FITBANK PAGAMENTOS ELETRÔNICOS

Política de Segurança Cibernética

Código	Documento	Data	Revisão	Páginas
PC018	Segurança Cibernética (Cibersecurity)	18/05/2020		08
PC018	Segurança Cibernética (Cibersecurity)	02/01/2023	01	

Aprovado por:

Rener Silva de Menezes

18 de janeiro de 2023

Sumário

PARTE I - IDENTIFICAÇÃO

1. OBJETIVO

Esta política visa atender os requisitos da Resolução CMN nº 4.893/2021, que dispõe 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.

2. APROVAÇÃO

Infraestrutura e Segurança – responsável pela manutenção desta política.

Compliance & Controles Internos – responsável pela revisão desta política.

Conselho de Administração – responsável pela aprovação desta política.

3. GLOSSÁRIO

AMEAÇA CIBERNÉTICA - conjunto de fatores externos com o potencial de causar dano para um sistema ou organização;

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.

COMPUTAÇÃO EM NUVEM - modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem (PSN);

CONFIDENCIALIDADE - princípio da segurança da informação do PJSC que assegura que a informação só seja acessada por pessoas, órgãos ou sistemas credenciados, ou seja, impede que a informação esteja disponível ou seja divulgada a indivíduos, entidades ou processos sem autorização específica;

CRIPTOGRAFIA - arte de proteção da informação, por meio de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de

procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno). A chave de decifragem pode ser igual (criptografia simétrica) ou diferente (criptografia assimétrica) da chave de cifragem;

DADO PESSOAL - informação relacionada à pessoa natural identificada ou identificável;

DADO PESSOAL SENSÍVEL - dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

DESASTRE - evento, ação ou omissão, repentino e não planejado, que tenha permitido acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica, gerando sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação;

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 problemas de segurança (intrusão).

DISPONIBILIDADE - princípio da segurança da informação que consiste em fazer com que a informação esteja acessível e utilizável, no momento escolhido por uma pessoa, órgão ou sistema, ou seja, garante o acesso à informação quando requisitado, de acordo com os seus requisitos de disponibilidade.;

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.

INSTITUIÇÃO FINANCEIRA – Uma organização responsável por intermediar o cliente e o mercado financeiro, oferecendo diferentes serviços, autorizada pelo BACEN (aqui chamada de “IF”).

INTEGRIDADE – princípio da segurança da informação que garante a não violação das informações para protegê-las contra alteração, gravação ou exclusão acidental ou proposital. A informação protegida deve ser íntegra, sem sofrer qualquer alteração indevida, não importa por quem e nem em qual etapa, se no processamento ou no envio;

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

PLANO DE CONTINUIDADE DE NEGÓCIOS EM SEGURANÇA DA INFORMAÇÃO - Documentação dos procedimentos e das informações necessárias para que a IF mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo, em um nível previamente definido, em caso de incidente;

PLANO DE GESTÃO DE INCIDENTES - Plano de ação claramente definido e documentado, para ser usado em caso de incidente que basicamente englobe os principais recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes;

PRESERVAÇÃO DE EVIDÊNCIA DE INCIDENTES CIBERNÉTICOS - processo que compreende a salvaguarda das evidências e dos dispositivos, de modo a garantir que os dados ou metadados não sofram alteração, preservando-se a integridade e a confidencialidade das informações;

PROVEDOR DE SERVIÇOS DE NUVEM - Ente, público ou privado, que fornece uma plataforma, infraestrutura, aplicativo, serviços de armazenamento ou ambientes de tecnologia da informação baseados em nuvem;

RISCO - No sentido amplo, trata-se da possibilidade de ocorrência de um evento que pode impactar o cumprimento dos objetivos. Pode ser mensurado em termos de impacto e de probabilidade;

RISCO DE SEGURANÇA DA INFORMAÇÃO - Risco potencial associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

SEGURANÇA CIBERNÉTICA - Ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço

cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis.

4. REVISÃO

- 18/05/2020 – Versão Original
- 02/01/2023 – Versão Atual – Revisão 01

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*, através de serviços flexíveis que permitem criar e distribuir soluções rapidamente e com mais segurança, usando as melhores práticas de mercado, incluindo, mas não se limitando, as normas ISO 27002, ISO 27701 e CIS. 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.

2. ESCOPO

Estão sujeitos à Política, as empresas do Grupo FitBank e todos os seus funcionários, consultores, terceiros, fornecedores e parceiros, caso acessem, armazenem, processem ou transmitam informações pertencentes, ou sob a guarda do FitBank.

3. OBJETIVOS

São objetivos dessa política de segurança:

I. Manter a confidencialidade, integridade e disponibilidade das informações pertencentes a, ou sob a custódia do FitBank;

II. Estabelecer medidas de proteção da infraestrutura de suporte aos serviços e atividades empresariais;

III. Prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados ao

ambiente cibernético;

IV. Definir diretrizes operacionais de segurança para o ambiente cibernético;

V. Adotar controles específicos para rastreabilidade da informação sensível.

4. DIRETRIZES E PROCEDIMENTOS

4.1. Identificação e Autenticação

Por meio de políticas específicas, a área de Infraestrutura e Segurança estabelecerá mecanismos, diretrizes e orientações 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 desabilitam todo e qualquer serviço de rede não autorizado.

4.2. Criptografia

Por meio de políticas específicas, a área de Infraestrutura e Segurança estabelecerá mecanismos, diretrizes e orientações 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;
- ✓ Aplicar algoritmos criptográficos nos dados em repouso, em trânsito e/ou em uso.

4.3. Prevenção e Detecção de Intrusão

Por meio de políticas específicas, a área de Infraestrutura e Segurança estabelecerá mecanismos, diretrizes e orientações 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 identificar comportamentos suspeitos.

4.4. Prevenção de vazamento de informações

Por meio de políticas específicas, a área de Infraestrutura e Segurança estabelecerá mecanismos, diretrizes e orientações que permitam:

- ✓ Monitorar de forma constante a transmissão de dados;
- ✓ Prevenir ou bloquear a saída de dados confidenciais da rede;
- ✓ Prevenir o uso mal-intencionado e equivocado de informações sensíveis;
- ✓ Monitorar e/ou bloquear, se necessário for, a transferência de dados.

4.5. Varreduras para detecção de vulnerabilidades

Por meio de políticas específicas, a área de Infraestrutura e Segurança estabelecerá mecanismos, diretrizes e orientações 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.

4.6. Proteção contra softwares maliciosos

Por meio de políticas específicas, a área de Infraestrutura e Segurança estabelecerá mecanismos, diretrizes e orientações 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.

4.7. Mecanismos de rastreabilidade da informação

Por meio de políticas específicas, a área de Infraestrutura e Segurança estabelecerá mecanismos, diretrizes e orientações 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;
- ✓ Orientar para o correto registro, análise de causa e do impacto e tratamento adequado de incidentes relevantes para as atividades da IF.

4.8. Segmentação da rede

Por meio de políticas específicas, a área de Infraestrutura e Segurança estabelecerá mecanismos, diretrizes e orientações que permitam:

- ✓ Restringir o acesso não autorizado;
- ✓ Efetuar o controle e a rastreabilidade das conexões;
- ✓ Segmentar redes públicas e privadas;
- ✓ Restringir acesso às rede sem-fio usando criptografia forte e autenticação de usuários.

4.9. Manutenção das cópias de segurança

Por meio de políticas específicas, a área de Infraestrutura e Segurança estabelecerá mecanismos, diretrizes e orientações 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.

4.10. Registro e análise de impacto de incidentes ocorridos

Por meio de políticas específicas, a área de Infraestrutura e Segurança estabelecerá mecanismos, diretrizes e orientações 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.

4.11. Criação e manutenção de Plano de Continuidade de Negócios (BCP)

Por meio de políticas específicas, a área de Infraestrutura e Segurança estabelecerá

mecanismos, diretrizes e orientações que permitam:

- ✓ Que, em situação de crise, os processos essenciais e críticos sejam devidamente mantidos, preservando, assim, a continuidade das funções, operações e serviços críticos do negócio;
- ✓ Que o BCP deve ser atualizado e testado anualmente.

4.12. Disseminação da cultura de segurança cibernética

Por meio de políticas específicas, a área de Infraestrutura e Segurança estabelecerá mecanismos, diretrizes e orientações que permitam:

- ✓ Manter no site da empresa informações referentes à segurança cibernética;
- ✓ Garantir a leitura, por parte dos funcionários, da Política de Segurança Cibernética;
- ✓ Garantir acesso a cursos internos sobre segurança da informação e outros assuntos relacionados à segurança corporativa em geral;
- ✓ Exigir que os colabores façam os cursos indicados e manter, para fins de auditoria, listas de presenças.

5. ATRIBUIÇÕES E RESPONSABILIDADES

5.1. Infraestrutura & Segurança

- Atualização da política de Segurança Cibernética;
- Criação das normas complementares;
- Criação da documentação técnica (manuais);
- Cumprimento das políticas, aplicação das diretrizes técnicas ao ambiente computacional.

5.2. Compliance & Controles Internos

- Revisão da política de Segurança Cibernética;
- Auditoria do ambiente interno
- Garantir que todos os colaboradores efetuem a leitura da Política de Segurança Cibernética.

Página de assinaturas

Rener Menezes
970.499.643-87
Aprovar

HISTÓRICO

10 jan 2023 16:59:23 — **Gustavo Castelo Branco Crisostomo Ramos** criou este documento. (E-mail: gustavo.ramos@fitbank.com.br)

12 jan 2023 10:24:49 — **Rener Silva de Menezes** *(E-mail: rener.menezes@fitbank.com.br, CPF: 970.499.643-87)* visualizou este documento por meio do IP 54.94.72.147 localizado em São Paulo - Sao Paulo - Brazil.

18 jan 2023 10:42:02 — **Rener Silva de Menezes** *(E-mail: rener.menezes@fitbank.com.br, CPF: 970.499.643-87)* aprovou este documento por meio do IP 54.94.72.147 localizado em São Paulo - Sao Paulo - Brazil.