****

**teste2**

**Informações Gerais**

Versão: teste2

Status do documento: Draft

Classificação: teste2

Cliente:

Nome do documento: teste2

Data: 19/07/2024

Consultor(es) de Segurança: teste2

Representante(s) do Cliente: teste2

Índice

[1 Introdução 3](#_Toc172120260)

[1.1 Contextualizando o relatório de impacto 3](#_Toc172120261)

[1.2 Objetivo do documento 3](#_Toc172120262)

[1.3 Siglas/Glossário 3](#_Toc172120263)

[2 Modelagem de contexto 4](#_Toc172120264)

[2.1 Identificação de ativos 4](#_Toc172120265)

[2.2 Identificação de vulnerabilidades 4](#_Toc172120266)

[2.3 Avaliação dos impactos 4](#_Toc172120267)

[Anexo A : Entrevista e coleta de informações 5](#_Toc172120268)

**Lido e aprovado pelos seguintes responsáveis :**

# Introdução

## Contextualizando o relatório de impacto

CONSIDERAÇÕES GERAIS

A Prefeitura Neogov se trata de uma pessoa jurídica de Direito Público fictício, especificamente dados anonimizados de uma Prefeitura Municipal com cenário reduzido e a finalidade de apresentação do nosso modelo de análise de riscos, a qual possui impacto em um município composto por 30.000 habitantes. Em sua estrutura, comporta 12 Secretarias, com 124 servidores em atividade. A infraestrutura física principal está situada na Rua das Flores, número 123, CEP 12345-678 Bairro Centro, Cidade Fictícia, Estado Hipotético.

A entidade possui uma variedade de tecnologias (hardware e software) que precisam ser revisadas para padronização. Ademais, a maturidade de conformidade à Lei Geral de Proteção de Dados (LGPD) e de requisitos de Segurança da Informação, segundo normas internacionais, são os dois objetivos principais da Entidade com a presente assessoria e consultoria em implementação de Privacidade, Proteção de Dados e Segurança da Informação, visto estar em situação muito aquém dos mínimos níveis necessários e requeridos por entidades de fiscalização, tais como Autoridade Nacional de Proteção de Dados (ANPD), Ministérios Públicos e Tribunais de Contas.

ABORDAGEM DE GESTÃO DE RISCO

A gestão de riscos de privacidade, proteção de dados e segurança da informação em órgãos públicos, como prefeituras, é uma tarefa crucial na era digital. Com o crescente volume de informações sensíveis e pessoais que as prefeituras coletam e processam, garantir a integridade, confidencialidade e disponibilidade desses dados se torna uma responsabilidade essencial. No entanto, muitas prefeituras, como a ora analisada, enfrentam uma série de desafios em sua gestão de riscos, incluindo falhas no mapeamento de dados e processos, ausência de controles de acesso, práticas inseguras de senhas e problemas com firewalls.

CRITÉRIOS BÁSICOS

A conformidade com as regulamentações e padrões de segurança da informação é uma prioridade crescente para organizações em todo o mundo, à medida que os dados se tornam um ativo crítico e sensível. No Brasil, a Lei Geral de Proteção de Dados (LGPD) estabeleceu uma estrutura legal para a proteção de informações pessoais, e internacionalmente, padrões como ISO, NIST e NIS definem diretrizes detalhadas para a gestão eficaz da segurança da informação. O objetivo de uma entidade em se adequar a essas regulamentações e normas é garantir a confidencialidade, integridade e disponibilidade dos dados, bem como demonstrar um compromisso com a privacidade e a segurança de informações críticas.

Os principais critérios a serem adotados são baseados nas seguintes normas:

     Lei Geral de Proteção de Dados (LGPD)

     ISO 27001: Gestão de Segurança da Informação

     ISO 27002: Código de Prática para Controles de Segurança da Informação

     ISO 27018: Código de Prática para a Proteção de Informações Pessoais em Serviços de Nuvem Pública que atuam como Processadores de Dados Pessoais

     ISO 29100: Privacidade em Sistemas de Informação

     NIST SP 800-53: Controles de Segurança da Informação

     NIS Directive: Diretiva sobre Segurança de Redes e Sistemas de Informação

ESCOPO E LIMITES

A implementação da Lei Geral de Proteção de Dados (LGPD) e a garantia da segurança da informação em entidades públicas são processos complexos que requerem um planejamento cuidadoso e expertise técnica. Para orientar com eficácia esses esforços, é crucial definir claramente o escopo e os limites das atividades. Essa definição ajuda a alinhar expectativas, otimizar recursos e garantir que a entidade pública atinja seus objetivos de conformidade e segurança.

ESCOPO DA CONSULTORIA E ASSESSORIA

Avaliação de Conformidade LGPD

A consultoria irá iniciar com uma avaliação abrangente da conformidade da entidade pública com os requisitos da LGPD. Isso inclui a revisão dos processos de coleta, processamento e armazenamento de dados pessoais, bem como a identificação de áreas de não conformidade. A principal atividade nesta fase é o mapeamento de dados e processos, a fim de levantar o inventário de dados pessoais e estabelecer seu fluxo na Entidade.

Análise de Riscos de Segurança da Informação

Uma análise detalhada dos riscos de segurança da informação deve ser realizada para identificar vulnerabilidades e ameaças que possam impactar a integridade, confidencialidade e disponibilidade dos dados.

Desenvolvimento de Políticas e Procedimentos

Com base na avaliação de conformidade e na análise de riscos, a consultoria auxiliará na criação de políticas e procedimentos específicos para a LGPD e Segurança da Informação. Isso inclui a definição de como os dados pessoais são tratados e protegidos.

Treinamento e Conscientização

O escopo deve incluir a implementação de programas de treinamento e conscientização para os servidores da entidade pública, visando garantir que eles compreendam as implicações da LGPD e as melhores práticas de segurança da informação, com foco na mudança da Cultura Organizacional da Entidade.

Tecnologia e Controles de Acesso

O trabalho abordará a implementação de tecnologias e controles de acesso que garantam a segurança dos dados e a conformidade com a LGPD. A principal implementação se trata dos softwares LGPDWEB e LGPDRIVE, com o objetivo de permitir a perenidade do processo de conformidade, com automação de diversas tarefas ligadas ao Encarregado de Dados e ampla visão dos requisitos de Segurança da Informação.

Gestão de Incidentes de Segurança

A definição de procedimentos para lidar com incidentes de segurança da informação é essencial. O trabalho abrangerá a criação de planos de resposta a incidentes e a estruturação de equipes de prontidão.

Auditoria e Monitoramento Contínuo

Um componente crítico é a implementação de processos de auditoria e monitoramento contínuo para garantir que as políticas e controles estejam sendo cumpridos. Esta fase está intrinsicamente ligada ao LGPDWEB, software capaz de permitir a ampla visão de todo o processo de adequação e maturidade.

LIMITES DA CONSULTORIA E ASSESSORIA

Advocacia

A consultoria não deve fornecer serviços jurídicos, como aconselhamento legal específico sobre disputas, litígios ou interpretação legal que não sejam relacionadas à LGPD. Nesse caso, é recomendável que a entidade pública consulte seu corpo técnico da procuradoria ou advogado contratado para tal finalidade.

Não Substitui a Responsabilidade da Entidade Pública

A consultoria e assessoria não eximem a entidade pública de sua responsabilidade principal na implementação da LGPD e segurança da informação. A entidade pública é a responsável pela conformidade e segurança de seus dados.

Recursos Limitados

A consultoria e assessoria estão sujeitas a recursos limitados e podem não cobrir todos os aspectos da implementação da LGPD e segurança da informação. A entidade pública deve estar ciente de que precisará alocar recursos internos para atender às necessidades de conformidade contínua e segurança da informação, visto que a NEOGOV apresentará todas as vulnerabilidades, gestão de riscos e traçará planos de ações cujas medidas corretivas podem requerer empenho financeiro por parte da Entidade para mitigação (compra de firewall, servidor, controles de acessos, etc.).

Evolução Constante

O cenário de privacidade e segurança da informação é dinâmico. Os regulamentos, as ameaças cibernéticas e as melhores práticas estão em constante evolução. A consultoria deve ajudar a entidade pública a se preparar para essas mudanças, mas a responsabilidade pela adaptação contínua é da própria entidade.

## Objetivo do documento

O objetivo deste documento é apresentar o contexto dos riscos, tal como entendidos e transpostos pelo responsável pela gestão dos riscos.

Este documento foi formulado em conjunto pela empresa Neogov e pelo cliente , recebendo assinatura e aquiescência dos responsáveis a fim de permitir que a missão seja prosseguida.

## Siglas/Glossário

**Ativo**: Qualquer item que represente valor para à instituição.

**Confidencialidade**: Propriedade de informações que não devem ser disponibilizadas ou divulgadas à indivíduos, entidades ou processos não autorizados.

**Disponibilidade**: A propriedade de ser acessível e utilizável a pedido de uma entidade autorizada.

**Integridade**: uma propriedade que preserva a precisão e a integridade de um ativo.

# Modelagem de contexto

## Identificação de ativos

 Bens e Ativos Importantes:

  •

**Infraestrutura Física:**

Prédios, escolas, hospitais, ruas e parques.

  •

**Recursos Humanos:**

Professores, médicos, policiais e funcionários.

  •

**Sistemas de Informação:**

Bancos de dados e sistemas de gerenciamento.

  •

**Documentos e Dados:**

Registros de cidadãos e documentos legais.

  •

**Equipamentos:**

Veículos, computadores e máquinas.

  •

**Reputação e Confiança Pública:**

A confiança da comunidade na administração.

**Impactos da Falta de Análise de Vulnerabilidades:**

  [1]

**Reputação:**

  •

**Impacto:**

Danos à imagem pública e perda de confiança.

  •

**Consequências:**

Menor cooperação e engajamento da comunidade.

  [2]

**Operacional:**

  •

**Impacto:**

Interrupções de serviços e perda de produtividade.

  •

**Consequências:**

Atrasos e dificuldades em manter serviços essenciais.

  [3]

**Jurídico:**

  •

**Impacto:**

Consequências legais por violações de dados.

  •

**Consequências:**

Multas, processos judiciais e notificações obrigatórias.

  [4]

**Financeiro:**

  •

**Impacto:**

Custos elevados para mitigar danos.

  •

**Consequências:**

Despesas inesperadas e redução de orçamento para outras áreas.

**Processos Críticos:**

  •

**Gestão Financeira:**

Administração do orçamento e arrecadação de impostos.

  •

**Prestação de Serviços:**

Saúde, educação, segurança e transporte.

  •

**Gestão de Recursos Humanos:**

Contratação e treinamento.

  •

**Planejamento Urbano:**

Desenvolvimento de infraestrutura e políticas econômicas.

**Ativo Mais Valioso:**

  •

**Confiança e Legitimidade:**

Essencial para governar e implementar políticas.

**Critério Mais Importante para Segurança:**

  •

**Proteção de Dados:**

Garantir confidencialidade, integridade e disponibilidade dos dados.

**Conformidade com Leis e Normas:**

  •

**Proteção de Dados:**

Cumprir a Lei Geral de Proteção de Dados (LGPD).

  •

**Normas de Segurança:**

Seguir padrões como a ISO/IEC 27001.

  •

**Serviços Essenciais:**

Garantir prestação contínua de serviços essenciais.

**Maior Ameaça:**

  •

**Cibersegurança:**

Riscos de ataques cibernéticos.

**Principais Preocupações:**

  •

**Recursos Insuficientes:**

Falta de recursos financeiros e humanos.

  •

**Corrupção e Transparência:**

Problemas que minam a confiança pública.

  •

**Gestão de Dados:**

Falhas na proteção de informações e prestação de serviços.

**Incidentes Passados:**

  •

**Desastres e Ataques:**

 Falta de backup nos sistemas essenciais causando a interrupção do serviço.

**Riscos Geográficos:**

  •

**Desastres Naturais:**

Inundações, incêndios e eventos climáticos extremos que afetam a infraestrutura e serviços.

## Identificação de vulnerabilidades

O uso da modelagem do LGPDWEB e seus objetos possibilita identificar vulnerabilidades com granularidade suficiente para essa iteração da análise de risco.

No entanto, fica a critério dos consultores criar novos riscos contextuais que eles possam descobrir durante o contrato.

## Avaliação dos impactos

A tabela abaixo representa a tabela de impacto para os principais ativos de . Para economizar tempo, todos os ativos secundários que entram na modelagem de ativos críticos herdarão esses impactos por padrão, mas podem ser refinados manualmente.

| **Impacto** | | | **Consequências** | | |
| --- | --- | --- | --- | --- | --- |

# Anexo A : Entrevista e coleta de informações