| Código | Documento | Data | Revisão | Páginas |
|---|---|---|---|---|
| PC018 | Segurança Cibernética (Cibersecurity) | 18/05/2020 | | 08 |

# ÍNDICE

# PARTE I - IDENTIFICAÇÃO

## 1. OBJETIVO

Esta política visa atender os requisitos da Resolução nº 4.658/2018 e Circular 3.909/2018, que dispõe sobre a política de segurança cibernética a ser observada pelas Instituições Financeiras e demais Instituições autorizadas a funcionar pelo Banco Central do Brasil.

## 2. ABRANGÊNCIA

A segurança cibernética inclui dispositivos de computação conectados, infraestrutura, aplicativos, serviços, sistemas de telecomunicações e a totalidade de informação transmitida e/ou armazenada no ambiente cibernético.

## 3. APROVAÇÃO

**Tecnologia** – responsável pela manutenção desta política.

**Compliance & Controles Internos** – responsável pela revisão desta política.

**Conselho de Administração – r**esponsável pela aprovação desta política.

## 4. GLOSSÁRIO

**Intrusão:** Ações realizadas com intuito de comprometer a estrutura básica da segurança de informação de um sistema informatizado, afetando sua integridade, confidencialidade e disponibilidade.

**Detecção de intrusão:** Processo de monitoramento e análise de logs/eventos que ocorrem em um ambiente de computadores ou em uma rede de dados, para que se possa realizar análises em busca de indícios de incidentes ilegal (intrusão).

**Espaço cibernético:** Ciberespaço é considerado como a metáfora que descreve o espaço não físico criado por redes de computadores, notadamente a Internet, em que as pessoas podem se comunicar de diferentes maneiras, como mensagens eletrônicas, salas de bate-papo, grupos de discussão, dentre outros.

**Segurança cibernética:** Mecanismos que visam assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no espaço cibernético, seus ativos de informação e suas infraestruturas críticas.

- **Ativos de informação:** Os meios de armazenamento, transmissão e processamento da informação, os sistemas de informação, bem como os locais em que se encontram esses meios, e as pessoas que a eles têm acesso.

- **AWS** – Amazon Web Services.

# 5. REVISÃO

- 18/05/2020 – Versão Original.

# PARTE II – DESCRITIVO

# 1. INTRODUÇÃO

Com o aumento exponencial das ameaças cibernéticas nos últimos anos, tanto em volume quanto em sofisticação, torna-se obrigação das empresas dispender atenção para a segurança cibernética a fim de verificar se suas estruturas estão preparadas para identificar e mitigar riscos cibernéticos, assim como para se recuperar de possíveis incidentes.

O Fitbank opera o seu ambiente de produção na nuvem - cloud - da Amazon Web Services™ (AWS), através de serviços flexíveis que permitem criar e distribuir soluções rapidamente e com mais segurança, usando as melhores práticas da AWS. Desta forma, simplifica-se o provisionamento e o gerenciamento: da infraestrutura, da implantação do código, da automatização de processos, do lançamento e atualização da plataforma e, do monitoramento de desempenho das aplicações.

## 1.1. O Risco Cibernético

- Conforme Resolução nº 4.658/2018, para mitigação do risco à ataques cibernéticos e consequentemente redução de ameaças à confidencialidade, integridade e disponibilidade dos dados ou dos sistemas, a empresa deve adotar algumas medidas, tais como:

I. **Identificação/avaliação de riscos (risk assessment)** – identificar os riscos internos e externos, os ativos de hardware e software e processos que precisam de proteção;

II. **Ações de prevenção e proteção** – estabelecer um conjunto de medidas cujo objetivo é mitigar e minimizar a concretização dos riscos identificados no item anterior, ou seja, buscar impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles;

III. **Monitoramento e testes** – detectar as ameaças em tempo hábil, reforçando os controles, caso necessário e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados;

IV. **Criação do plano de resposta** – ter um plano de ação, tratamento e recuperação de incidentes, incluindo um plano de comunicação interna e externa, caso necessário. Tal plano deve estar alinhado com a Política de Continuidade de Negócio, a qual aborda como deve se dar a comunicação interna e externa e por quais colaboradores, bem como o estabelecimento de um Comitê de Crise;

V. **Reciclagem e revisão** – manter o programa de segurança cibernética continuamente atualizado, identificando novos riscos e reavaliando os riscos residuais;

VI. **Capacitação** - fornecer treinamento para os colaboradores para que estejam cientes do que significa ataque cibernético, quais são os mais frequentes e como são operacionalizados, para que estejam preparados quando se depararem com essa situação e como devem agir;

VII. **Teste Controlado** - submeter a empresa a teste de ataque cibernético controlado, para mensurar o nível de maturidade dos controles de prevenção.

- As áreas Tecnologia e Compliance & Controles Internos devem trabalhar conjuntamente para colocar em prática as medidas descritas nesta política.

## 1.2. Objetivos

- Em consonância com a Resolução nº 4.658, a empresa estabelece como objetivo da Segurança Cibernética: proteger o ambiente virtual e os ativos da empresa e do Cliente.

- A proteção do ambiente virtual está embasada em diretrizes que visam assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

- O método adotado para proteção do ambiente virtual baseia-se em prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

## 1.3. Compromisso

- A Diretoria Executiva atua ativamente no sentido de apoiar a implantação, o desenvolvimento e a promoção da cultura de Segurança Cibernética.

# 2. DIRETRIZES E PROCEDIMENTOS

## 2.1. Identificação e Autenticação

- Por meio de procedimentos a área Tecnologia estabelece mecanismos que permitam:

  - ✓ Determinar quem pode acessar determinado sistema (login);
  - ✓ Efetuar a verificação por meio de credencial (senha) fornecida pelo usuário;
  - ✓ Liberar acesso lógico somente aos recursos e informações necessários e indispensáveis ao desempenho das atividades do colaborador;

- ✓ Bloquear ou desabilitar todo e qualquer serviço de rede não autorizado.

## 2.2. Criptografia

- Por meio de procedimentos a área Tecnologia estabelece mecanismos que permitam:

  - ✓ Criptografar toda e qualquer informação transmitida pela Internet classificada como sigilosa conforme padrões homologados;
  - ✓ Criptografar informações que são alvo típico de criminosos, tais como senhas de acesso, entre outras;
  - ✓ Executar processo contínuo e periódico que teste as regras criptográficas aplicadas, a fim de assegurar o perfeito funcionamento da tecnologia no ambiente.

## 2.3. Prevenção e Detecção de Intrusão

- Por meio de procedimentos a área Tecnologia estabelece mecanismos que permitam:

  - ✓ Monitorar o tráfego e as atividades da rede;
  - ✓ Examinar o tráfego da rede em busca de ameaças que gerem padrões incomuns de fluxo de dados;
  - ✓ Disponibilizar informações sobre as atividades da rede a fim de que se possa identificar atividades suspeitas.

## 2.4. Prevenção de vazamento de informações

- Por meio de procedimentos a área Tecnologia estabelece mecanismos que permitam:

  - ✓ Monitorar de forma constante a transmissão de dados;
  - ✓ Prevenir ou bloquear a saída de dados confidenciais da rede;
  - ✓ Monitorar e/ou bloquear, se necessário for, a transferência de dados.

## 2.5. Varreduras para detecção de vulnerabilidades

- Por meio de procedimentos a área Tecnologia estabelece mecanismos que permitam:

  - ✓ Identificar possíveis vulnerabilidades na rede;
  - ✓ Identificar possíveis brechas em sistemas e políticas de segurança;
  - ✓ Classificar por nível de impacto as vulnerabilidades identificadas;
  - ✓ Executar testes que visem reduzir vulnerabilidades que possam ser exploradas por códigos maliciosos.

## 2.6. Proteção contra softwares maliciosos

- Por meio de procedimentos a área Tecnologia estabelece mecanismos que permitam:

  - ✓ Proteger servidores físicos e virtuais, equipamentos de mesa, dispositivos móveis e dispositivos de segurança da informação contra softwares maliciosos;
  - ✓ Atualizar periodicamente, conforme disponibilização de versão do fabricante, os produtos utilizados para proteção contra softwares maliciosos;
  - ✓ Estabelecer procedimentos que visem os controles de detecção, prevenção e combate a softwares maliciosos;
  - ✓ Verificar a presença de códigos maliciosos, antes de serem utilizados, em todos os arquivos recebidos por meio de redes, em qualquer mídia de armazenamento, correio eletrônico, arquivos baixados (download) ou em páginas web;
  - ✓ Procurar por softwares maliciosos em arquivos anexados aos e-mails;
  - ✓ Emitir alertas sempre que um software malicioso for detectado.

## 2.7. Mecanismos de rastreabilidade da informação

- Por meio de procedimentos a área Tecnologia estabelece mecanismos que permitam:

  - ✓ Identificação de todos os sistemas que contenham informações de clientes da empresa;
  - ✓ Garantir que os sistemas identificados possuam trilhas de auditoria;
  - ✓ Garantir que as operações de entrada e saída de informações dos clientes estejam gravadas nas trilhas de auditoria;
  - ✓ Garantir a implantação de controles internos que permitam auditar a rastreabilidade das informações.

## 2.8. Segmentação da rede

- Por meio de procedimentos a área Tecnologia estabelece mecanismos que permitam:

  - ✓ Restringir o acesso não autorizado;
  - ✓ Efetuar o controle e a rastreabilidade das conexões.

## 2.9. Manutenção das cópias de segurança

- Por meio de procedimentos a área Tecnologia estabelece mecanismos que permitam:

  - ✓ Estabelecer rotinas de backup com periodicidade diária, semanal, mensal e anual;
  - ✓ Estabelecer a periodicidade para retenção e liberação das cópias de backup;

- ✓ Estabelecer as rotinas para recuperação das informações utilizando as cópias de backup.

## 2.10. Registro e análise de impacto de incidentes ocorridos

- Por meio de procedimentos a área Tecnologia estabelece mecanismos que permitam:

  - ✓ Efetuar o registro das informações pertinentes ao incidente ocorrido;
  - ✓ Analisar o incidente e estabelecer plano de ação visando a sua solução;
  - ✓ Gerenciar os incidentes garantindo que sejam solucionados o mais rápido possível.

## 2.11. Análise de Ameaças e Vulnerabilidades para Criação de Imagem Master

- A criação de Imagem Master deverá ser precedida de uma análise de ameaças e vulnerabilidades.
- A análise deverá ser feita 24 horas antes do processo de criação da imagem.
- Por meio de procedimentos a área Tecnologia estabelece mecanismos para a criação de Imagem Master que permitem:

  - ✓ Identificar as vulnerabilidades existentes para o sistema operacional a ser instalado na Imagem Master: Windows Server 2016.
  - ✓ Identificar as ameaças e vulnerabilidades através do site https://www.cvedetails.com/.
  - ✓ Identificar a lista de ameaças e vulnerabilidades existentes para o fornecedor / produto através do endereço https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-34965/year-2018/Microsoft-Windows-Server-2016.html.
  - ✓ Analisar e tratar todas as ameaças consideradas críticas, tais como: aplicações remote desktop, authentication vulnerability, unauthentication vulnerability, script execution without authentication, entre outros.

## 2.12. Disseminação da cultura de segurança cibernética

- Por meio de procedimentos a área Tecnologia estabelece mecanismos que permitam:

  - ✓ Manter no site da empresa informações referentes à segurança cibernética;
  - ✓ Garantir a leitura, por parte dos funcionários, da Política de Segurança Cibernética.

# 3. ATRIBUIÇÕES E RESPONSABILIDADES

## 3.1. Compliance & Controles Internos

- Garantir que todos os colaboradores efetuem a leitura da Política de Segurança Cibernética.