****

**Avaliação e tratamento de riscos**

**Informações Gerais**

Versão: v1

Status do documento: Draft

Classificação: Interno

Nome do documento: Avaliação e tratamento de riscos

Data: 19/07/2024

Consultor(es) de Segurança: Gustavo Pereira

Representante(s) do Cliente: Paladino

**Resumo**

Principais Componentes da Avaliação de Risco:  [1] Identificação de Riscos:  • Riscos Tecnológicos: Falta de análise de vulnerabilidades, ataques cibernéticos, falhas de sistemas.  • Riscos Físicos: Desastres naturais (inundações, incêndios), falhas na infraestrutura.  • Riscos Humanos: Erros humanos, corrupção, falta de treinamento adequado.  [2] Impacto dos Riscos:  • Reputacional: Danos à imagem pública e perda de confiança da comunidade.  • Operacional: Interrupções nos serviços públicos, perda de produtividade.  • Jurídico: Consequências legais, multas, processos judiciais.  • Financeiro: Custos elevados para mitigar danos, redução do orçamento.  [3] Classificação dos Impactos:  • Baixo: Impacto mínimo, serviços não críticos afetados.  • Médio: Impacto moderado, serviços importantes afetados.  • Alto: Impacto significativo, serviços críticos interrompidos.  [4] Prioridade dos Riscos:  • Riscos são priorizados com base na probabilidade de ocorrência e na severidade do impacto.  [5] Mitigação dos Riscos:  • Medidas Preventivas: Implementação de sistemas de segurança, treinamento de funcionários, manutenção regular da infraestrutura.  • Planos de Contingência: Desenvolvimento de planos de resposta a emergências, backups de dados, comunicação eficaz durante crises.  [6] Monitoramento Contínuo:  • Revisão e atualização contínua das medidas de mitigação e dos planos de contingência para se adaptar a novos riscos e mudanças no ambiente externo.

**Mapa de risco atual**

**Riscos de informação**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | **TxV** | | | | | | | | | | | | | |
| **Impacto** |  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **8** | **9** | **10** | **12** | **15** | **16** | **20** |
| **0** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **1** | **1** |  |  | **1** |  |  |  |  |  |  |  |  |  |  |
| **2** | **1** |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **3** | **1** | **1** | **1** |  |  |  |  |  |  |  |  |  |  |  |
| **4** | **1** |  |  |  | **1** |  |  | **2** |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **7 Riscos baixos** |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **1 Riscos médios** |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **2 Riscos elevados** |  |  |

**Riscos operacionais**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | **Probabilidade** | | | | |
| **Impacto** |  | **0** | **1** | **2** | **3** | **4** |
| **0** |  |  |  |  |  |
| **1** |  | **1** | **1** |  |  |
| **2** |  | **3** | **1** |  |  |
| **3** |  |  |  | **1** |  |
| **4** |  |  |  | **2** | **1** |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **5 Riscos baixos** |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **1 Riscos médios** |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **4 Riscos elevados** |  |  |

**Mapa de risco residual**

**Riscos de informação**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | **TxV** | | | | | | | | | | | | | |
| **Impacto** |  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **8** | **9** | **10** | **12** | **15** | **16** | **20** |
| **0** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **1** | **1** |  |  | **1** |  |  |  |  |  |  |  |  |  |  |
| **2** | **1** |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **3** | **1** | **1** | **1** |  |  |  |  |  |  |  |  |  |  |  |
| **4** | **1** |  |  |  | **1** |  |  | **2** |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **7 Riscos baixos** |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **1 Riscos médios** |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **2 Riscos elevados** |  |  |

**Riscos operacionais**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | **Probabilidade** | | | | |
| **Impacto** |  | **0** | **1** | **2** | **3** | **4** |
| **0** |  |  |  |  |  |
| **1** |  | **1** | **1** |  |  |
| **2** |  | **3** | **1** |  |  |
| **3** |  |  |  | **1** |  |
| **4** |  |  |  | **2** | **1** |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **5 Riscos baixos** |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **1 Riscos médios** |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **4 Riscos elevados** |  |  |

Índice

[1 Introdução 4](#_Toc102393843)

[1.1 Contextualizando a Análise de Risco 4](#_Toc102393844)

[1.2 Objetivos do documento 4](#_Toc102393845)

[1.3 Referências 4](#_Toc102393846)

[1.4 Siglas/Glossário 4](#_Toc102393847)

[1.5 Descrição do "LGPDWEB” 5](#_Toc102393848)

[2 Contextualizando 7](#_Toc102393849)

[2.1 Descrição do contexto 7](#_Toc102393850)

[2.2 Definição dos critérios de avaliação dos riscos 7](#_Toc102393851)

[2.2.1 Riscos da Informação 7](#_Toc102393852)

[2.2.1.1 Escala de Impacto 7](#_Toc102393853)

[2.2.1.2 Escala de ameaças 7](#_Toc102393854)

[2.2.1.3 Escala de vulnerabilidade 7](#_Toc102393855)

[2.2.1.4 Limiares de aceitação de riscos 8](#_Toc102393856)

[2.2.2 Riscos Operacionais 8](#_Toc102393857)

[2.2.2.1 Escala de Impacto 8](#_Toc102393858)

[2.2.2.2 Escala de Probabilidade 8](#_Toc102393859)

[2.2.2.3 Limiares de aceitação de riscos 8](#_Toc102393860)

[2.3 Avaliação de tendências e ameaças 9](#_Toc102393861)

[3 Modelagem de contexto 10](#_Toc102393862)

[3.1 Identificação de Ativos 10](#_Toc102393863)

[3.2 Identificação de vulnerabilidades 10](#_Toc102393864)

[3.3 Avaliação das consequências 10](#_Toc102393865)

[4 Avaliação de Risco e Tratamento 11](#_Toc102393866)

[4.1 Resumo da avaliação dos riscos 11](#_Toc102393867)

[4.1.1 Riscos da Informação 11](#_Toc102393868)

[4.1.2 Riscos Operacionais 11](#_Toc102393869)

[4.2 Tratamento de Risco 12](#_Toc102393870)

[4.2.1 Tipo de tratamento 12](#_Toc102393871)

[4.2.2 Plano de Tratamento 12](#_Toc102393872)

[Apêndice A: Entrevista e COLETA de Informações 13](#_Toc102393873)

[Apêndice B: Avaliação das tendências 14](#_Toc102393874)

[Apêndice C: Avaliação de ameaças 15](#_Toc102393875)

[Apêndice D: Contexto do ativo 16](#_Toc102393876)

[Apêndice E: Proprietários de risco 17](#_Toc102393877)

[Apêndice F: Notas e observações do ANALISTA 18](#_Toc102393878)

[Riscos da Informação 18](#_Toc102393879)

[Riscos Operacionais 19](#_Toc102393880)

# 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.

## Objetivos do documento

Este documento resume a metodologia e apresenta os resultados da análise de risco realizada com o LGPDWEB no ambiente do cliente. O LGPDWEB é influenciado pela norma internacional ISO 27005:2011.

Os resultados obtidos destinam-se a identificar os principais riscos, compreender o nível de segurança existente e fornecer recomendações para o estabelecimento de medidas de segurança. As partes entendem que as recomendações não são exclusivas nem exaustivas.

A lista de riscos detectados é baseada nas informações fornecidas pelo Cliente e/ou seus representantes, sem qualquer busca por evidências. A análise resultante desta avaliação não pode vincular a Câmara de Cibersegurança por qualquer omissão ou erro que se deva a qualquer pessoa envolvida ou a terceiros.

## Referências

1. ISO/IEC 27005 (2011), Gestão de Riscos de Segurança da Informação.
2. <http://www.iso.org/iso/fr/catalogue_detail?csnumber=56742>. A norma ISO 27005 explica em detalhes como conduzir a avaliação e o tratamento de riscos, no contexto da segurança da informação

## Siglas/Glossário

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

**Confidencialidade**: Propriedade de informações que não devem ser disponibilizadas ou divulgadas a 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.

**LGPDWEB**: Método de Análise de Risco WEB.

## Descrição do Método de Análise de Riscos LGPDWEB

O LGPDWEB simplifica a gestão de riscos, oferecendo uma solução de gerenciamento de riscos e até mesmo governança de segurança da informação, com base no estado da arte no campo. Permite que a análise seja realizada em um curto espaço de tempo a partir de modelos existentes e personalizáveis, mantendo-se em conformidade com a norma internacional ISO/IEC 27005:2011.

O LGDWEB é baseado em uma biblioteca de modelos de risco que oferece objetos compostos por cenários de risco por ativo ou grupo de ativos. Essa abordagem facilita o gerenciamento dos riscos mais comuns e permite maior objetividade e eficiência. Como o LGPDWEB é completamente iterativo, esses resultados podem ser aprofundados e ajustados à maturidade de cada organização, aumentando a granularidade dos cenários de risco.

**Definindo o contexto**

Esta 1ª etapa tem como objetivo fazer um balanço do contexto, questões e prioridades específicas da empresa ou organização que deseja analisar seus riscos.

Em particular, trata-se de identificar as atividades essenciais e os processos críticos da empresa, a fim de direcionar a análise de risco para os elementos mais importantes. Para isso, é organizada uma reunião de kick-off com membros da administração e pessoas-chave. O objetivo é descobrir o que faz a empresa viver e o que pode destruí-la, identificar processos-chave, ameaças internas e externas, vulnerabilidades organizacionais, técnicas e humanas.

**Modelagem de contexto**

Essa fase inclui a modelagem de árvores de objetos. Os ativos foram definidos na fase anterior. Eles agora devem ser detalhados e formalizados em um diagrama que represente suas interdependências.

Os impactos são definidos ao nível dos ativos primários (serviços ou informação). Os ativos secundários herdam o impacto do ativo primário ao qual estão anexados (árvore de objetos).

É possível modificar manualmente os impactos no nível do ativo secundário.

**Avaliação e tratamento de risco**

A avaliação consiste em quantificar ameaças, vulnerabilidades e impactos para calcular riscos.

Para isso, é necessário ter informações de qualidade sobre a probabilidade exata de ameaças, a facilidade com que as vulnerabilidades podem ser exploradas e os impactos potenciais... Por isso, é importante contar com métricas que foram validadas por especialistas.

Quando a avaliação dos riscos identifica um risco acima do nível aceitável (grelha de aceitação do risco), devem ser tomadas medidas para fazer face a esse risco, a fim de reduzir o risco para um nível aceitável.

**Implementação & Monitoramento**

Uma vez realizado o primeiro tratamento de risco, é necessário entrar em uma fase de gestão contínua da segurança com monitoramento e controle recorrentes das medidas de segurança, a fim de poder melhorá-las de forma sustentável.

Esta 4ª fase também possibilita otimizar continuamente a segurança, aumentando a granularidade dos objetos utilizados ou ampliando o escopo da análise de risco.

# Definindo o contexto

## Descrição do contexto

A organização da gestão dos riscos na prefeitura é fundamental para garantir a segurança e integridade dos sistemas de informação e dados.

Diante da evolução constante da atividade pública e da crescente digitalização de serviços, torna-se essencial adotar uma abordagem proativa e estruturada para identificar, avaliar e mitigar os riscos associados.

A gestão de riscos deve ser integrada às práticas de governança da organização, alinhando-se às estratégias e objetivos institucionais.

É necessário estabelecer políticas claras, procedimentos e controles de segurança da informação que atendam às regulamentações específicas, como a proteção de dados pessoais e informações de saúde.

Os processos de negócios críticos, como gestão financeira, cadastros de cidadãos e sistemas de saúde, devem receber atenção especial na identificação e mitigação de riscos.

A proteção da base de dados de cidadãos, considerado o ativo mais valioso, requer medidas robustas de segurança, focando na confidencialidade, integridade e disponibilidade das informações.

Além disso, é fundamental estar preparado para enfrentar ameaças variadas, como ataques cibernéticos, desastres naturais e falhas de sistemas, desenvolvendo planos de resposta a incidentes e estratégias de recuperação de desastres.

O ambiente geográfico da região também deve ser considerado, implementando medidas de prevenção e preparação para riscos como inundações e tempestades.

Em suma, a organização da gestão dos riscos requer uma abordagem holística, envolvendo todos os níveis da organização, para garantir a resiliência operacional e a proteção dos ativos e informações críticas da prefeitura.

## Definição dos critérios de avaliação de impacto

### Riscos à Informação

### Escala de impacto

A tabela abaixo representa a escala de impacto e consequências que um risco pode ter na instituição. 0 não é impacto, por isso não tem risco.

| **Nível** | **Impacto** | | | **Consequências** |
| --- | --- | --- | --- | --- |
| **Confidencialidade** | **Integridade** | **Disponibilidade** |
| 0 | Nenhum impacto. O critério de confidencialidade não é importante | Nenhum impacto. O critério de integridade não é importante. | Nenhum impacto. O critério de disponibilidade não é importante |
| 1 | Impacto baixo e insignificante A divulgação é desfavorável aos interesses da organização Exemplos: - Divulgação de informações internas que não devem sair da organização - Memorando - Lista telefônica interna | Impacto baixo e insignificante Corrupção fácil de corrigir e sem grandes consequências. Exemplos: - Correio interno, email interno | Impacto baixo e insignificante Indisponibilidade irritante, mas ainda não prejudicial para as partes interessadas |
| 2 | Impacto médio, aceitável A divulgação prejudica os interesses da organização Exemplos: - Divulgação de informações moderadamente sensíveis restritas a um grupo de pessoas - diagrama de rede interna - Documentação ou programa fonte não | Impacto médio, aceitável Corrupção causando inconvenientes moderados às partes interessadas. A recuperação é fácil. Exemplos: - Site informativo | Impacto médio, aceitável Indisponibilidade causando transtornos moderados às partes interessadas. Exemplos: - Prazos máximos considerados insuportáveis ​​ainda não atingidos |
| 3 | Impacto grave, difícil de suportar A divulgação prejudica gravemente os interesses da organização Exemplos: - Divulgação de informações confidenciais - Sigilo bancário - Dados pessoais sensíveis - Incidentes de segurança | Impacto muito sério e insuportável Corrupção não recuperável que leva à indisponibilidade permanente | Impacto sério, difícil de suportar Indisponibilidade causando transtornos consideráveis ​​às partes interessadas. Exemplos: - Atingir prazos máximos considerados insuportáveis |
| 4 | Impacto muito sério e insuportável A divulgação é quase insuperavelmente prejudicial aos interesses da organização. Exemplos: - Divulgação de informações secretas ou muito sensíveis - Informações classificadas por lei | Impacto muito sério e insuportável Corrupção não recuperável que leva à indisponibilidade permanente | Impacto muito sério e insuportável Indisponibilidade que exige um esforço de recuperação muito grande, mesmo permanente. Exemplos: - Grandes ultrapassagens de prazos máximos |

### Escala de ameaças

A tabela abaixo representa a escala de probabilidade de uma ameaça.

| **Nível** | **Comentário** |
| --- | --- |
| 0 | Impossível |
| 1 | Pouco provável |
| 2 | Improvável |
| 3 | Pode acontecer de vez em quando |
| 4 | Muito provável |

### Escala de vulnerabilidades

A tabela abaixo representa a escala de vulnerabilidade do ativo em questão. A qualificação da vulnerabilidade leva em conta as medidas de segurança em vigor.

| **Nível** | **Comentário** |
| --- | --- |
| 0 | Sem vulnerabilidade |
| 1 | Vulnerabilidade muito baixa: Estão em vigor medidas eficazes e a sua eficácia é monitorizada. Muito boa maturidade: Boas práticas são implementadas e verificadas periodicamente. |
| 2 | Baixa vulnerabilidade: Estão em vigor medidas eficazes. Boa maturidade: Boas práticas são implementadas. |
| 3 | Vulnerabilidade normal: As medidas estão em vigor, mas ainda podem ser melhoradas. Maturidade média: Boas práticas são implementadas sem busca de melhorias. |
| 4 | Alta vulnerabilidade: As medidas estão em vigor, mas são ineficazes ou inadequadas. Baixa maturidade: Boas práticas não são implementadas, práticas primárias sem reflexão. |
| 5 | Vulnerabilidade muito elevada: não existem medidas em vigor. Maturidade muito baixa - Sem maturidade. |

### Definições de aceitação de risco

A tabela abaixo representa a tabela de cálculo de risco. As cores são meramente informativas e deverão ser aceitas e/ou modificadas pelo Conselho de Administração / Comitê de Gestão.

Vermelho : Risco inaceitável a ser enfrentado

Laranja : Risco médio que deve ou não ser tratado

Verde : Baixo risco que não requer ação

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | **TxV** | | | | | | | | | | | | | |
| **Impacto** |  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **8** | **9** | **10** | **12** | **15** | **16** | **20** |
| **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** |
| **1** | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **8** | **9** | **10** | **12** | **15** | **16** | **20** |
| **2** | **0** | **2** | **4** | **6** | **8** | **10** | **12** | **16** | **18** | **20** | **24** | **30** | **32** | **40** |
| **3** | **0** | **3** | **6** | **9** | **12** | **15** | **18** | **24** | **27** | **30** | **36** | **45** | **48** | **60** |
| **4** | **0** | **4** | **8** | **12** | **16** | **20** | **24** | **32** | **36** | **40** | **48** | **60** | **64** | **80** |

### Riscos operacionais

### Escala de impacto

| **Nível** | **Pessoa** |
| --- | --- |
| 0 | Sem impacto |
| 1 | Alguns inconvenientes que serão superados sem dificuldade (perda de tempo, repetição de procedimentos, incômodo, aborrecimento, etc.) |
| 2 | Inconveniências significativas que podem ser superadas apesar de algumas dificuldades (custos adicionais, recusa de acesso a serviços comerciais, medo, incompreensão, stress, pequenas doenças físicas, etc.) |
| 3 | Consequências significativas que devem ser superadas, mas com sérias dificuldades (desvio de dinheiro, interdição bancária, danos materiais, perda de emprego, intimação judicial, agravamento do estado de saúde, etc.) |
| 4 | Consequências significativas, mesmo irremediáveis, que podem não ser superadas (perigo financeiro, dívidas elevadas, incapacidade para o trabalho, doença psicológica ou física prolongada, morte, etc.) |

### Escala de probabilidade

| **Nível** | **Comentário** |
| --- | --- |
| 0 | Impossível |
| 1 | Pouco provável |
| 2 | Improvável |
| 3 | Pode acontecer de vez em quando |
| 4 | Muito provável |

### Definições de aceitação de risco

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | **Probabilidade** | | | | |
| **Impacto** |  | **0** | **1** | **2** | **3** | **4** |
| **0** | **0** | **0** | **0** | **0** | **0** |
| **1** | **0** | **1** | **2** | **3** | **4** |
| **2** | **0** | **2** | **4** | **6** | **8** |
| **3** | **0** | **3** | **6** | **9** | **12** |
| **4** | **0** | **4** | **8** | **12** | **16** |

## Avaliação das tendências e ameaças

A atividade da prefeitura tem evoluído com a digitalização de serviços e dependência crescente de sistemas de informação.

O contexto externo mostra avanços tecnológicos, aumento das ameaças cibernéticas e mudanças na legislação de proteção de dados.

Os principais riscos incluem ataques cibernéticos, comprometimento de dados sensíveis e desastres naturais.

A confidencialidade dos dados é crucial, e a prefeitura deve cumprir regulamentos específicos de proteção de dados  e saúde.

A tabela abaixo representa as ameaças que receberam atenção especial.

| **Ameaça** | **CID** | **Tend.** | **Prob.** | **Comentário** |
| --- | --- | --- | --- | --- |
| VPN Insegura | C | - |  | Os certificados digitais desempenham um papel crucial na segurança das comunicações VPN, especialmente no contexto de proteção contra interceptação de comunicações, comprometimento de chaves privadas e ataques de força bruta.  Os certificados digitais são usados para autenticar os participantes da comunicação VPN. Cada parte envolvida na comunicação VPN possui um certificado digital único, que é usado para verificar a identidade e a autenticidade dos participantes. Isso impede que invasores se infiltrem na rede VPN, pois os certificados digitais fornecem uma maneira confiável de verificar a identidade dos usuários e dos servidores. |
| Atividades Não Registradas | CI | + |  | O monitoramento regular dos logs permite identificar padrões incomuns de atividade na rede, como tentativas de acesso não autorizadas, tentativas de login com credenciais inválidas ou acessos a recursos não autorizados. Isso ajuda a detectar potenciais ameaças de segurança antes que elas causem danos significativos.  Resposta rápida a incidentes: Ao analisar os logs de eventos em tempo real, é possível detectar e responder rapidamente a incidentes de segurança, como ataques de malware, tentativas de intrusão ou vazamentos de dados. Isso minimiza o tempo de resposta e reduz o impacto potencial desses incidentes.  Além da segurança, o monitoramento de logs também pode ajudar a melhorar a eficiência operacional, identificando gargalos de desempenho, problemas de configuração e falhas de sistema que podem impactar a produtividade e a disponibilidade dos serviços oferecidos pelo setor público. |
| Superaquecimento | ID | + |  | Os equipamentos de TI, como servidores, switches e dispositivos de armazenamento, geram calor durante a operação. Se a temperatura ambiente dentro do data center não for controlada adequadamente, esses equipamentos podem superaquecer, o que pode levar a falhas no hardware e interrupções nos serviços. |
| Falha No Equipamento | ID | + |  | Em ambientes do setor público avaliado , como câmaras municipais, hospitais, escolas e secretarias, a disponibilidade contínua de serviços é essencial para garantir o funcionamento adequado das operações e o atendimento às necessidades da comunidade. Nesses cenários, a importância da redundância de hardware e sistemas é ainda mais evidente:  Em instituições públicas, muitos serviços são críticos e não podem ser interrompidos, como sistemas de saúde, registros municipais, sistemas educacionais, entre outros. A redundância de hardware e sistemas ajuda a garantir que esses serviços permaneçam disponíveis mesmo em caso de falha de componentes ou sistemas principais. Isso evita interrupções no fornecimento de serviços essenciais para os cidadãos.  Falhas de hardware ou sistemas podem ocorrer devido a várias razões, como falhas de energia, defeitos de componentes ou erros humanos. A presença de componentes e sistemas redundantes reduz significativamente o tempo de inatividade, permitindo uma rápida recuperação em caso de falha. Isso é especialmente crítico em ambientes onde qualquer interrupção pode afetar negativamente a segurança pública ou o bem-estar dos cidadãos. |
| Atividades Não Rastreadas | CI | ++ |  | Muitas instituições do setor público avaliado lidam com informações sensíveis, como registros de alunos, documentos legais, dados financeiros e informações de cidadãos. O monitoramento de acesso a arquivos e diretórios ajuda a garantir que apenas pessoas autorizadas tenham acesso a essas informações. Ele registra quem acessou, modificou ou excluiu arquivos e diretórios, permitindo que qualquer atividade suspeita seja identificada e investigada.  O monitoramento de acesso a arquivos e diretórios ajuda a garantir a conformidade com essas regulamentações, fornecendo registros detalhados de todas as atividades relacionadas aos dados sensíveis. Isso é especialmente importante em setores como educação e governo, onde a conformidade com leis de proteção de dados é essencial. |
| Falhas Não Detectadas | CI | + |  | Instituições do setor público avaliado lidam com uma variedade de informações sensíveis, incluindo dados pessoais de cidadãos, registros financeiros e informações governamentais. O monitoramento de segurança em tempo real ajuda a identificar tentativas de acesso não autorizado a esses dados, garantindo sua proteção contra vazamentos e uso indevido.  O uso de ferramentas de monitoramento em tempo real permite detectar atividades suspeitas ou padrões incomuns na rede ou nos sistemas. Isso inclui tentativas de invasão, malware, phishing e outras ameaças cibernéticas. Identificar essas ameaças precocemente ajuda a tomar medidas corretivas antes que causem danos significativos. |
| Tráfego Não Filtrado | CID | ++ |  | O firewall de borda desempenha um papel crucial na proteção da rede de uma organização contra ameaças externas e no controle do tráfego de dados que entra e sai da rede, especialmente em relação à implementação de filtros que bloqueiam ou monitoram o acesso a sites maliciosos, conteúdo impróprio ou não relacionado ao trabalho:  O firewall de borda atua como a primeira linha de defesa contra ameaças externas, como ataques de hackers, malware e phishing. Ele examina o tráfego de entrada para identificar e bloquear tentativas de acesso não autorizado à rede, impedindo assim que ameaças prejudiciais atinjam os sistemas internos.  Os firewalls de borda podem ser configurados para implementar filtros que bloqueiam o acesso a sites conhecidos por hospedar malware, phishing ou outras formas de conteúdo malicioso. Isso protege os usuários da rede contra downloads involuntários de software malicioso ou exposição a sites que podem comprometer a segurança dos sistemas. |
| Usuários Não Gerenciados | I | ++ |  | A implementação de um sistema centralizado, como o Active Directory (AD), para gerenciar e controlar as identidades dos usuários:  Um sistema centralizado de gestão de identidade e acesso permite que as organizações estabeleçam políticas de segurança consistentes em toda a infraestrutura de TI. Isso inclui a aplicação de políticas de senha fortes, autenticação de dois fatores e controle granular de acesso a recursos. Ao garantir que apenas usuários autorizados tenham acesso aos sistemas e dados relevantes, a organização pode reduzir significativamente o risco de violações de segurança e acesso não autorizado.  A capacidade de rastrear e auditar atividades de usuários é fundamental para a conformidade com regulamentos de segurança e privacidade, bem como para investigações de incidentes de segurança. Um sistema centralizado de IAM fornece registros detalhados de atividades de usuários, permitindo que as organizações monitorem o acesso aos recursos e identifiquem qualquer comportamento suspeito ou não autorizado. |
| Vulnerabilidades Não Identificadas | CID | - |  | Muitas organizações do setor público avaliado lidam com uma quantidade considerável de dados sensíveis, como informações de pacientes em hospitais, dados pessoais de alunos em escolas e dados confidenciais de cidadãos em câmaras municipais. A realização regular de testes de segurança e auditorias ajuda a identificar vulnerabilidades que poderiam comprometer a segurança desses dados, garantindo que medidas adequadas sejam tomadas para protegê-los.  Cumprimento de Regulamentações: As organizações do setor público avaliado estão sujeitas a uma série de regulamentações e normas de segurança, como a LGPD (Lei Geral de Proteção de Dados) no Brasil. A realização de testes de segurança e auditorias ajuda a garantir que essas organizações estejam em conformidade com as exigências legais e regulatórias, evitando possíveis penalidades e danos à reputação. |
| Uso Indevido de Dispositivos de Rede ou Dispositivo Não Autorizado | CI | ++ |  | A gestão de dispositivos de rede é de extrema importância para garantir a segurança e eficiência das operações de uma entidade.  A gestão eficaz dos dispositivos de rede permite identificar e autorizar apenas os dispositivos autorizados a se conectarem à infraestrutura da entidade. Isso ajuda a prevenir a entrada de dispositivos não autorizados que possam representar uma ameaça à segurança da rede, como dispositivos comprometidos por malware ou invasores.  Um inventário detalhado dos dispositivos de rede facilita o monitoramento e controle desses dispositivos. Administradores de rede podem acompanhar o status, configurações e atividades dos dispositivos, permitindo uma resposta rápida a quaisquer problemas ou ameaças que possam surgir. |
| Uso Indevido de Dispositivos Móveis | CI | + |  | O controle de dispositivos móveis é crucial para garantir a segurança e proteção dos dados sensíveis. Dispositivos móveis, como smartphones e tablets, são frequentemente perdidos ou roubados. O controle de dispositivos móveis permite que as organizações implementem medidas de segurança, como a capacidade de rastrear dispositivos perdidos ou roubados, bloquear remotamente seu acesso e até mesmo limpar os dados armazenados neles para evitar acesso não autorizado. |
| Falha No Fornecimento de Energia | ID | + |  | A importância da redundância de energia em ambientes do setor público avaliado é fundamental para garantir a continuidade operacional e a prestação de serviços essenciais, mesmo em situações de falha na fonte principal de energia:  Em instituições públicas, a interrupção dos serviços devido a falhas de energia pode ter impactos significativos na comunidade local. A redundância de energia garante que esses serviços permaneçam disponíveis, mesmo durante falhas na fonte principal de energia, garantindo o funcionamento contínuo das atividades essenciais. |
| Acesso não Verificado | CID | - |  | O 2FA, ou Autenticação de Dois Fatores, pode ser eficaz em caso de um ataque de phishing porque adiciona uma camada adicional de segurança além das credenciais de login usuais, como nome de usuário e senha. |
| Movimentação Lateral | CID | - |  | A segmentação de rede é essencial em ambientes do setor público avaliado , como câmaras municipais, hospitais, escolas e secretarias.  Muitas organizações do setor público avaliado lidam com dados sensíveis, como informações de saúde, dados financeiros e registros pessoais. A segmentação da rede ajuda a proteger esses dados, limitando o acesso apenas aos usuários autorizados em segmentos específicos da rede. Isso reduz significativamente o risco de acesso não autorizado e vazamento de informações confidenciais.  Resposta a Ataques: Em caso de um possível ataque cibernético, a segmentação de rede ajuda a limitar a propagação do ataque. Ao dividir a rede em segmentos menores, é possível isolar as partes afetadas do restante da rede, impedindo que o ataque se espalhe e cause danos adicionais. Isso permite uma resposta mais eficaz e rápida ao incidente de segurança, minimizando o impacto sobre os serviços essenciais oferecidos pelo setor público. |
| Acesso Não Autorizado a Instalações Físicas | CI | + |  | O controle de acesso físico é essencial para garantir a segurança de instalações e equipamentos, impedindo que pessoas não autorizadas entrem em áreas restritas. Isso é fundamental para proteger instalações contra invasões, roubos e danos causados por indivíduos mal-intencionados. |
| Acesso Indiscrimidado | CI | + |  | O controle de acesso lógico é essencial para proteger sistemas de informações e dados confidenciais contra violações, ataques de credenciais e acessos não autorizados  O controle de acesso lógico permite que as organizações implementem políticas de acesso granulares, determinando quem tem permissão para acessar quais recursos. Isso ajuda a garantir que apenas usuários autorizados possam acessar informações sensíveis e aplicativos críticos, prevenindo violações de políticas de acesso. |
| Danos à Infraestrutura | CID | - |  | A importância de considerar a perda ambiental, que inclui eventos como incêndios, inundações, poluição por poeira e sujeira, é vital para garantir a continuidade das operações e a segurança dos funcionários e do público em geral.   Eventos ambientais como incêndios e inundações podem representar sérios riscos à segurança dos funcionários e do público que frequentam essas instalações. A fumaça tóxica, a falta de acesso seguro e outras consequências desses eventos podem colocar em perigo a vida e a saúde das pessoas. Portanto, é crucial desenvolver planos de evacuação e procedimentos de segurança para lidar com emergências ambientais e garantir a segurança de todos os envolvidos.  Continuidade dos serviços públicos: As câmaras municipais, escolas e secretarias desempenham um papel vital na prestação de serviços públicos à comunidade. Qualquer evento ambiental que torne essas instalações inutilizáveis pode interromper a prestação desses serviços, causando inconvenientes para os cidadãos e prejudicando a confiança no governo local. Portanto, é importante implementar estratégias de resiliência e recuperação para garantir a continuidade dos serviços públicos, mesmo diante de eventos ambientais adversos. |
| Invasão Física | CID | - |  | A implementação de medidas de segurança física, como câmeras de vigilância, controle de acesso físico e alarmes, ajuda a proteger esses ativos de informação contra roubo, vandalismo e acesso não autorizado.  Prevenção de Acesso Não Autorizado: O controle de acesso físico, por meio de medidas como cartões de acesso, crachás, fechaduras simples ou eletrônicas, portões controlados ou uma pessoa responsável pelo fluxo de pessoas, impede que pessoas não autorizadas entrem em áreas restritas onde estão armazenados dados sensíveis. Isso reduz significativamente o risco de violações de segurança e vazamento de informações. |
| Ataques Não Detectados | CID | + |  | O monitoramento de atividades de rede e a utilização de ferramentas e sistemas de detecção de intrusão (IDS/IPS):  Prevenção de invasões: As câmaras municipais, escolas e secretarias são frequentemente alvos de ataques cibernéticos, devido à natureza das informações que possuem. O uso de sistemas de detecção de intrusão permite detectar e bloquear tentativas de invasão antes que os invasores possam causar danos significativos à rede ou aos sistemas.  Melhoria da conscientização em segurança: Ao implementar sistemas de monitoramento de atividades de rede e IDS/IPS, as organizações do setor público avaliado também promovem uma cultura de segurança cibernética entre seus funcionários e usuários. Isso pode levar a uma maior conscientização sobre as ameaças cibernéticas e a adoção de práticas de segurança mais robustas em toda a organização. |
| Proteção contra ataques de Força Bruta | CID | ++ |  | Devido à sensibilidade e à confidencialidade dos dados e sistemas envolvidos é vital implementar medidas de proteção contra esse tipo de ataque.  Ataques de força bruta podem comprometer a integridade dos sistemas, causando danos à infraestrutura de TI e interrompendo os serviços essenciais oferecidos pelas organizações do setor público avaliado . Ao implementar medidas de proteção contra esses ataques, as organizações podem reduzir o risco de interrupções e manter a estabilidade dos sistemas.  Um ataque de força bruta bem-sucedido pode permitir que invasores acessem informações confidenciais ou executem atividades maliciosas dentro dos sistemas das organizações do setor público avaliado . Limitar o número de tentativas de login e impedir esses ataques ajuda a prevenir o acesso não autorizado e protege os recursos e dados da organização. |
| Senhas Fracas | CID | ++ |  | Senhas fortes e trocas regulares dificultam que invasores acessem sistemas e informações confidenciais. Isso é especialmente importante em organizações governamentais, onde os dados podem ser alvo de ataques cibernéticos por parte de agentes maliciosos. |
| Acesso a Conteúdo Malicioso | I | + |  | O filtro de conteúdo web é uma ferramenta vital para garantir a segurança, produtividade e conformidade nas organizações:  Um filtro de conteúdo web pode bloquear o acesso a sites maliciosos conhecidos, como páginas que hospedam malware, phishing ou outros tipos de ameaças cibernéticas.   Isso protege os dispositivos e a rede da organização contra infecções por malware e ataques de phishing, reduzindo o risco de comprometimento da segurança.  Ao bloquear o acesso a sites que possam representar riscos de vazamento de informações confidenciais, como sites de compartilhamento de arquivos ou redes sociais não autorizadas, o filtro de conteúdo web ajuda a proteger os dados sensíveis da empresa contra exposição não autorizada. |
| Uso Inseguro | CID | + |  | As políticas de Uso Aceitável desempenham um papel crucial em ambientes do setor público avaliado  As políticas de Uso Aceitável estabelecem diretrizes claras sobre como os recursos de informação da entidade podem ser utilizados de forma segura. Isso inclui orientações sobre o manuseio adequado de dados confidenciais, prevenção de acesso não autorizado e proteção contra ameaças cibernéticas.  Essas políticas definem padrões para o uso e a divulgação de informações pessoais dos cidadãos e funcionários. Ao estabelecer restrições sobre como os dados podem ser coletados, armazenados e compartilhados, as políticas de Uso Aceitável garantem a conformidade com regulamentos de privacidade e protegem a privacidade dos indivíduos. |
| Conexão Interrompida | ID | + |  | A importância da redundância de link de internet em ambientes do setor público avaliado é fundamental para garantir a continuidade das operações e serviços essenciais.  Em ambientes do setor público avaliado , muitas operações e serviços dependem da conectividade à internet. Ter dois links de internet permite que as organizações continuem funcionando normalmente, mesmo se um dos links falhar. Isso evita interrupções nos serviços prestados à comunidade e garante que as atividades administrativas e operacionais possam continuar sem problemas. |

# 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 das consequências

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** | | |
| --- | --- | --- | --- | --- | --- |

# Avaliação e tratamento de riscos

O resultado da coleta de informações, codificações e avaliações diversas são processados na ferramenta LGPDWEB e ficam à disposição do cliente. Algumas dessas informações também podem ser encontradas no anexo deste documento.

O restante deste capítulo apresenta os resultados e recomendações que finalizam essa análise de risco.

## Resumo da avaliação de riscos

Principais Componentes da Avaliação de Risco:  [1] Identificação de Riscos:  • Riscos Tecnológicos: Falta de análise de vulnerabilidades, ataques cibernéticos, falhas de sistemas.  • Riscos Físicos: Desastres naturais (inundações, incêndios), falhas na infraestrutura.  • Riscos Humanos: Erros humanos, corrupção, falta de treinamento adequado.  [2] Impacto dos Riscos:  • Reputacional: Danos à imagem pública e perda de confiança da comunidade.  • Operacional: Interrupções nos serviços públicos, perda de produtividade.  • Jurídico: Consequências legais, multas, processos judiciais.  • Financeiro: Custos elevados para mitigar danos, redução do orçamento.  [3] Classificação dos Impactos:  • Baixo: Impacto mínimo, serviços não críticos afetados.  • Médio: Impacto moderado, serviços importantes afetados.  • Alto: Impacto significativo, serviços críticos interrompidos.  [4] Prioridade dos Riscos:  • Riscos são priorizados com base na probabilidade de ocorrência e na severidade do impacto.  [5] Mitigação dos Riscos:  • Medidas Preventivas: Implementação de sistemas de segurança, treinamento de funcionários, manutenção regular da infraestrutura.  • Planos de Contingência: Desenvolvimento de planos de resposta a emergências, backups de dados, comunicação eficaz durante crises.  [6] Monitoramento Contínuo:  • Revisão e atualização contínua das medidas de mitigação e dos planos de contingência para se adaptar a novos riscos e mudanças no ambiente externo.

### Riscos de Informação

A lista de riscos abordados é fornecida em anexo. Enumera 10 risco(s) do(s) qual(is):

  - 2 risco(s) crítico(s) a tratar como prioridade

  - 1 risco(s) médio(s) a ser(em) parcialmente tratado(s)

  - 7 baixo(s) risco(s) insignificante(s)

### Riscos Operacionais

A lista de riscos abordados é fornecida em anexo. Enumera 10 risco(s) do(s) qual(is):

  - 2 risco(s) crítico(s) a tratar como prioridade

  - 3 risco(s) médio(s) a ser(em) parcialmente tratado(s)

  - 5 baixo(s) risco(s) insignificante(s)

## Tratamento de riscos

### Tipo de tratamento

|  |
| --- |
| **Redução** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Itens** | **Impacto** | | | **Ameaça** | | **Vulnerabilidade** | | | **Risco atual** | | | **Risco residual** |
| **C** | **I** | **D** | **Etiqueta** | **Prob.** | **Etiqueta** | **Controles existentes** | **Qualif.** | **C** | **I** | **D** |
| Riscos de Informação > Antivírus e Antimalware | 4 | 1 | 2 | Infecção Por Vírus ou Malware | 4 | Ausência de Antivírus e Antimalware | Antivírus XPTY em uso mas em versão que não é a mais recente. | 2 | **32** | **8** | **16** | **32** |
| Riscos de Informação > Treinamento de Conscientização em Segurança | 2 | 2 | 2 | Conduta Indevida Por Falta de Conscientização | 1 | Ausência de Treinamento de Conscientização em Segurança | Possui campanhas periódicas para o treinamento em segurança da informação. | 0 |  | **0** |  | **0** |

|  |
| --- |
| **Negado** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Itens** | **Impacto** | | | **Ameaça** | | **Vulnerabilidade** | | | **Risco atual** | | | **Risco residual** |
| **C** | **I** | **D** | **Etiqueta** | **Prob.** | **Etiqueta** | **Controles existentes** | **Qualif.** | **C** | **I** | **D** |
| Riscos de Informação > Perda Ambiental (fogo, água, poeira, sujeira, etc.) | 3 | 3 | 3 | Danos à Infraestrutura | 2 | Ausência de Controles Relacionados a Perda Ambiental (fogo, água, poeira, sujeira, etc.) | Não possuem controles aplicados para o risco de informação identificado | 1 | **6** | **6** | **6** | **6** |

|  |
| --- |
| **Aceito** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Itens** | **Impacto** | | | **Ameaça** | | **Vulnerabilidade** | | | **Risco atual** | | | **Risco residual** |
| **C** | **I** | **D** | **Etiqueta** | **Prob.** | **Etiqueta** | **Controles existentes** | **Qualif.** | **C** | **I** | **D** |
| Riscos de Informação > Backup e Recuperação de Dados | 3 | 3 | 3 | Perda Permanente de Informações | 1 | Ausência de Backup e Recuperação de Dados | Empresa XPTO | 1 |  | **3** | **3** | **3** |
| Riscos de Informação > Sistema de Refrigeração | 4 | 3 | 3 | Superaquecimento | 2 | Ausência de Sistema de Refrigeração | Não possuem controles aplicados para o risco de informação identificado | 0 |  | **0** | **0** | **0** |

|  |
| --- |
| **Partilhado** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Itens** | **Impacto** | | | **Ameaça** | | **Vulnerabilidade** | | | **Risco atual** | | | **Risco residual** |
| **C** | **I** | **D** | **Etiqueta** | **Prob.** | **Etiqueta** | **Controles existentes** | **Qualif.** | **C** | **I** | **D** |
| Riscos de Informação > Políticas de Uso Aceitável | 1 | 1 | 1 | Uso Inseguro | 3 | Ausência de Políticas de Uso Aceitável | Política vigente que abrange o uso aceitável de ativos. | 1 | **3** | **3** | **3** | **3** |
| Riscos de Informação > Políticas de Segurança da Informação | 1 | 1 | 1 | Violações de Conformidade | 4 | Ausência de Políticas de Segurança da Informação | Política vigente que abrange os controles de Segurança da Informação | 0 | **0** | **0** | **0** | **0** |

### Plano de tratamento

A tabela a seguir contém as principais recomendações da análise de risco e do plano de tratamento de risco. A avaliação e a formulação de recomendações baseiam-se na seguinte escala:

●●● : Recomendação prioritária.

●● : Uma recomendação que requer uma ação dedicada para lidar com uma vulnerabilidade ou práticas recomendadas que estão faltando.

● : Indicação útil para segurança, conselhos.

#### Riscos da informação

| **Itens** | **Ameaça** | **Vulnerabilidade** | **Controles existentes** | **Risco atual** | | | **Tratamento** | **Risco residual** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **C** | **I** | **D** |
| **●● CR-21 - 8.3.2 Descarte de Mídias** | | | | | | | | |
| Riscos de Informação > Controle de Remoção de Dados | Vazamento de Dados Não Removidos | Ausência de Controle de Remoção de Dados | Não possuem controles aplicados para o risco de informação identificado | **0** | **0** |  | Não tratado | **0** |
| **●● TA-12 - 12.7.1 Controles de auditoria de sistemas de informação** | | | | | | | | |
| Riscos de Informação > Testes de Segurança e Auditorias | Vulnerabilidades Não Identificadas | Ausência de Testes de Segurança e Auditorias | Não possuem controles aplicados para o risco de informação identificado | **32** | **32** | **32** | Não tratado | **32** |
| **●●● PA-33 - 11.1.4 Proteção contra ameaças externas e do meio ambiente** | | | | | | | | |
| Riscos de Informação > Perda Ambiental (fogo, água, poeira, sujeira, etc.) | Danos à Infraestrutura | Ausência de Controles Relacionados a Perda Ambiental (fogo, água, poeira, sujeira, etc.) | Não possuem controles aplicados para o risco de informação identificado | **6** | **6** | **6** | Negado | **6** |
| **●●● PSI-01 - 5.1.1 Políticas para segurança da informação** | | | | | | | | |
| Riscos de Informação > Antivírus e Antimalware | Infecção Por Vírus ou Malware | Ausência de Antivírus e Antimalware | Antivírus XPTY em uso mas em versão que não é a mais recente. | **32** | **8** | **16** | Redução | **32** |
| **●● BR-07 - 12.3 Cópias de Segurança** | | | | | | | | |
| Riscos de Informação > Perda Ambiental (fogo, água, poeira, sujeira, etc.) | Danos à Infraestrutura | Ausência de Controles Relacionados a Perda Ambiental (fogo, água, poeira, sujeira, etc.) | Não possuem controles aplicados para o risco de informação identificado | **6** | **6** | **6** | Negado | **6** |
| Riscos de Informação > Backup e Recuperação de Dados | Perda Permanente de Informações | Ausência de Backup e Recuperação de Dados | Empresa XPTO |  | **3** | **3** | Aceito | **3** |
| **●● AV-18 - 14.1.1 Análise e Especificação dos Requisitos de Segurança da Informação** | | | | | | | | |
| Riscos de Informação > Antivírus e Antimalware | Infecção Por Vírus ou Malware | Ausência de Antivírus e Antimalware | Antivírus XPTY em uso mas em versão que não é a mais recente. | **32** | **8** | **16** | Redução | **32** |
| **● SF-28 - 11 Segurança física e do ambiente** | | | | | | | | |
| Riscos de Informação > Perda Ambiental (fogo, água, poeira, sujeira, etc.) | Danos à Infraestrutura | Ausência de Controles Relacionados a Perda Ambiental (fogo, água, poeira, sujeira, etc.) | Não possuem controles aplicados para o risco de informação identificado | **6** | **6** | **6** | Negado | **6** |
| **● RE-26 - 11.2.2 Utilidades** | | | | | | | | |
| Riscos de Informação > Redundância de Link de Internet | Conexão Interrompida | Ausência de Redundância de Link de Internet | Não possuem controles aplicados para o risco de informação identificado |  | **12** | **16** | Não tratado | **16** |
| Riscos de Informação > Sistema de Refrigeração | Superaquecimento | Ausência de Sistema de Refrigeração | Não possuem controles aplicados para o risco de informação identificado |  | **0** | **0** | Aceito | **0** |
| **● TS-09 - 7.2.2 Conscientização, educação e treinamento em segurança da informação** | | | | | | | | |
| Riscos de Informação > Treinamento de Conscientização em Segurança | Conduta Indevida Por Falta de Conscientização | Ausência de Treinamento de Conscientização em Segurança | Possui campanhas periódicas para o treinamento em segurança da informação. |  | **0** |  | Redução | **0** |
| Riscos de Informação > Políticas de Segurança da Informação | Violações de Conformidade | Ausência de Políticas de Segurança da Informação | Política vigente que abrange os controles de Segurança da Informação | **0** | **0** | **0** | Partilhado | **0** |
| **● PU-20 - 8.1.3 Uso aceitável dos ativos** | | | | | | | | |
| Riscos de Informação > Políticas de Uso Aceitável | Uso Inseguro | Ausência de Políticas de Uso Aceitável | Política vigente que abrange o uso aceitável de ativos. | **3** | **3** | **3** | Partilhado | **3** |

#### Riscos operacionais

| **Itens** | **Descrição do risco** | **Controles existentes** | **Risco atual** | **Tratamento** | **Risco residual** |
| --- | --- | --- | --- | --- | --- |

# Anexo A : Entrevista e coleta de informação

As informações utilizadas para a realização da análise foram coletadas por meio de entrevistas com pessoas-chave do negócio e gestores técnicos.

Gostaríamos de agradecer aos seguintes departamentos e áreas por sua contribuição ativa durante as entrevistas e visitas realizadas como parte de nossa missão listadas abaixo:

# Anexo B : Avaliação das tendências

|  |
| --- |
| **Qual é o propósito da estrutura governamental em questão?** |
| Atender às necessidades da comunidade local. Isso inclui fornecer serviços públicos essenciais, como educação, saúde, transporte, segurança pública, infraestrutura e serviços sociais, além de administrar questões relacionadas ao planejamento urbano, desenvolvimento econômico e cultural, entre outros. |
| **Como tem sido a evolução das atividades do setor público nos últimos anos?** |
| Uma maior digitalização de serviços, a adoção de práticas de governança mais transparentes e participativas, e uma ênfase crescente na eficiência, responsabilidade e sustentabilidade. |
| **Como tem evoluído o contexto externo que afeta o setor público, incluindo aspectos como concorrência entre órgãos públicos, desenvolvimento do mercado, e mudanças na legislação?** |
| Tem sido marcado por uma maior competição entre órgãos públicos e a pressão por eficiência e eficácia na prestação de serviços. Além disso, mudanças na legislação, como regulamentações relacionadas à proteção de dados e transparência governamental, têm impactado as práticas e políticas do setor público. |
| **Quais podem ser os motivos por trás de potenciais ataques ou ameaças à segurança do setor público, como questões financeiras, disputas políticas, vingança, ou interesse em obter vantagens econômicas?** |
| - Dinheiro - Vingança (ex-interna, externa) - Vantagem política - Espionagem econômica |
| **Quais são os processos mais críticos para o funcionamento do setor público em questão?** |
| A gestão financeira, prestação de serviços essenciais, gestão de recursos humanos, segurança pública, planejamento urbano e desenvolvimento econômico. |
| **Qual é o ativo mais valioso que o setor público possui?** |
| O ativo mais valioso que o setor público possui são dados dos cidadãos, e o gerenciamento financeiro do município para prestar serviços de forma eficaz. |
| **Qual é o critério mais importante para a segurança e proteção das atividades e dados do setor público?** |
| O critério mais importante é garantir a confidencialidade, integridade e disponibilidade dos dados e sistemas, além de implementar medidas robustas de segurança cibernética e proteção física. |
| **O setor público está sujeito a cumprir leis, normas e regulamentos específicos, como legislação relacionada à segurança de informações sensíveis ou à prestação de serviços essenciais?** |
| Diversas legislações como as relacionadas à segurança de informações sensíveis, proteção de dados pessoais e prestação de serviços essenciais à comunidade. |
| **Qual é a maior ameaça que o setor público enfrenta atualmente?** |
| Uma das maiores ameaças que o setor público enfrenta atualmente é a cibersegurança, incluindo ataques cibernéticos direcionados a sistemas e dados governamentais. |
| **Quais são as principais preocupações que podem potencialmente afetar negativamente o funcionamento do setor público?** |
| As principais preocupações incluem falta de recursos financeiros, corrupção, falta de transparência, má gestão de dados e sistemas, e pressões políticas e sociais. |
| **Houve algum incidente de desastre ou ataque cibernético que afetou o setor público?** |
| Não foi divulgado nenhum ataque à infraestrutura avaliada mas é possível que tenham ocorrido incidentes de desastre ou ataques cibernéticos visto que ocorreram interrupções de serviços essenciais e informatizados que não foram devidamente mapeados. |
| **Houve algum caso em que outros órgãos governamentais foram alvo de desastres ou ataques cibernéticos?** |
| É de conhecimento que pelo menos um município vizinho foi alvo de ataques cibernéticos. |
| **O ambiente geográfico do setor público aumenta algum tipo específico de risco, como inundação, incêndio, ou eventos climáticos extremos?** |
| Devido à localização geográfica, o setor público avaliado pode enfrentar riscos específicos, como inundações, incêndios, desastres naturais. |

# Anexo C : Avaliação das ameaças

| **Ameaça** | **CID** | **Tend.** | **Prob.** | **Comentário** |
| --- | --- | --- | --- | --- |
| Perda Permanente de Informações | ID | n |  | A realização de backup e recuperação de dados é crucial para garantir a segurança e a disponibilidade das informações digitais de uma organização  Os backups regulares ajudam a prevenir a perda de dados em caso de falhas de hardware, erros humanos, ataques de malware, desastres naturais ou outras situações imprevistas. Se os dados originais forem perdidos ou corrompidos, os backups podem ser usados para restaurar as informações perdidas. |
| VPN Insegura | C | - |  | Os certificados digitais desempenham um papel crucial na segurança das comunicações VPN, especialmente no contexto de proteção contra interceptação de comunicações, comprometimento de chaves privadas e ataques de força bruta.  Os certificados digitais são usados para autenticar os participantes da comunicação VPN. Cada parte envolvida na comunicação VPN possui um certificado digital único, que é usado para verificar a identidade e a autenticidade dos participantes. Isso impede que invasores se infiltrem na rede VPN, pois os certificados digitais fornecem uma maneira confiável de verificar a identidade dos usuários e dos servidores. |
| Atividades Não Registradas | CI | + |  | O monitoramento regular dos logs permite identificar padrões incomuns de atividade na rede, como tentativas de acesso não autorizadas, tentativas de login com credenciais inválidas ou acessos a recursos não autorizados. Isso ajuda a detectar potenciais ameaças de segurança antes que elas causem danos significativos.  Resposta rápida a incidentes: Ao analisar os logs de eventos em tempo real, é possível detectar e responder rapidamente a incidentes de segurança, como ataques de malware, tentativas de intrusão ou vazamentos de dados. Isso minimiza o tempo de resposta e reduz o impacto potencial desses incidentes.  Além da segurança, o monitoramento de logs também pode ajudar a melhorar a eficiência operacional, identificando gargalos de desempenho, problemas de configuração e falhas de sistema que podem impactar a produtividade e a disponibilidade dos serviços oferecidos pelo setor público. |
| Superaquecimento | ID | + |  | Os equipamentos de TI, como servidores, switches e dispositivos de armazenamento, geram calor durante a operação. Se a temperatura ambiente dentro do data center não for controlada adequadamente, esses equipamentos podem superaquecer, o que pode levar a falhas no hardware e interrupções nos serviços. |
| Falha No Equipamento | ID | + |  | Em ambientes do setor público avaliado , como câmaras municipais, hospitais, escolas e secretarias, a disponibilidade contínua de serviços é essencial para garantir o funcionamento adequado das operações e o atendimento às necessidades da comunidade. Nesses cenários, a importância da redundância de hardware e sistemas é ainda mais evidente:  Em instituições públicas, muitos serviços são críticos e não podem ser interrompidos, como sistemas de saúde, registros municipais, sistemas educacionais, entre outros. A redundância de hardware e sistemas ajuda a garantir que esses serviços permaneçam disponíveis mesmo em caso de falha de componentes ou sistemas principais. Isso evita interrupções no fornecimento de serviços essenciais para os cidadãos.  Falhas de hardware ou sistemas podem ocorrer devido a várias razões, como falhas de energia, defeitos de componentes ou erros humanos. A presença de componentes e sistemas redundantes reduz significativamente o tempo de inatividade, permitindo uma rápida recuperação em caso de falha. Isso é especialmente crítico em ambientes onde qualquer interrupção pode afetar negativamente a segurança pública ou o bem-estar dos cidadãos. |
| Atividades Não Rastreadas | CI | ++ |  | Muitas instituições do setor público avaliado lidam com informações sensíveis, como registros de alunos, documentos legais, dados financeiros e informações de cidadãos. O monitoramento de acesso a arquivos e diretórios ajuda a garantir que apenas pessoas autorizadas tenham acesso a essas informações. Ele registra quem acessou, modificou ou excluiu arquivos e diretórios, permitindo que qualquer atividade suspeita seja identificada e investigada.  O monitoramento de acesso a arquivos e diretórios ajuda a garantir a conformidade com essas regulamentações, fornecendo registros detalhados de todas as atividades relacionadas aos dados sensíveis. Isso é especialmente importante em setores como educação e governo, onde a conformidade com leis de proteção de dados é essencial. |
| Infecção da Rede ou Vazamento de Dados | CID | n |  | O controle de mídia removível, como pendrives e unidades USB, é de extrema importância na proteção de dados sensíveis e confidenciais de uma organização que podem ser facilmente perdidos, roubados ou usados indevidamente para transferir dados fora da rede corporativa.   Implementar políticas e tecnologias de controle de mídia removível ajuda a prevenir vazamentos de dados não autorizados, garantindo que apenas dados autorizados sejam transferidos para dispositivos externos. |
| Conduta Indevida Por Falta de Conscientização | I | n |  | Proteção de dados sensíveis: Instituições do setor público avaliado lidam com uma grande quantidade de dados sensíveis, como informações pessoais, registros médicos, dados financeiros e documentos governamentais.   O treinamento de conscientização em segurança ajuda os funcionários a entender a importância de proteger esses dados contra acesso não autorizado, manipulação ou roubo. |
| Falta de Gerenciamento de TI | CID | n |  | Vulnerabilidades Cibernéticas: Sem um responsável de TI para monitorar e atualizar regularmente os sistemas de segurança, as agências governamentais ficam mais vulneráveis a ataques cibernéticos. Isso pode resultar no comprometimento de dados confidenciais, interrupção de serviços essenciais e até mesmo ataques de ransomware.  Manutenção de Ativos Deficiente: A ausência de gerenciamento de TI pode levar à falta de manutenção adequada dos ativos de tecnologia. Isso significa que hardware e software desatualizados podem permanecer em uso, aumentando os riscos de falhas e vulnerabilidades de segurança.  Redes Inseguras: Sem uma gestão adequada, as redes governamentais podem não ser configuradas e protegidas corretamente. Isso pode resultar em brechas de segurança que podem ser exploradas por invasores. |
| Atraso na Resposta a Incidentes | CID | n |  | As organizações do setor público avaliado frequentemente lidam com dados sensíveis e pessoais de cidadãos, como informações de saúde, dados financeiros e registros educacionais.   Um plano de resposta a incidentes ajuda a proteger esses dados, garantindo que sejam detectados e tratados rapidamente em caso de violação de segurança.  Muitos serviços essenciais para a comunidade são prestados por instituições do setor público avaliado . Interrupções causadas por incidentes de segurança cibernética podem afetar a entrega desses serviços, impactando diretamente os cidadãos. Um plano de resposta a incidentes ajuda a minimizar o tempo de inatividade e a restaurar os serviços o mais rápido possível.  A confiança do público nas instituições do setor público avaliado é fundamental. Incidentes de segurança cibernética podem abalar essa confiança, especialmente se os dados dos cidadãos forem comprometidos. Ter um plano de resposta a incidentes demonstra um compromisso com a segurança e a proteção dos interesses dos cidadãos, o que ajuda a preservar a reputação e a confiança pública. |
| Falhas Não Detectadas | CI | + |  | Instituições do setor público avaliado lidam com uma variedade de informações sensíveis, incluindo dados pessoais de cidadãos, registros financeiros e informações governamentais. O monitoramento de segurança em tempo real ajuda a identificar tentativas de acesso não autorizado a esses dados, garantindo sua proteção contra vazamentos e uso indevido.  O uso de ferramentas de monitoramento em tempo real permite detectar atividades suspeitas ou padrões incomuns na rede ou nos sistemas. Isso inclui tentativas de invasão, malware, phishing e outras ameaças cibernéticas. Identificar essas ameaças precocemente ajuda a tomar medidas corretivas antes que causem danos significativos. |
| Tráfego Não Filtrado | CID | ++ |  | O firewall de borda desempenha um papel crucial na proteção da rede de uma organização contra ameaças externas e no controle do tráfego de dados que entra e sai da rede, especialmente em relação à implementação de filtros que bloqueiam ou monitoram o acesso a sites maliciosos, conteúdo impróprio ou não relacionado ao trabalho:  O firewall de borda atua como a primeira linha de defesa contra ameaças externas, como ataques de hackers, malware e phishing. Ele examina o tráfego de entrada para identificar e bloquear tentativas de acesso não autorizado à rede, impedindo assim que ameaças prejudiciais atinjam os sistemas internos.  Os firewalls de borda podem ser configurados para implementar filtros que bloqueiam o acesso a sites conhecidos por hospedar malware, phishing ou outras formas de conteúdo malicioso. Isso protege os usuários da rede contra downloads involuntários de software malicioso ou exposição a sites que podem comprometer a segurança dos sistemas. |
| Violações de Conformidade | CID | n |  | As entidades do setor público avaliado lidam com uma quantidade significativa de dados sensíveis, como informações dos cidadãos, registros financeiros e documentos governamentais. As Políticas de Segurança da Informação estabelecem diretrizes claras sobre como esses dados devem ser protegidos contra acesso não autorizado, alteração e exclusão.  O setor público está sujeito a várias leis e regulamentos relacionados à proteção de dados e privacidade. As Políticas de Segurança da Informação garantem que a entidade esteja em conformidade com essas obrigações legais, estabelecendo procedimentos para lidar com dados de acordo com as leis e regulamentos aplicáveis. |
| Usuários Não Gerenciados | I | ++ |  | A implementação de um sistema centralizado, como o Active Directory (AD), para gerenciar e controlar as identidades dos usuários:  Um sistema centralizado de gestão de identidade e acesso permite que as organizações estabeleçam políticas de segurança consistentes em toda a infraestrutura de TI. Isso inclui a aplicação de políticas de senha fortes, autenticação de dois fatores e controle granular de acesso a recursos. Ao garantir que apenas usuários autorizados tenham acesso aos sistemas e dados relevantes, a organização pode reduzir significativamente o risco de violações de segurança e acesso não autorizado.  A capacidade de rastrear e auditar atividades de usuários é fundamental para a conformidade com regulamentos de segurança e privacidade, bem como para investigações de incidentes de segurança. Um sistema centralizado de IAM fornece registros detalhados de atividades de usuários, permitindo que as organizações monitorem o acesso aos recursos e identifiquem qualquer comportamento suspeito ou não autorizado. |
| Vulnerabilidades Não Identificadas | CID | - |  | Muitas organizações do setor público avaliado lidam com uma quantidade considerável de dados sensíveis, como informações de pacientes em hospitais, dados pessoais de alunos em escolas e dados confidenciais de cidadãos em câmaras municipais. A realização regular de testes de segurança e auditorias ajuda a identificar vulnerabilidades que poderiam comprometer a segurança desses dados, garantindo que medidas adequadas sejam tomadas para protegê-los.  Cumprimento de Regulamentações: As organizações do setor público avaliado estão sujeitas a uma série de regulamentações e normas de segurança, como a LGPD (Lei Geral de Proteção de Dados) no Brasil. A realização de testes de segurança e auditorias ajuda a garantir que essas organizações estejam em conformidade com as exigências legais e regulatórias, evitando possíveis penalidades e danos à reputação. |
| Uso Indevido de Dispositivos de Rede ou Dispositivo Não Autorizado | CI | ++ |  | A gestão de dispositivos de rede é de extrema importância para garantir a segurança e eficiência das operações de uma entidade.  A gestão eficaz dos dispositivos de rede permite identificar e autorizar apenas os dispositivos autorizados a se conectarem à infraestrutura da entidade. Isso ajuda a prevenir a entrada de dispositivos não autorizados que possam representar uma ameaça à segurança da rede, como dispositivos comprometidos por malware ou invasores.  Um inventário detalhado dos dispositivos de rede facilita o monitoramento e controle desses dispositivos. Administradores de rede podem acompanhar o status, configurações e atividades dos dispositivos, permitindo uma resposta rápida a quaisquer problemas ou ameaças que possam surgir. |
| Uso Indevido de Dispositivos Móveis | CI | + |  | O controle de dispositivos móveis é crucial para garantir a segurança e proteção dos dados sensíveis. Dispositivos móveis, como smartphones e tablets, são frequentemente perdidos ou roubados. O controle de dispositivos móveis permite que as organizações implementem medidas de segurança, como a capacidade de rastrear dispositivos perdidos ou roubados, bloquear remotamente seu acesso e até mesmo limpar os dados armazenados neles para evitar acesso não autorizado. |
| Exposição a Potenciais Brechas de Segurança | CID | n |  | A análise de vulnerabilidades é crucial para garantir a segurança de sistemas de informação e redes, pois ajuda a identificar e corrigir potenciais pontos fracos que podem ser explorados por atacantes. |
| Falha No Fornecimento de Energia | ID | + |  | A importância da redundância de energia em ambientes do setor público avaliado é fundamental para garantir a continuidade operacional e a prestação de serviços essenciais, mesmo em situações de falha na fonte principal de energia:  Em instituições públicas, a interrupção dos serviços devido a falhas de energia pode ter impactos significativos na comunidade local. A redundância de energia garante que esses serviços permaneçam disponíveis, mesmo durante falhas na fonte principal de energia, garantindo o funcionamento contínuo das atividades essenciais. |
| Acesso não Verificado | CID | - |  | O 2FA, ou Autenticação de Dois Fatores, pode ser eficaz em caso de um ataque de phishing porque adiciona uma camada adicional de segurança além das credenciais de login usuais, como nome de usuário e senha. |
| Movimentação Lateral | CID | - |  | A segmentação de rede é essencial em ambientes do setor público avaliado , como câmaras municipais, hospitais, escolas e secretarias.  Muitas organizações do setor público avaliado lidam com dados sensíveis, como informações de saúde, dados financeiros e registros pessoais. A segmentação da rede ajuda a proteger esses dados, limitando o acesso apenas aos usuários autorizados em segmentos específicos da rede. Isso reduz significativamente o risco de acesso não autorizado e vazamento de informações confidenciais.  Resposta a Ataques: Em caso de um possível ataque cibernético, a segmentação de rede ajuda a limitar a propagação do ataque. Ao dividir a rede em segmentos menores, é possível isolar as partes afetadas do restante da rede, impedindo que o ataque se espalhe e cause danos adicionais. Isso permite uma resposta mais eficaz e rápida ao incidente de segurança, minimizando o impacto sobre os serviços essenciais oferecidos pelo setor público. |
| Acesso Não Autorizado a Instalações Físicas | CI | + |  | O controle de acesso físico é essencial para garantir a segurança de instalações e equipamentos, impedindo que pessoas não autorizadas entrem em áreas restritas. Isso é fundamental para proteger instalações contra invasões, roubos e danos causados por indivíduos mal-intencionados. |
| Acesso Indiscrimidado | CI | + |  | O controle de acesso lógico é essencial para proteger sistemas de informações e dados confidenciais contra violações, ataques de credenciais e acessos não autorizados  O controle de acesso lógico permite que as organizações implementem políticas de acesso granulares, determinando quem tem permissão para acessar quais recursos. Isso ajuda a garantir que apenas usuários autorizados possam acessar informações sensíveis e aplicativos críticos, prevenindo violações de políticas de acesso. |
| Danos à Infraestrutura | CID | - |  | A importância de considerar a perda ambiental, que inclui eventos como incêndios, inundações, poluição por poeira e sujeira, é vital para garantir a continuidade das operações e a segurança dos funcionários e do público em geral.   Eventos ambientais como incêndios e inundações podem representar sérios riscos à segurança dos funcionários e do público que frequentam essas instalações. A fumaça tóxica, a falta de acesso seguro e outras consequências desses eventos podem colocar em perigo a vida e a saúde das pessoas. Portanto, é crucial desenvolver planos de evacuação e procedimentos de segurança para lidar com emergências ambientais e garantir a segurança de todos os envolvidos.  Continuidade dos serviços públicos: As câmaras municipais, escolas e secretarias desempenham um papel vital na prestação de serviços públicos à comunidade. Qualquer evento ambiental que torne essas instalações inutilizáveis pode interromper a prestação desses serviços, causando inconvenientes para os cidadãos e prejudicando a confiança no governo local. Portanto, é importante implementar estratégias de resiliência e recuperação para garantir a continuidade dos serviços públicos, mesmo diante de eventos ambientais adversos. |
| Invasão Física | CID | - |  | A implementação de medidas de segurança física, como câmeras de vigilância, controle de acesso físico e alarmes, ajuda a proteger esses ativos de informação contra roubo, vandalismo e acesso não autorizado.  Prevenção de Acesso Não Autorizado: O controle de acesso físico, por meio de medidas como cartões de acesso, crachás, fechaduras simples ou eletrônicas, portões controlados ou uma pessoa responsável pelo fluxo de pessoas, impede que pessoas não autorizadas entrem em áreas restritas onde estão armazenados dados sensíveis. Isso reduz significativamente o risco de violações de segurança e vazamento de informações. |
| Ataques Não Detectados | CID | + |  | O monitoramento de atividades de rede e a utilização de ferramentas e sistemas de detecção de intrusão (IDS/IPS):  Prevenção de invasões: As câmaras municipais, escolas e secretarias são frequentemente alvos de ataques cibernéticos, devido à natureza das informações que possuem. O uso de sistemas de detecção de intrusão permite detectar e bloquear tentativas de invasão antes que os invasores possam causar danos significativos à rede ou aos sistemas.  Melhoria da conscientização em segurança: Ao implementar sistemas de monitoramento de atividades de rede e IDS/IPS, as organizações do setor público avaliado também promovem uma cultura de segurança cibernética entre seus funcionários e usuários. Isso pode levar a uma maior conscientização sobre as ameaças cibernéticas e a adoção de práticas de segurança mais robustas em toda a organização. |
| Proteção contra ataques de Força Bruta | CID | ++ |  | Devido à sensibilidade e à confidencialidade dos dados e sistemas envolvidos é vital implementar medidas de proteção contra esse tipo de ataque.  Ataques de força bruta podem comprometer a integridade dos sistemas, causando danos à infraestrutura de TI e interrompendo os serviços essenciais oferecidos pelas organizações do setor público avaliado . Ao implementar medidas de proteção contra esses ataques, as organizações podem reduzir o risco de interrupções e manter a estabilidade dos sistemas.  Um ataque de força bruta bem-sucedido pode permitir que invasores acessem informações confidenciais ou executem atividades maliciosas dentro dos sistemas das organizações do setor público avaliado . Limitar o número de tentativas de login e impedir esses ataques ajuda a prevenir o acesso não autorizado e protege os recursos e dados da organização. |
| Infecção Por Vírus ou Malware | CID | n |  | O uso de antivírus e antimalware é fundamental na proteção contra uma ampla gama de ameaças cibernéticas, incluindo vírus, worms, trojans e ransomware. |
| Vazamento de Dados Não Removidos | CI | n |  | O controle de remoção de dados é fundamental para garantir a segurança e a privacidade das informações sensíveis.   Durante o processo de remoção de dados, é importante garantir que as informações sensíveis não sejam expostas inadvertidamente a pessoas não autorizadas. Isso pode acontecer se não forem seguidos protocolos adequados durante o processo de remoção de dados, como a visualização indevida de arquivos antes de serem excluídos ou a transferência inadequada de dados para outros dispositivos. |
| Vulnerabilidades Não Corrigidas | CID | n |  | A gestão de patches é crucial para manter a segurança dos sistemas e softwares, pois garante que quaisquer vulnerabilidades conhecidas sejam corrigidas por meio da implementação de patches de segurança mais recentes.  Ignorar essas atualizações de patches pode deixar os sistemas vulneráveis a ataques de hackers que exploram essas brechas de segurança.  Muitos ataques cibernéticos exploram vulnerabilidades conhecidas em sistemas e softwares desatualizados. Ao implementar patches de segurança, as organizações reduzem significativamente o risco de exploração dessas vulnerabilidades, tornando seus sistemas menos atrativos para hackers. |
| Senhas Fracas | CID | ++ |  | Senhas fortes e trocas regulares dificultam que invasores acessem sistemas e informações confidenciais. Isso é especialmente importante em organizações governamentais, onde os dados podem ser alvo de ataques cibernéticos por parte de agentes maliciosos. |
| Acesso a Conteúdo Malicioso | I | + |  | O filtro de conteúdo web é uma ferramenta vital para garantir a segurança, produtividade e conformidade nas organizações:  Um filtro de conteúdo web pode bloquear o acesso a sites maliciosos conhecidos, como páginas que hospedam malware, phishing ou outros tipos de ameaças cibernéticas.   Isso protege os dispositivos e a rede da organização contra infecções por malware e ataques de phishing, reduzindo o risco de comprometimento da segurança.  Ao bloquear o acesso a sites que possam representar riscos de vazamento de informações confidenciais, como sites de compartilhamento de arquivos ou redes sociais não autorizadas, o filtro de conteúdo web ajuda a proteger os dados sensíveis da empresa contra exposição não autorizada. |
| Uso Inseguro | CID | + |  | As políticas de Uso Aceitável desempenham um papel crucial em ambientes do setor público avaliado  As políticas de Uso Aceitável estabelecem diretrizes claras sobre como os recursos de informação da entidade podem ser utilizados de forma segura. Isso inclui orientações sobre o manuseio adequado de dados confidenciais, prevenção de acesso não autorizado e proteção contra ameaças cibernéticas.  Essas políticas definem padrões para o uso e a divulgação de informações pessoais dos cidadãos e funcionários. Ao estabelecer restrições sobre como os dados podem ser coletados, armazenados e compartilhados, as políticas de Uso Aceitável garantem a conformidade com regulamentos de privacidade e protegem a privacidade dos indivíduos. |
| Conexão Interrompida | ID | + |  | A importância da redundância de link de internet em ambientes do setor público avaliado é fundamental para garantir a continuidade das operações e serviços essenciais.  Em ambientes do setor público avaliado , muitas operações e serviços dependem da conectividade à internet. Ter dois links de internet permite que as organizações continuem funcionando normalmente, mesmo se um dos links falhar. Isso evita interrupções nos serviços prestados à comunidade e garante que as atividades administrativas e operacionais possam continuar sem problemas. |
| Dados Desprotegidos | CI | n |  | ‭A criptografia desempenha um papel‬ crucial na proteção da privacidade,‬ ‭segurança e confidencialidade das‬ ‭informações digitais. ‭ A criptografia permite que os dados‬ ‭sejam transformados em um formato‬ ‭ilegível, conhecido como texto cifrado,‬ ‭que só pode ser decifrado por aqueles‬ ‭que possuem a chave de criptografia‬ ‭correspondente. Isso assegura que‬ ‭apenas os destinatários autorizados‬ ‭possam acessar e compreender as‬ ‭informações, protegendo a‬ ‭privacidade e confidencialidade dos‬ ‭dados. |

# Anexo D : Contexto dos ativos

# Anexo E : Proprietários dos riscos

| **Owner** | **Itens** | **Risco** | |
| --- | --- | --- | --- |
| **Partilhado entre responsável de TI e gestão do município.** | Riscos de Informação > Backup e Recuperação de Dados | Perda Permanente de Informações | Ausência de Backup e Recuperação de Dados |
| Riscos de Informação > Antivírus e Antimalware | Infecção Por Vírus ou Malware | Ausência de Antivírus e Antimalware |
| Riscos de Informação > Controle de Remoção de Dados | Vazamento de Dados Não Removidos | Ausência de Controle de Remoção de Dados |
| Riscos de Informação > Perda Ambiental (fogo, água, poeira, sujeira, etc.) | Danos à Infraestrutura | Ausência de Controles Relacionados a Perda Ambiental (fogo, água, poeira, sujeira, etc.) |
| Riscos de Informação > Políticas de Segurança da Informação | Violações de Conformidade | Ausência de Políticas de Segurança da Informação |
| Riscos de Informação > Redundância de Link de Internet | Conexão Interrompida | Ausência de Redundância de Link de Internet |
| Riscos de Informação > Testes de Segurança e Auditorias | Vulnerabilidades Não Identificadas | Ausência de Testes de Segurança e Auditorias |
| Riscos de Informação > Treinamento de Conscientização em Segurança | Conduta Indevida Por Falta de Conscientização | Ausência de Treinamento de Conscientização em Segurança |
| Riscos de Informação > Sistema de Refrigeração | Superaquecimento | Ausência de Sistema de Refrigeração |

# Anexo F : Notas e observações do analista

## Riscos da Informação

### Riscos de Informação

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Riscos de Informação > Antivírus e Antimalware** | | | | | | | | | | | | |
| 4 | 1 | 2 | Infecção Por Vírus ou Malware | 4 | Ausência de Antivírus e Antimalware | Antivírus XPTY em uso mas em versão que não é a mais recente. | 2 | **32** | **8** | **16** | Redução | **32** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Riscos de Informação > Backup e Recuperação de Dados** | | | | | | | | | | | | |
| 3 | 3 | 3 | Perda Permanente de Informações | 1 | Ausência de Backup e Recuperação de Dados | Empresa XPTO | 1 |  | **3** | **3** | Aceito | **3** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Riscos de Informação > Controle de Remoção de Dados** | | | | | | | | | | | | |
| 4 | 4 | 4 | Vazamento de Dados Não Removidos | 2 | Ausência de Controle de Remoção de Dados | Não possuem controles aplicados para o risco de informação identificado | 0 | **0** | **0** |  | Não tratado | **0** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Riscos de Informação > Perda Ambiental (fogo, água, poeira, sujeira, etc.)** | | | | | | | | | | | | |
| 3 | 3 | 3 | Danos à Infraestrutura | 2 | Ausência de Controles Relacionados a Perda Ambiental (fogo, água, poeira, sujeira, etc.) | Não possuem controles aplicados para o risco de informação identificado | 1 | **6** | **6** | **6** | Negado | **6** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Riscos de Informação > Políticas de Segurança da Informação** | | | | | | | | | | | | |
| 1 | 1 | 1 | Violações de Conformidade | 4 | Ausência de Políticas de Segurança da Informação | Política vigente que abrange os controles de Segurança da Informação | 0 | **0** | **0** | **0** | Partilhado | **0** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Riscos de Informação > Políticas de Uso Aceitável** | | | | | | | | | | | | |
| 1 | 1 | 1 | Uso Inseguro | 3 | Ausência de Políticas de Uso Aceitável | Política vigente que abrange o uso aceitável de ativos. | 1 | **3** | **3** | **3** | Partilhado | **3** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Riscos de Informação > Redundância de Link de Internet** | | | | | | | | | | | | |
| 3 | 3 | 4 | Conexão Interrompida | 4 | Ausência de Redundância de Link de Internet | Não possuem controles aplicados para o risco de informação identificado | 1 |  | **12** | **16** | Não tratado | **16** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Riscos de Informação > Sistema de Refrigeração** | | | | | | | | | | | | |
| 4 | 3 | 3 | Superaquecimento | 2 | Ausência de Sistema de Refrigeração | Não possuem controles aplicados para o risco de informação identificado | 0 |  | **0** | **0** | Aceito | **0** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Riscos de Informação > Testes de Segurança e Auditorias** | | | | | | | | | | | | |
| 4 | 4 | 4 | Vulnerabilidades Não Identificadas | 4 | Ausência de Testes de Segurança e Auditorias | Não possuem controles aplicados para o risco de informação identificado | 2 | **32** | **32** | **32** | Não tratado | **32** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Riscos de Informação > Treinamento de Conscientização em Segurança** | | | | | | | | | | | | |
| 2 | 2 | 2 | Conduta Indevida Por Falta de Conscientização | 1 | Ausência de Treinamento de Conscientização em Segurança | Possui campanhas periódicas para o treinamento em segurança da informação. | 0 |  | **0** |  | Redução | **0** |

## Riscos Operacionais

### Risco Operacional

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Risco Operacional > Elaboração, implementação e atualização da Política de Privacidade** | | | | | | |
| Inexistência de Política de Privacidade e Proteção de Dados | 4 | 4 | **16** | Não possuem controles aplicados para o risco de operacional identificado | Não tratado | **16** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Risco Operacional > Base Legal de Consentimento** | | | | | | |
| Coleta inadequada de consentimento (quando necessário) | 3 | 2 | **6** | Não possuem controles aplicados para o risco de operacional identificado | Não tratado | **6** |
| Falta de consentimento específico nos casos de tratamento de dados de crianças (0 a 12 anos incompletos) e adolescentes (12 a 18 anos) | 3 | 1 | **3** | Não possuem controles aplicados para o risco de operacional identificado | Não tratado | **3** |
| A evidência e rastreabilidade do consentimento não é adequada | 2 | 1 | **2** | Não possuem controles aplicados para o risco de operacional identificado | Não tratado | **2** |
| Inexistência de Termo de Ciência e Consentimento claro e específico quando o tratamento de dados possuir como base legal o Consentimento do Titular | 1 | 2 | **2** | Não possuem controles aplicados para o risco de operacional identificado | Não tratado | **2** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Risco Operacional > Mapeamento de Dados Pessoais** | | | | | | |
| Inexistência ou falha no Mapeamento do Fluxo de Dados Pessoais | 1 | 2 | **2** | Não possuem controles aplicados para o risco de operacional identificado | Não tratado | **2** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Risco Operacional > Finalidade do Tratamento de Dados** | | | | | | |
| Coleta de dados pessoais desnecessários para a finalidade do tratamento que serão submetidos (Princípio da Necessidade) | 3 | 3 | **9** | Não possuem controles aplicados para o risco de operacional identificado | Não tratado | **9** |
| Tratamento de dados pessoais em desconformidade com a finalidade legal para a qual foram coletados (Princípio da Finalidade e Adequação) | 1 | 1 | **1** | Não possuem controles aplicados para o risco de operacional identificado | Não tratado | **1** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Risco Operacional > Proteção de dados em acervo físico documental** | | | | | | |
| Inexistência ou falha na Proteção de Dados de Acervos Físicos Documentais | 2 | 2 | **4** | Não possuem controles aplicados para o risco de operacional identificado | Não tratado | **4** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Risco Operacional > Finalidade do Tratamento de Dados** | | | | | | |
| Coleta de dados pessoais desnecessários para a finalidade do tratamento que serão submetidos (Princípio da Necessidade) | 1 | 1 | **1** | Não possuem controles aplicados para o risco de operacional identificado | Não tratado | **1** |