (Smartphones);
- Guarda em repositórios do exame que comprova a capacitação dos profissionais.

15. COMUNICAÇÃO

A Pernambucanas e suas empresas controladas dispõem de um Canal de Ética independente, administrado por uma empresa especializada, que possui a experiência necessária para obter informações em situações como má conduta, fraude e desvios de recursos, tanto no que se refere a esta política quanto em relação a quaisquer outras.

Todos aqueles que identificarem qualquer inconformidade diante das diretrizes estabelecidas nesta política ou não condizentes com o Código de Conduta Ética da empresa poderão relatar ao Canal de Ética, não sendo necessário identificar-se e serão tratadas com imparcialidade, sigilo e confidencialidade.

Caso ocorram situações que possam caracterizar conflito de interesses ou que estejam em desacordo com as determinações desta política, cabe àquele que identificar tal situação, prontamente, alertar a área de Compliance, de forma pessoal ou por meio do Canal de Ética, através dos seguintes meios:

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

16. RESPONSABILIDADE E COMPROMETIMENTO DA ALTA ADMINISTRAÇÃO

A Alta Administração da Pernambucanas e suas empresas controladas se compromete com a melhoria contínua dos procedimentos e controles relacionados nesta Política, os quais são pautas recorrentes em Comitês internos da empresa. Os atuais Comitês da Pernambucanas e suas empresas controladas são:

- COMEX;
- Comitê de Conformidade;
- Comitê Pefisa / Gestão de Riscos Comitê de Gestão de Riscos Comitê de 'Profit Sharing';
- Comitê Digital;
- Comitê Segurança da Informação;
- CTC - Comitê Tático Comercial;
- RD - Reunião de Diretoria;

17. MONITORAMENTO CONTÍNUO

As políticas abaixo na Pernambucanas e suas empresas controladas, estão integradas e conectas à política de segurança cibernética detalhada neste documento:

- Política Geral de Segurança da Informação;
- Política de Segurança em Operações;
- Política de Tratamento a Incidentes de Segurança da Informação;
- Política de Segurança da Comunicação;
- Política de Programa de Continuidade de Negócios;
- Política de Continuidade de Serviços de TI;
- Política de Gestão dos Acessos;
- Política de Gestão da Classificação da Informação.

18. DOCUMENTO (S) DE REFERÊNCIA

- ABNT NBR ISO/IEC 27001:2013 – Norma Brasileira - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos;
- ABNT NBR ISO/IEC 27002:2013 – Norma Brasileira - Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação;
- NIST Cyber Security Framework - framework de segurança cibernética NIST, fornece uma estrutura, com base nos padrões, diretrizes e práticas existentes para organizações do setor privado nos Estados Unidos, a fim de gerenciar e reduzir melhor o risco de segurança cibernética.