Código	Documento	Data	Revisão	Páginas
PC016	Governança de TI	18/05/2020	01	09

ÍNDICE

PARTE I - IDENTIFICAÇÃO

1. OBJETIVO

Esta política estabelece diretrizes que visam alinhar a Tecnologia da Informação com o negócio da empresa, tornando a Governança de TI parte estratégica do FitBank. A Governança de TI tem como papel fundamental proteger um dos principais elementos da organização: a informação.

As diretrizes buscam proporcionar o mínimo indispensável de segurança operacional de maneira a manter o FitBank em conformidade com a Resolução nº 4.557, que dispõe sobre a estrutura de gerenciamento de riscos, especificamente:

- Art. 33. A estrutura de gerenciamento deve prever, adicionalmente, para o risco operacional:

  IV - sistemas, processos e infraestrutura de TI que: a) assegurem integridade, segurança e disponibilidade dos dados e dos sistemas de informação utilizados; b) sejam robustos e adequados às necessidades e às mudanças do modelo de negócio, tanto em circunstâncias normais quanto em períodos de estresse; c) incluam mecanismos de proteção e segurança da informação com vistas a prevenir, detectar e reduzir a vulnerabilidade a ataques digitais.

2. ABRANGÊNCIA

Além de institucionalizar boas práticas pertinentes aos serviços, a Governança de TI deve também servir de base para:

- Desenvolver mecanismos para manter a disponibilidade e continuidade do negócio;
- Desenvolver controles e alinhamentos de TI a marcos de regulação externos.

3. APROVAÇÃO

Tecnologia – responsável pela manutenção desta política.

Riscos e PLD – responsável pela revisão desta política.

Conselho de Administração – responsável pela aprovação desta política.

4. GLOSSÁRIO

5. REVISÃO

- 18/05/2020 – Versão Original.

PARTE II – DESCRITIVO

1. INTRODUÇÃO

- De forma constante, as empresas dependem da Tecnologia da Informação para suportar e gerir o seu negócio, aumentando, desta forma, a necessidade de transparência e controle dos recursos de TI aplicados.

- Em um cenário de negócios dinâmicos, as empresas, para se manterem competitivas, buscam soluções e estratégias que visam potencializar forças de forma a não sucumbirem.

- A Governança de TI é de responsabilidade dos executivos, consistindo em aspectos de liderança, estrutura organizacional e processos que garantam que a área de Tecnologia da Informação suporte e aprimore os objetivos e as estratégias da empresa.

- Assim sendo, este documento busca estabelecer diretrizes para o uso da TI dentro do FitBank como um guia de suporte ao negócio, monitorando o seu uso conforme estratégias e políticas estabelecidas.

2. DIRETRIZES E PROCEDIMENTOS

2.1 Gerais

- A Governança baseia-se na execução de processos de suporte ao serviço prestado pela área de Tecnologia. Os processos relacionados a este tipo de suporte são: Gestão de Incidente; Gestão de Problemas; Gestão de Configuração; Gestão de Mudança; Gestão de Liberação; Gestão de Nível de Serviço; Gestão de Software; Gestão de Hardware e Gestão de Segregação de Função.

2.2 Gestão de Incidente

- Um incidente é qualquer evento que não faz parte do funcionamento padrão de um serviço de TI e que causa, ou pode causar, uma interrupção no serviço ou uma redução do seu nível de desempenho.

- Assim sendo, ocorrido um incidente, a Gestão de Incidente tem por objetivo restaurar o serviço à sua condição original de funcionamento, no menor tempo possível, minimizando o impacto sobre o nível dos serviços prestados, até mesmo na indisponibilidade total.

- O processo contempla:

  ✓ Preparação e planejamento de resposta a incidentes;

- ✓ Monitoramento, detecção, análise e notificação de incidentes e eventos de segurança da informação;
- ✓ Registros das atividades de gerenciamento de incidentes;
- ✓ Veiculação de respostas, incluindo aquelas relativas a escalação, recuperação controlada de um incidente e comunicação às pessoas ou organizações relevantes, internas e externas;
- ✓ Equipe especializada para tratamento de incidentes de segurança da informação;
- ✓ Atualização constante em relação a assuntos pertinentes à segurança de informações, através de participação em grupos de discussão, fóruns, cursos, palestras.
- ✓ Tratamento disciplinar formal estabelecido para lidar com colaboradores que cometam violações de segurança da informação;
- ✓ Processo de realimentação adequado para assegurar que as pessoas que notificaram um evento de segurança da informação sejam informadas dos resultados após o assunto ter sido tratado e encerrado.

2.3 Gestão de Problemas

- Este processo é focado tanto na solução de problemas decorrentes de um ou mais incidentes (atuação corretiva), quanto na identificação e na resolução de problemas e erros conhecidos antes que os incidentes ocorram (atuação preventiva).
- Busca minimizar o impacto negativo de incidentes e problemas decorrentes de situações de TI e que afetam o negócio, evitando novos incidentes relacionados com os mesmos erros.
- O objetivo é atacar a causa do problema e assim aplicar uma solução definitiva, elevando o nível de produtividade e disponibilidade dos serviços de TI.

2.4 Gestão de Mudança

- Conceitualmente, é qualquer remoção, inclusão ou alteração de aplicação ou infraestrutura que possa afetar os serviços de TI.
- Este processo é responsável pelo controle das mudanças na infraestrutura e aplicações de TI, ou mudanças que afetem os níveis de serviço de TI acordados. Este controle se dá através de processos

planejados, documentados e controlados de modo que mudanças não tenham grande impacto nos serviços disponibilizados.

- O processo Gestão de Mudanças visa a assegurar que as alterações em um serviço existente ou a entrada de novos serviços no ambiente de produção sejam realizadas de forma planejada e controlada (avaliadas, priorizadas, planejadas, testadas, implantadas, documentadas e comunicadas), reduzindo o risco e o impacto nas áreas de negócio da empresa.

- O processo contempla:

  - ✓ Levantamento e registro de mudanças;

  - ✓ Avaliação do impacto, custos necessários, benefícios que a mudança trará para a empresa e os riscos da mudança;

  - ✓ Elaboração da justificativa de mudança para obter a devida aprovação;

  - ✓ Gerenciamento e coordenação na implementação da mudança;

  - ✓ Encerramento da mudança.

- Nem toda solicitação requer o registro de uma mudança, é necessário analisá-la a fim de identificar se deve ser aplicado o Gerenciamento de Mudança. A análise baseia-se em:

  - ✓ Mudança nível 1: mudanças pré-autorizadas, que não representam risco ao ambiente de TI e, como são rotineiras, possuem um procedimento de execução;

  - ✓ Mudança nível 2: mudanças que podem gerar impacto no ambiente de TI;

  - ✓ Mudança nível 3: mudanças que necessitam de implementação imediata e que, caso não seja executada, poderá resultar em indisponibilidade de serviços.

- Principais atividades:

  - ✓ Registro e classificação das solicitações de mudança conforme o tipo: nível 1, nível 2, nível 3;

  - ✓ Priorização das solicitações recebidas;

  - ✓ Aprovação formal da solicitação para implementação;

  - ✓ Agendamento das mudanças a serem aplicadas no mesmo dia reduzindo riscos;

- ✓ Execução de teste de implementação para validar se a mudança atingiu seu objetivo.

2.5 Gestão de Liberação

- Visa proteger o ambiente de produção da empresa. A proteção ocorre com a utilização de procedimentos formais e rotinas de testes que procuram avaliar todos os fatores envolvidos no processo de mudança de software ou hardware.
- Este processo é executado em conjunto com a Gestão de Mudança.
- O processo contempla:
  - ✓ Gerenciar a implantação dos itens de configuração de hardware e software aprovados;
  - ✓ Gerenciar as expectativas dos usuários em relação aos serviços de TI;
  - ✓ Negociar o plano de implementação de liberações;
  - ✓ Garantir que somente itens de configuração aprovados e com qualidade adequada sejam utilizados no ambiente de produção.

2.6 Gestão do Nível de Serviço

- Visa a garantir a entrega dos serviços de TI a todos os usuários respeitando os níveis de qualidade adequados e priorizados conforme a necessidade da empresa.
- O processo contempla:
  - ✓ Melhorar a qualidade dos serviços de TI entregue aos usuários;
  - ✓ Manter a disponibilidade dos serviços para evitar prejuízos;
  - ✓ Garantir o alinhamento entre a linha de negócio da empresa e a TI;
  - ✓ Prover comunicação entre as partes interessadas;
  - ✓ Disponibilizar mecanismos de verificação;
  - ✓ Manter o controle das entregas e execuções;
  - ✓ Estipular formas de contabilização e apresentação dos resultados.

2.7 Gestão de Software

- Visa: a) garantir a não utilização de software não autorizado pela empresa, b) identificar software instalado que nunca foi utilizado (possível ponto de atenção para redução de custos) e c) definir as autorizações para instalação de software.

- Principais atividades:

  ✓ Quinzenalmente efetuar o inventário de softwares instalados;

  ✓ Quinzenalmente executar procedimentos para eliminação de software não autorizado;

  ✓ Manter controle sobre aquisição e uso das licenças;

  ✓ Gerar informações gerenciais sobre a gestão de software.

2.8 Gestão de Hardware

- Visa garantir a padronização e a manutenção dos ativos de hardware da empresa.

- O objetivo é atuar de forma efetiva na aquisição ou substituição do hardware, atentando sempre para a evolução das necessidades que são exigidas pelo software que será utilizado.

- Principais atividades:

  ✓ Mapear os ativos de hardware, identificando seus componentes e seus usuários;

  ✓ Quinzenalmente executar o inventário de hardware;

  ✓ Quinzenalmente executar procedimentos para retirada de hardware não autorizado;

  ✓ Monitorar o ciclo de vida do hardware visando em uma utilização mais eficiente;

  ✓ Auxiliar na tomada de decisão sobre a compra, reparo ou atualização de algum ativo, ampliando a sua vida útil.

2.9 Gestão de Segregação de Função

- Visa manter a separação de atividades que envolvem autorização, aprovação, execução e controle de operações, de tal maneira que nenhum funcionário detenha poderes e atribuições em desacordo com este princípio.

- A segregação de função visa coibir o usuário de, exercendo certa atividade, executar outra atividade ao mesmo tempo que implique em risco operacional para a empresa.

- O Manual da Organização, através da Estrutura Organizacional implementada, descreve as atribuições bem como a segregação de função estabelecida.

- Principais atividades:

  ✓ Atuar de forma sistemática no sentido de garantir a separação das funções de autorização, execução e controle.

  ✓ Manter uma estrutura de pontos de controle a fim de garantir a segregação de funções pertinente a autorização e execução.

3. ATRIBUIÇÕES E RESPONSABILIDADES

3.1 Tecnologia

- Atuar na manutenção e atualização deste documento periodicamente.

- Submeter o documento para aprovação da Diretoria Executiva.