Política de Manutenção e Desenvolvimento de Sistemas

Grupo Edson Queiroz

#### ÍNDICE

Sumário

[2. APRESENTAÇÃO 3](#_Toc147237718)

[2.1. Objetivo 3](#_Toc147237719)

[2.2. Abrangência 3](#_Toc147237720)

[2.3. Vigência 3](#_Toc147237721)

[2.4. Área técnica responsável pela política 3](#_Toc147237722)

[2.5. Aprovação 4](#_Toc147237723)

[3. ESCOPO 5](#_Toc147237724)

[3.1. Esta política se aplica a todos os sistemas desenvolvidos internamente ou contratados, bem como a todas as equipes envolvidas na manutenção/sustentação desses sistemas. 5](#_Toc147237725)

[4. DIRETRIZES 5](#_Toc147237726)

[4.1. Todos os sistemas devem ser desenvolvidos ou contratados seguindo as melhores práticas de desenvolvimento de software, incluindo documentação adequada, testes e revisão de código; 5](#_Toc147237727)

[4.2. Todos os sistemas devem ser mantidos atualizados em conformidade com os padrões de segurança de informação da empresa; 5](#_Toc147237728)

[4.3. Todas as alterações nos sistemas já existentes ou nos sistemas mantidos devem ser documentadas e passar por um processo de aprovação antes de serem implementadas. 5](#_Toc147237729)

[5.1. A equipe de Aplicações de TI é responsável por garantir que esta política seja seguida por todas as equipes envolvidas no processo de desenvolvimento e manutenção de sistemas; 5](#_Toc147237730)

[5.2. As áreas usuárias são responsáveis por fornecer os requisitos técnicos necessários para o desenvolvimento e manutenção dos sistemas, aprovar escopo de trabalho e colaborar com as equipes de TI para garantir que os sistemas atendam às suas necessidades. 5](#_Toc147237731)

[5.3. Compete as áreas de negócio do Grupo Edson Queiroz: 5](#_Toc147237732)

[5.4. Compete ao Comitê de TI e ao Comitê de cada Negócio do Grupo Edson Queiroz: 5](#_Toc147237733)

[5.5. Compete a TI corporativa, as seguintes atribuições: 6](#_Toc147237734)

[6.1. Para garantir a continuidade, a segurança e evitar mudanças não registradas e autorizadas em sistemas de informação, os acessos aos códigos-fonte devem ser restritos e controlados, inclusive para a área de infraestrutura. 7](#_Toc147237735)

[6.2. Para maior previsibilidade nas entregas de soluções de TI a contratação de soluções deve prever acordos de nível de serviço e acordos operacionais quando envolver as áreas internas dos Negócios do GEQ. 7](#_Toc147237736)

[7.1. Esta política deve ser revisada anualmente ou conforme o entendimento do Comitê Gestor de Segurança da Informação, para garantir que continue relevante e eficaz. 7](#_Toc147237737)

[8.1. Caberá à Diretoria de Tecnologia da Informação levar qualquer situação excepcional e/ou não contemplada nesta política ao Chief Financial Officer (CFO), para que seja tomada a decisão emergencial sobre a medida a ser adotada e, se for o caso, providencia a inclusão de nova diretriz neste documento. 7](#_Toc147237738)

# APRESENTAÇÃO

## Objetivo

Esta política estabelece diretrizes para o desenvolvimento e manutenção de sistemas/aplicações no Grupo Edson Queiroz, visando garantir a qualidade, transparência, eficiência e segurança da informação.

## Abrangência

Esta política é aplicável a todas as empresas do Grupo Edson Queiroz.

## Vigência

Esta política terá prazo indeterminado e entrará em vigor a partir da data de sua publicação, com revisão periódica a cada 12 meses ou quando for necessária.

## Área técnica responsável pela política

O conteúdo dessa política é de responsabilidade da área de Aplicações de TI.

## Aprovação

|  |  |  |
| --- | --- | --- |
| Carlos Rotella | Presidente |  |
| Roberto Costa | Diretor Jurídico, de RI e *Compliance* |  |
| Aleksandro Oliveira | *Chief Financial Officer* (CFO) |  |

# ESCOPO

## Esta política se aplica a todos os sistemas desenvolvidos internamente ou mantidos pela área de Aplicações de TI, bem como a todas as equipes envolvidas na manutenção/sustentação desses sistemas.

# DIRETRIZES

## Todos os sistemas devem ser mantidos atualizados em conformidade com os padrões de segurança de informação da empresa;

## Todas as alterações nos sistemas já existentes ou nos sistemas mantidos devem ser documentadas e passar por um processo de aprovação antes de serem implementadas.

## Processo de desenvolvimento seguro, por meio da utilização de padrões de design de aplicação segura, práticas de compromissos seguros, treinamento de desenvolvedores, gestão de vulnerabilidades, segurança de código de terceiros e procedimentos de teste de segurança.

## Utilização de ferramentas de análise estática e dinâmica, e realização de testes de invasão para identificar vulnerabilidades em aplicações.

## Infraestrutura Segura, com a aplicação de configurações de segurança padrão para componentes de infraestrutura de aplicações e manutenção de ambientes separados para sistemas de produção e não produção.

## Treinamentos periódicos em práticas de desenvolvimento seguro e promoção da cultura de segurança dentro das equipes.

1. RESPONSABILIDADES

## A equipe de Aplicações de TI é responsável por garantir que esta política seja seguida por todas as equipes envolvidas no processo de desenvolvimento e manutenção de sistemas;

## As áreas usuárias são responsáveis por fornecer os requisitos técnicos necessários para o desenvolvimento e manutenção dos sistemas, aprovar escopo de trabalho e colaborar com as equipes de TI para garantir que os sistemas atendam às suas necessidades.

## Compete as áreas de negócio do Grupo Edson Queiroz:

1. Informar as necessidades de informações, tanto gerenciais quanto operacionais;
2. Realizar testes de usuário, de acordo com plano de testes, das aplicações mantidas ou desenvolvidas pela área de Aplicações de TI;
3. Homologar as funcionalidades dos sistemas de informação.

## Compete ao Comitê de TI e ao Comitê de cada Negócio do Grupo Edson Queiroz:

1. Realizar a priorização das demandas de TI;
2. Aprovar as demandas de TI.

## Compete a TI corporativa, as seguintes atribuições:

1. Classificar e priorizar, junto ao Negócio, as demandas de sistemas de informação;
2. Realizar a especificação técnica necessária das funcionalidades dos sistemas de informação para a disponibilização da aplicação;
3. Desenvolver e/ou providenciar a contratação de sistemas de informação;
4. Garantir a disponibilidade operacional dos sistemas de informação
5. Adotar e manter práticas de desenvolvimento seguro, participar de treinamentos de segurança, e colaborar com equipes de segurança na identificação e correção de vulnerabilidades.
6. Garantir que os recursos necessários à segurança das aplicações estejam disponíveis e que a cultura de segurança seja promovida em toda a organização.
7. DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO
   * 1. Todas as solicitações de melhoria de sistemas de informação devem ser solicitadas através de chamado;
     2. Todas as mudanças em sistemas de informações devem estar em conformidade com os processos internos da área de TI;
     3. A TI deve desenvolver uma metodologia de desenvolvimento e manutenção de sistemas, a qual de ser seguida de forma a garantir a usabilidade, a necessidade de documentação da aplicação, garantindo a atendimento necessário aos Negócios;
     4. Para toda solução de sistema de informação a ser desenvolvido e/ou adquirido de terceiro deve ser elaborado documento com descrição técnica detalhada da solução;
     5. Deve ser estabelecido ambientes de bases de dados específicos para desenvolvimento, testes, homologação e de produção;
     6. Antes de disponibilizar uma nova aplicação e/ou atualização de versão para o ambiente de produção:
        + 1. O usuário responsável deve realizar os devidos testes de validação, com a geração das evidências necessárias, formalizando a homologação para posterior liberação para o ambiente de produção.

## Para garantir a continuidade, a segurança e evitar mudanças não registradas e autorizadas em sistemas de informação, os acessos aos códigos-fonte devem ser restritos e controlados, inclusive para a área de infraestrutura.

## Para maior previsibilidade nas entregas de soluções de TI a contratação de soluções deve prever acordos de nível de serviço e acordos operacionais quando envolver as áreas internas dos Negócios do GEQ.

1. REVISÕES

## Esta política deve ser revisada anualmente ou conforme o entendimento do Comitê Gestor de Segurança da Informação, para garantir que continue relevante e eficaz.

1. EXCEÇÕES

## Caberá à Diretoria de Tecnologia da Informação levar qualquer situação excepcional e/ou não contemplada nesta política ao Chief Financial Officer (CFO), para que seja tomada a decisão emergencial sobre a medida a ser adotada e, se for o caso, providenciar a inclusão de nova diretriz neste documento.

A presente política foi aprovada no dia \_\_/\_\_/\_\_\_\_

**HISTÓRICO DE REVISÕES**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versão** | **Data da Revisão** | **Alterado por** | **Comentários** |
| 1.0 | 15/09/2023 | Andressa Gomes | Redação inicial |
| 1.1 | 02/10/2023 | Thiago Correia | Citação de sistemas contratados em alguns tópicos e citação do local do documento referenciado de Gestão de Mudança e Gestão de Configuração |
| 1.2 | 03/10/2023 | Andressa Gomes | Alteração do escopo para inclusão de sistemas mantidos pela área de aplicações e remoção da referência aos processos de mudança e configuração. |
| 1.3 | 18/10/2023 | Andressa Gomes | Diretrizes e Competências da TI Corporativa, baseada na CIS Control, |

\* \* \*