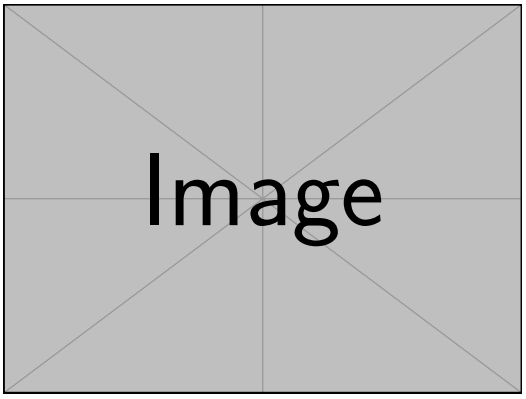
# Guia Prático das Normas ISO/IEC 27000

## Para Servidores Públicos




*Um guia completo sobre ISO/IEC 27001, 27002 e 27005*
*para implementação da segurança da informação no contexto brasileiro*

24 de abril de 2025

# Sumário

# Capítulo 1

# Introdução à Família ISO/IEC 27000

## 1.1 Contexto e Importância

A segurança da informação tornou-se um pilar fundamental para o funcionamento eficaz das instituições públicas brasileiras. Com o crescente número de ameaças cibernéticas e a expansão da digitalização dos serviços públicos, proteger dados sensíveis e assegurar a continuidade operacional dos sistemas governamentais deixou de ser apenas uma boa prática para se tornar uma necessidade crítica.

A família de normas ISO/IEC 27000 representa o conjunto de padrões internacionalmente reconhecidos para gestão da segurança da informação, fornecendo um framework abrangente para implementar, manter e aprimorar um Sistema de Gestão de Segurança da Informação (SGSI). Estas normas, desenvolvidas pela Organização Internacional para Padronização (ISO) em conjunto com a Comissão Eletrotécnica Internacional (IEC), oferecem diretrizes baseadas em melhores práticas globais.

Para os servidores públicos brasileiros, compreender e aplicar estas normas é essencial não apenas para cumprir requisitos legais como a Lei Geral de Proteção de Dados (LGPD), mas também para proteger informações críticas dos cidadãos e garantir a confiabilidade dos serviços públicos.

**Informação Importante**

A implementação efetiva das normas ISO/IEC 27000 nas instituições públicas contribui diretamente para:

- Proteção dos dados dos cidadãos brasileiros
- Conformidade com legislações nacionais como a LGPD
- Redução de riscos e custos associados a incidentes de segurança
- Aumento da confiança da sociedade nas instituições públicas
- Melhoria da eficiência operacional e continuidade dos serviços

## 1.2 Visão Geral da Família ISO/IEC 27000

A família ISO/IEC 27000 é composta por diversas normas complementares, cada uma focada em diferentes aspectos da segurança da informação. Embora este guia se concentre nas normas 27001, 27002 e 27005, é importante compreender a estrutura completa das principais normas desta família:

| Norma | Foco Principal |
|---|---|
| ISO/IEC 27000 | Visão geral e vocabulário |
| ISO/IEC 27001 | Requisitos para um SGSI |
| ISO/IEC 27002 | Código de prática (controles de segurança) |
| ISO/IEC 27003 | Diretrizes para implementação do SGSI |
| ISO/IEC 27004 | Medições de segurança da informação |
| ISO/IEC 27005 | Gestão de riscos de segurança da informação |
| ISO/IEC 27701 | Extensão para gestão de informações de privacidade |
| ISO/IEC 27017 | Controles de segurança para serviços em nuvem |
| ISO/IEC 27018 | Proteção de dados pessoais em nuvens públicas |
| ISO/IEC 27036 | Segurança da informação para relações com fornecedores |

Tabela 1.1: Principais normas da família ISO/IEC 27000

A adoção destas normas segue uma abordagem integrada, com a ISO/IEC 27001 estabelecendo os requisitos fundamentais, enquanto as outras normas proporcionam orientações mais detalhadas sobre aspectos específicos da segurança da informação.

Este guia aborda especificamente as versões mais recentes das normas:

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- ISO/IEC 27005:2019

É importante verificar regularmente atualizações nas versões das normas para garantir conformidade com os padrões mais recentes.

# Capítulo 2

# ISO/IEC 27001:2022 - Requisitos para um SGSI

## 2.1 Fundamentos da ISO/IEC 27001

A ISO/IEC 27001 é a norma central da família 27000, estabelecendo os requisitos para implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI). Diferentemente das outras normas da família, que oferecem orientações e recomendações, a 27001 especifica requisitos obrigatórios para a certificação.

A versão 2022 da norma introduziu mudanças significativas em relação à versão anterior, especialmente na estrutura de alto nível (HLS - High Level Structure) para melhor integração com outros sistemas de gestão como ISO 9001 (Qualidade) e ISO 14001 (Ambiental).

Para os servidores públicos brasileiros, a implementação da ISO 27001 fornece uma base estruturada para proteger informações sensíveis, assegurando:

- Conformidade com requisitos legais e regulatórios, incluindo a LGPD
- Identificação sistemática de riscos de segurança da informação
- Implementação de controles proporcionais aos riscos identificados
- Monitoramento contínuo e melhoria do sistema de gestão

## 2.2 Estrutura da ISO/IEC 27001:2022

A ISO 27001:2022 segue uma estrutura baseada no ciclo PDCA (Plan-Do-Check-Act), proporcionando uma abordagem processual para implementação e operação do SGSI:

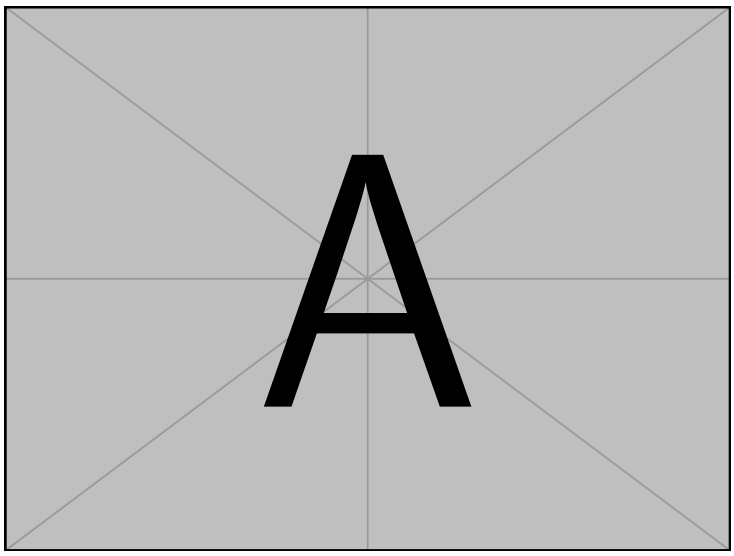



Figura 2.1: Ciclo PDCA aplicado ao SGSI

A norma está organizada em dez seções principais, seguindo a estrutura de alto nível comum a outras normas ISO de sistemas de gestão:

1. Escopo
2. Referências normativas
3. Termos e definições
4. Contexto da organização
5. Liderança
6. Planejamento
7. Suporte
8. Operação
9. Avaliação de desempenho

10. Melhoria

As seções 4 a 10 contêm os requisitos que devem ser atendidos para conformidade com a norma, enquanto o Anexo A apresenta os controles de referência que podem ser implementados conforme a avaliação de riscos da organização.

## 2.3 Implementação de um SGSI

A implementação de um SGSI conforme a ISO 27001 em instituições públicas brasileiras envolve os seguintes passos fundamentais:

### 2.3.1 Contexto da Organização (Seção 4)

- Compreender a organização e seu contexto (fatores internos e externos relevantes)
- Identificar necessidades e expectativas das partes interessadas
- Determinar o escopo do SGSI
- Estabelecer o SGSI considerando os processos necessários e suas interações

### 2.3.2 Liderança (Seção 5)

- Garantir compromisso da alta direção com o SGSI
- Estabelecer e comunicar uma política de segurança da informação
- Atribuir e comunicar responsabilidades e autoridades para funções relevantes

### 2.3.3 Planejamento (Seção 6)

- Identificar riscos e oportunidades relacionados ao SGSI
- Realizar avaliação de riscos de segurança da informação
- Tratamento de riscos de segurança da informação
- Estabelecer objetivos de segurança da informação e planejar como alcançá-los

**Informação Importante**

O processo de avaliação e tratamento de riscos é o coração do SGSI, determinando quais controles do Anexo A devem ser implementados. Para órgãos públicos brasileiros, esta etapa deve considerar:

- Riscos específicos do setor público (exemplo: ataques direcionados a sistemas governamentais)
- Requisitos da LGPD quanto ao tratamento de dados pessoais
- Impactos potenciais na prestação de serviços públicos essenciais
- Exigências específicas de legislações setoriais (saúde, educação, etc.)

### 2.3.4 Suporte (Seção 7)

- Determinar e prover recursos necessários para o SGSI
- Assegurar competência das pessoas que afetam o desempenho do SGSI
- Conscientizar as pessoas sobre a política e contribuição para o SGSI
- Estabelecer processos de comunicação interna e externa
- Controlar a informação documentada requerida pela norma

### 2.3.5 Operação (Seção 8)

- Planejar, implementar e controlar processos para atender aos requisitos de segurança
- Realizar avaliações de risco de segurança da informação em intervalos planejados
- Implementar plano de tratamento de riscos de segurança da informação

### 2.3.6 Avaliação de Desempenho (Seção 9)

- Monitorar, medir, analisar e avaliar o desempenho do SGSI
- Conduzir auditorias internas em intervalos planejados
- Realizar análises críticas pela direção do SGSI

### 2.3.7 Melhoria (Seção 10)

- Reagir a não conformidades e tomar ações corretivas
- Melhorar continuamente a adequação, suficiência e eficácia do SGSI

**Dica para Servidores Públicos:** A implementação da ISO 27001 pode parecer complexa, mas pode ser facilitada através de:

- Abordagem gradual, começando por áreas críticas
- Integração com sistemas de gestão existentes
- Uso de ferramentas de apoio para documentação e gestão de riscos
- Treinamento contínuo das equipes envolvidas
- Compartilhamento de experiências com outros órgãos públicos

# Capítulo 3

# ISO/IEC 27002:2022 - Código de Prática para Controles de Segurança

## 3.1 Fundamentos da ISO/IEC 27002

A ISO/IEC 27002:2022 é um código de prática que fornece orientações detalhadas sobre a implementação dos controles de segurança da informação. Diferentemente da ISO 27001, que especifica requisitos, a 27002 fornece diretrizes e melhores práticas para seleção, implementação e gerenciamento de controles de segurança da informação.

A versão 2022 da norma apresentou uma reestruturação significativa em relação à versão anterior, passando de 14 seções para 4 temas principais, com controles agrupados de forma mais lógica e funcional. Esta nova estrutura facilita a aplicação prática dos controles no contexto de uma organização.

Para servidores públicos, a ISO 27002 serve como um catálogo abrangente de controles que podem ser implementados após uma avaliação de riscos, conforme exigido pela ISO 27001. A implementação adequada desses controles ajuda a:

- Proteger informações sensíveis contra acesso não autorizado
- Garantir a integridade dos dados públicos
- Manter a disponibilidade de serviços essenciais
- Cumprir requisitos regulatórios de segurança da informação

## 3.2 Estrutura da ISO/IEC 27002:2022

A versão 2022 da norma organiza os controles de segurança em quatro temas principais:

| Tema | Descrição |
|---|---|
| Controles Organizacionais | Controles que formam a base para a governança da SI |
| Controles de Pessoas | Foco nas pessoas e seus comportamentos |
| Controles Físicos | Proteção física de ativos e ambientes |
| Controles Tecnológicos | Soluções tecnológicas para segurança da informação |

Tabela 3.1: Temas principais da ISO/IEC 27002:2022

A norma apresenta 93 controles de segurança distribuídos entre esses quatro temas. Cada controle está estruturado de forma uniforme, incluindo:

- Título do controle
- Atributos do controle (tipo, propriedade de SI, conceitos de cibersegurança, capacidades operacionais)
- Texto do controle
- Orientações de implementação
- Outras informações

## 3.3 Principais Grupos de Controles da ISO/IEC 27002:2022

Vamos explorar os principais controles em cada uma das quatro áreas temáticas, com ênfase na aplicação prática no contexto do serviço público brasileiro:

### 3.3.1 Controles Organizacionais

| Código | Controle | Aplicação no Serviço Público |
|---|---|---|

| | | |
|---|---|---|
| 5.1 | Políticas de segurança | Desenvolvimento de políticas claras, atualizadas e aprovadas pela alta direção, alinhadas com os requisitos governamentais |
| 5.10 | Uso de tecnologia aprovada | Assegurar que apenas software e sistemas autorizados sejam utilizados, evitando "TI Sombra" |
| 5.14 | Classificação da informação | Classificar informações públicas conforme Lei de Acesso à Informação e informações pessoais conforme LGPD |
| 5.17 | Gestão de senhas | Implementar políticas de senhas fortes e autenticação multifator para sistemas governamentais |
| 5.23 | Gestão de vulnerabilidades técnicas | Processo estruturado para identificar e corrigir vulnerabilidades em sistemas públicos |
| 5.34 | Acordos de compartilhamento | Estabelecer acordos formais para compartilhamento de informações entre órgãos e com terceiros |

### 3.3.2 Controles de Pessoas

| **Código** | **Controle** | **Aplicação no Serviço Público** |
|---|---|---|
| 6.3 | Conscientização e treinamento | Programas regulares de treinamento para servidores sobre segurança da informação e proteção de dados |
| 6.7 | Trabalho remoto | Políticas específicas para trabalho remoto de servidores, especialmente após a experiência da pandemia |
| 6.8 | Relatório de eventos de segurança | Canais claros para servidores reportarem incidentes de segurança sem medo de represálias |

### 3.3.3 Controles Físicos

| **Código** | **Controle** | **Aplicação no Serviço Público** |
|---|---|---|
| 7.3 | Segurança de escritórios | Proteção física de espaços governamentais, com atenção especial para áreas que tratam dados sensíveis |

| | | |
|---|---|---|
| 7.7 | Mesa limpa e tela limpa | Políticas para evitar exposição de documentos sensíveis e informações em telas desbloqueadas |
| 7.9 | Equipamentos fora das instalações | Controles para dispositivos usados fora das instalações governamentais, como laptops |
| 7.10 | Mídia de armazenamento | Gestão segura de dispositivos de armazenamento como HDs externos, pendrives e documentos físicos |

### 3.3.4 Controles Tecnológicos

| **Código** | **Controle** | **Aplicação no Serviço Público** |
|---|---|---|
| 8.1 | Dispositivos dos usuários | Gestão segura de dispositivos usados por servidores públicos para acessar informações |
| 8.3 | Controle de acesso | Gestão de identidades e acessos com base no princípio do menor privilégio |
| 8.5 | Autenticação da informação | Mecanismos robustos de autenticação para sistemas governamentais |
| 8.7 | Proteção contra malware | Soluções antivírus e anti-malware em todos os dispositivos |
| 8.8 | Gestão de vulnerabilidades técnicas | Processos para identificar e corrigir vulnerabilidades em sistemas |
| 8.10 | Deleção da informação | Procedimentos para exclusão segura de dados, especialmente dados pessoais conforme LGPD |
| 8.13 | Backup da informação | Estratégia de backup para garantir recuperação de informações críticas |
| 8.15 | Registro de eventos | Manutenção de logs e trilhas de auditoria em sistemas governamentais |
| 8.20 | Segurança de rede | Proteção das redes governamentais contra ameaças cibernéticas |
| 8.24 | Criptografia | Uso de criptografia para proteção de dados sensíveis em repouso e em trânsito |

**Informação Importante**

As agências governamentais brasileiras devem priorizar controles com base em:

- Resultados da avaliação de riscos conforme ISO 27005
- Requisitos específicos da LGPD para órgãos públicos
- Natureza dos dados processados (ex.: saúde, educação, segurança)
- Recursos disponíveis e maturidade em segurança da informação

Lembre-se: a implementação dos controles deve ser proporcional aos riscos identificados e aos recursos disponíveis.

## 3.4 Aplicação Prática no Serviço Público

A implementação dos controles da ISO 27002 em instituições públicas deve considerar desafios específicos do contexto brasileiro:

### 3.4.1 Desafios comuns

- Restrições orçamentárias que limitam investimentos em segurança
- Infraestrutura tecnológica muitas vezes defasada
- Cultura organizacional que pode resistir a mudanças
- Complexidade do arcabouço legal brasileiro (LGPD, LAI, etc.)
- Necessidade de continuidade dos serviços públicos essenciais

### 3.4.2 Estratégias de implementação

- Abordagem baseada em riscos, priorizando controles para riscos críticos
- Implementação gradual, começando por "quick wins"de alto impacto
- Aproveitamento de recursos e tecnologias já existentes quando possível
- Desenvolvimento de competências internas para reduzir dependência de consultoria externa

- Estabelecimento de indicadores claros para medir efetividade dos controles

**Exemplo Prático:** O controle 5.14 (Classificação da informação) pode ser implementado em uma secretaria estadual através de:

1. Criação de uma política de classificação alinhada com a LAI e LGPD
2. Desenvolvimento de matriz simplificada de classificação (público, interno, restrito, confidencial)
3. Treinamento de servidores sobre como classificar documentos
4. Implementação de etiquetas visuais para documentos físicos
5. Adoção de metadados de classificação para documentos digitais
6. Auditoria periódica para verificar conformidade

# Capítulo 4

# ISO/IEC 27005:2019 - Gestão de Riscos de Segurança da Informação

## 4.1 Fundamentos da ISO/IEC 27005

A ISO/IEC 27005:2019 fornece diretrizes para o processo de gestão de riscos de segurança da informação. Esta norma é particularmente relevante para órgãos públicos brasileiros, pois complementa a ISO 27001 ao detalhar métodos para identificação, análise, avaliação e tratamento de riscos de segurança da informação.

A gestão eficaz de riscos permite às instituições públicas:

- Identificar ameaças potenciais aos seus ativos de informação
- Priorizar recursos limitados para áreas de maior risco
- Selecionar controles apropriados da ISO 27002 com base em critérios objetivos
- Justificar investimentos em segurança da informação
- Cumprir requisitos da LGPD quanto à responsabilidade no tratamento de dados

## 4.2 O Processo de Gestão de Riscos

A ISO 27005 estabelece um processo estruturado para gestão de riscos de segurança da informação, alinhado com a ISO 31000 (Gestão de Riscos). Este processo inclui as seguintes etapas principais:

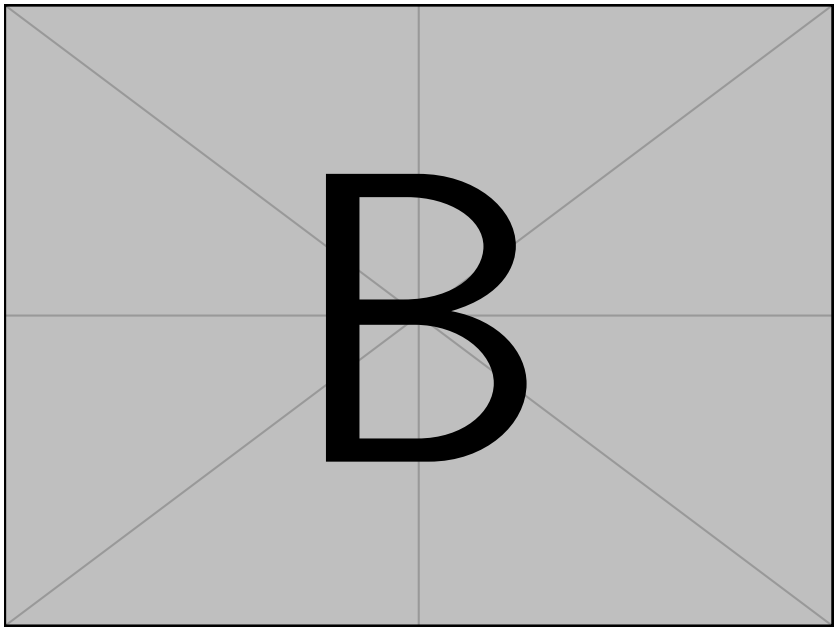



Figura 4.1: Processo de gestão de riscos segundo ISO 27005

### 4.2.1 Estabelecimento do contexto

Nesta fase inicial, é fundamental:

- Definir o escopo do processo de gestão de riscos
- Estabelecer critérios básicos (critérios de risco, impacto e aceitação)
- Definir a organização para gestão de riscos

Para instituições públicas brasileiras, o contexto deve considerar:

- Requisitos regulatórios específicos (LGPD, LAI, regulamentações setoriais)
- Estrutura organizacional e governança do órgão público
- Interfaces com outros órgãos e entidades
- Restrições orçamentárias e de recursos
- Percepção pública e confiança no órgão

### 4.2.2 Processo de avaliação de riscos

**Identificação de riscos**

Esta etapa visa identificar o que poderia causar perdas potenciais, incluindo:

- Identificação de ativos de informação e seus valores
- Identificação de ameaças a esses ativos
- Identificação de vulnerabilidades existentes
- Identificação de controles existentes
- Identificação das consequências potenciais

**Informação Importante**

Para órgãos públicos brasileiros, exemplos típicos de ativos de informação incluem:

- Bancos de dados com informações de cidadãos
- Sistemas de gestão financeira e orçamentária
- Documentos oficiais e processos administrativos
- Sistemas de comunicação interna e externa
- Infraestrutura de TI e sistemas de atendimento ao cidadão

**Análise de riscos**

A análise de riscos envolve:

- Avaliação das consequências (impacto) se os riscos se materializarem
- Avaliação da probabilidade realista da ocorrência dos riscos
- Determinação dos níveis de risco

A análise pode ser qualitativa (escala descritiva), semi-quantitativa (escala numérica) ou quantitativa (valores monetários), dependendo do contexto e dos recursos disponíveis.

| Probabilidade | Impacto | Nível de Risco |
|---|---|---|
| Alta | Alto | Crítico |
| Alta | Médio | Alto |
| Alta | Baixo | Médio |
| Média | Alto | Alto |
| Média | Médio | Médio |
| Média | Baixo | Baixo |
| Baixa | Alto | Médio |
| Baixa | Médio | Baixo |
| Baixa | Baixo | Baixo |

Tabela 4.1: Exemplo de matriz simplificada para classificação de riscos

#### Avaliação de riscos

Esta etapa compara os resultados da análise com os critérios de risco estabelecidos para determinar quais riscos necessitam de tratamento e sua prioridade. Envolve:

- Comparar níveis de risco com critérios de aceitação
- Priorizar riscos para tratamento
- Considerar requisitos legais, operacionais e técnicos

### 4.2.3 Tratamento de riscos

Após a avaliação, os riscos identificados precisam ser tratados através de uma ou mais opções:

1. **Mitigação do risco**: Implementar controles para reduzir o risco a um nível aceitável
2. **Retenção do risco**: Aceitar o risco conforme critérios de aceitação estabelecidos
3. **Evitação do risco**: Evitar a atividade ou condição que origina o risco
4. **Compartilhamento do risco**: Transferir o risco para terceiros (ex.: seguros, contratos)

Para cada risco, deve-se desenvolver um plano de tratamento que documente como as opções escolhidas serão implementadas. Para órgãos públicos brasileiros, é crucial documentar as justificativas para aceitação de riscos, especialmente aqueles relacionados a dados pessoais.

**Informação Importante**

Na seleção de controles para mitigação de riscos, instituições públicas devem considerar:

- Restrições orçamentárias e de recursos humanos
- Eficácia esperada dos controles
- Requisitos legais específicos (ex.: LGPD, normativos do TCU, GSI/PR)
- Impacto potencial nos serviços prestados aos cidadãos
- Facilidade de implementação e manutenção

### 4.2.4 Comunicação e consulta

A comunicação e consulta com partes interessadas internas e externas deve ocorrer durante todas as fases do processo de gestão de riscos. Para órgãos públicos, isso inclui:

- Desenvolvimento de planos de comunicação específicos para diferentes partes interessadas
- Promoção da transparência dos processos (respeitando informações sensíveis)
- Consulta a especialistas técnicos quando necessário
- Alinhamento com outros órgãos e entidades governamentais
- Comunicação clara sobre medidas adotadas para proteção de dados pessoais

### 4.2.5 Monitoramento e análise crítica

O processo de gestão de riscos deve ser continuamente monitorado e revisado para:

- Detectar mudanças precocemente nos contextos interno e externo
- Identificar riscos emergentes
- Garantir que controles permaneçam eficazes
- Capturar lições aprendidas com incidentes e quase-incidentes
- Identificar oportunidades de melhoria

**Atenção:** A ISO 27005 recomenda revisões periódicas da avaliação de riscos, mas para órgãos públicos brasileiros, é recomendável também realizar reavaliações após:

- Mudanças significativas na infraestrutura de TI
- Alterações relevantes na legislação (ex.: novas regulamentações da LGPD)
- Incidentes de segurança graves
- Reorganizações estruturais do órgão
- Implementação de novos sistemas ou serviços críticos

## 4.3 Métodos e Técnicas para Gestão de Riscos

A ISO 27005 não prescreve um método específico para análise de riscos, permitindo que as organizações adotem abordagens que melhor se adequem ao seu contexto. Algumas metodologias comumente utilizadas incluem:

### 4.3.1 Análise Preliminar de Riscos (APR)

Uma abordagem qualitativa simples que pode ser um bom ponto de partida para órgãos públicos com menor maturidade em gestão de riscos. Envolve:

- Identificação de ativos críticos
- Listagem de ameaças possíveis
- Avaliação qualitativa de probabilidade e impacto
- Priorização baseada em matriz simples de riscos

### 4.3.2 FMEA (Failure Mode and Effects Analysis)

Técnica que identifica modos de falha potenciais em sistemas e processos, avaliando:

- Severidade do impacto
- Probabilidade de ocorrência
- Detectabilidade do problema

Multiplicando estes três fatores, obtém-se o Número de Prioridade de Risco (RPN), que facilita a priorização.

### 4.3.3 Método Delphi

Útil para órgãos públicos com acesso a especialistas, mas sem dados históricos confiáveis. Envolve:

- Consulta estruturada a especialistas em segurança da informação
- Várias rodadas de questionários com feedback
- Convergência para um consenso sobre níveis de risco

## 4.4 Aplicação Prática no Serviço Público

A implementação da gestão de riscos conforme a ISO 27005 no serviço público brasileiro apresenta desafios específicos, mas também oportunidades significativas:

### 4.4.1 Desafios comuns

- Cultura organizacional com baixa percepção de riscos
- Recursos limitados para análises aprofundadas
- Estruturas hierárquicas complexas que dificultam decisões ágeis
- Dificuldade em quantificar impactos intangíveis (ex.: confiança pública)
- Mudanças frequentes de liderança que afetam continuidade de projetos

### 4.4.2 Estratégias de implementação

- Iniciar com escopo reduzido, focando em sistemas críticos
- Adotar abordagens qualitativas simples e evoluir para métodos mais sofisticados
- Integrar gestão de riscos de SI com gestão de riscos corporativos
- Desenvolver modelos padronizados e adaptáveis para diferentes contextos
- Criar repositório de riscos comuns para compartilhamento entre órgãos

**Informação Importante**

**Exemplo Prático:** Uma secretaria municipal de saúde pode implementar gestão de riscos para seu sistema de agendamento de consultas através de:

1. Identificação dos ativos (banco de dados de pacientes, sistema de agendamento, infraestrutura)
2. Listagem de ameaças comuns (invasões, indisponibilidade, vazamento de dados)
3. Avaliação de vulnerabilidades técnicas e organizacionais
4. Análise de impacto (ex.: impossibilidade de atendimento, exposição de dados médicos)
5. Seleção de controles proporcionais aos riscos identificados
6. Desenvolvimento de plano de resposta a incidentes específico
7. Monitoramento contínuo e revisões periódicas

# Capítulo 5

# Implementação Integrada no Serviço Público Brasileiro

## 5.1 Alinhamento com a LGPD

A implementação das normas ISO/IEC 27001, 27002 e 27005 deve estar alinhada com os requisitos da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, especialmente considerando que o poder público é um importante controlador de dados pessoais.

### 5.1.1 Pontos de convergência entre ISO 27000 e LGPD

| **Requisito LGPD** | **Norma ISO relacionada** | **Implementação prática** |
|---|---|---|
| Medidas de segurança (Art. 46) | ISO 27001 (Sistema de Gestão) | Implementar um SGSI com escopo incluindo processos de tratamento de dados pessoais |
| Padrões técnicos (Art. 46 §1º) | ISO 27002 (Controles) | Selecionar controles específicos para proteção de dados pessoais |
| Confidencialidade (Art. 6) | ISO 27002 (5.14, 8.24) | Implementar classificação de informação e criptografia |
| Gestão de riscos à privacidade | ISO 27005 | Incluir riscos relacionados a dados pessoais na análise de riscos |

| | | |
|---|---|---|
| Relatório de impacto (Art. 38) | ISO 27005 | Utilizar metodologias de avaliação de riscos como base para RIPD |
| Comunicação de incidentes (Art. 48) | ISO 27002 (6.8) | Desenvolver procedimentos específicos para incidentes com dados pessoais |

### 5.1.2 Adaptações necessárias para conformidade com a LGPD

Embora as normas ISO 27000 forneçam um excelente framework para segurança da informação, algumas adaptações são necessárias para alinhamento específico com a LGPD:

- Inclusão explícita dos princípios de proteção de dados (Art. 6º da LGPD) nas políticas de segurança
- Desenvolvimento de procedimentos específicos para atendimento aos direitos dos titulares
- Adaptação dos procedimentos de classificação de informações para identificar dados pessoais e dados pessoais sensíveis
- Implementação de controles específicos para registros de operações de tratamento
- Desenvolvimento de metodologia específica para Relatório de Impacto à Proteção de Dados (RIPD)

**Informação Importante**

A implementação de um SGSI baseado nas normas ISO 27000 não garante automaticamente conformidade total com a LGPD, mas fornece uma base sólida para demonstrar adoção de medidas técnicas e administrativas adequadas para proteção de dados pessoais, conforme exigido pelo Art. 46 da LGPD.

## 5.2 Checklist Mensal de Segurança da Informação

Com base nas normas ISO 27001, 27002 e 27005, e considerando os requisitos da LGPD, é recomendável que os servidores públicos realizem verificações

periódicas de segurança da informação. Abaixo está um resumo das principais categorias de verificação extraídas do checklist mensal:

1. **Documentos e Dados Sensíveis**
    - Verificar ausência de documentos sensíveis em mesas de trabalho
    - Garantir armazenamento seguro de papéis sensíveis
    - Verificar destruição adequada de documentos descartados
    - Confirmar que mídias removíveis não estão expostas
2. **Segurança no Computador e Navegador**
    - Confirmar bloqueio do computador ao ausentar-se
    - Verificar atualizações de navegadores e sistemas
    - Confirmar ausência de software não autorizado
    - Verificar atividade do antivírus
3. **E-mails e Comunicação Segura**
    - Evitar abertura de e-mails ou links suspeitos
    - Marcar e-mails sensíveis como confidenciais
    - Garantir uso de criptografia para dados pessoais
    - Verificar remetentes antes de abrir anexos
4. **Senhas e Acessos**
    - Confirmar uso de senhas fortes
    - Garantir que senhas não foram compartilhadas
    - Verificar uso de autenticação multifator
    - Evitar salvar senhas em documentos desprotegidos
5. **Conformidade LGPD e Prevenção**
    - Garantir coleta de dados pessoais com consentimento
    - Reportar solicitações de titulares ao DPO
    - Verificar proteção de dados em contratos com fornecedores
    - Confirmar participação em treinamentos de segurança
6. **Proteção contra Ameaças e Práticas de Home Office**

- Garantir uso de VPN em conexões remotas
- Verificar segurança de impressoras e scanners domésticos
- Evitar abrir links ou QR Codes suspeitos
- Verificar segurança de redes Wi-Fi domésticas

7. **Conscientização e Boas Práticas**
   - Evitar clicar em promoções ou descontos suspeitos
   - Garantir bloqueio de tela em dispositivos móveis
   - Evitar discussão de informações sensíveis em locais públicos
   - Reportar comportamentos suspeitos ao gestor ou TI

É recomendável que cada órgão público adapte este checklist às suas necessidades específicas, considerando o tipo de dados tratados, a infraestrutura tecnológica disponível e os riscos identificados na avaliação de riscos (ISO 27005).

## 5.3 Governança e Responsabilidades

Para implementação efetiva das normas ISO 27000 no serviço público brasileiro, é fundamental estabelecer uma estrutura clara de governança e responsabilidades:

### 5.3.1 Alta Administração

- Demonstrar comprometimento com a segurança da informação
- Aprovar políticas e diretrizes de segurança
- Prover recursos necessários para implementação dos controles
- Designar responsabilidades claras para segurança da informação
- Assegurar integração dos requisitos de SI nos processos organizacionais

### 5.3.2 Comitê de Segurança da Informação

- Coordenar implementação da política de segurança da informação
- Analisar resultados de avaliações de riscos
- Priorizar ações e recursos para tratamento de riscos
- Acompanhar indicadores de desempenho do SGSI
- Promover cultura de segurança na organização

### 5.3.3 Equipe de Segurança da Informação

- Implementar e operar controles técnicos de segurança
- Realizar avaliações de risco periódicas
- Monitorar e responder a incidentes de segurança
- Fornecer suporte técnico para implementação de controles
- Manter-se atualizado sobre ameaças e vulnerabilidades emergentes

### 5.3.4 Gestores Departamentais

- Assegurar implementação de controles em suas áreas
- Identificar necessidades específicas de segurança
- Promover conscientização entre suas equipes
- Reportar incidentes e riscos identificados
- Participar das análises de impacto nos negócios

### 5.3.5 Servidores Públicos

- Seguir políticas e procedimentos de segurança
- Participar de treinamentos e campanhas de conscientização
- Reportar incidentes e vulnerabilidades observadas
- Aplicar boas práticas no dia a dia
- Sugerir melhorias nos processos de segurança

**Informação Importante**

Em órgãos públicos sujeitos à LGPD, é recomendável que o Encarregado de Dados (DPO) trabalhe em estreita colaboração com a equipe de segurança da informação para garantir alinhamento entre os requisitos de proteção de dados e controles de segurança.

# Capítulo 6

# Estudos de Caso e Melhores Práticas

## 6.1 Implementação do SGSI em um Órgão Público Federal

### 6.1.1 Contextualização

Um órgão federal responsável por processamento de dados previdenciários iniciou a implementação de um SGSI baseado nas normas ISO 27000 após sofrer tentativas de ataques cibernéticos. O processo incluiu as seguintes etapas:

### 6.1.2 Abordagem

1. **Análise de Contexto**
    - Mapeamento de partes interessadas (cidadãos, servidores, outros órgãos)
    - Levantamento de requisitos legais específicos do setor previdenciário
    - Análise de interdependências com outros sistemas governamentais
2. **Avaliação de Riscos**
    - Inventário de ativos de informação críticos
    - Identificação de vulnerabilidades em sistemas legados
    - Análise de impacto na prestação de serviços aos cidadãos
    - Priorização de riscos considerando criticidade dos dados
3. **Implementação de Controles**

- Seleção de controles prioritários da ISO 27002
- Desenvolvimento de política específica para dados previdenciários
- Implementação de autenticação multifator para acesso a sistemas críticos
- Revisão de contratos com fornecedores para incluir requisitos de SI

4. **Monitoramento e Melhoria**
    - Estabelecimento de métricas de desempenho dos controles
    - Implementação de análise de logs centralizada
    - Testes periódicos de vulnerabilidade e penetração
    - Auditorias internas semestrais

### 6.1.3 Resultados e Lições Aprendidas

- Redução de 70% nos incidentes de segurança reportados
- Melhoria significativa na capacidade de detecção e resposta a tentativas de ataque
- Desafios na integração com sistemas legados com limitações técnicas
- Importância do apoio da alta direção para superar resistências culturais
- Necessidade de adaptação das normas ISO ao contexto específico da administração pública

## 6.2 Programa de Conscientização em Segurança da Informação

### 6.2.1 Contextualização

Uma secretaria estadual de educação implementou um programa abrangente de conscientização em segurança da informação para servidores, baseado nas diretrizes da ISO 27002, com foco em proteção de dados de estudantes.

### 6.2.2 Abordagem

1. **Análise de Necessidades**
    - Pesquisa sobre nível de conhecimento dos servidores
    - Levantamento de incidentes prévios causados por erro humano
    - Identificação de comportamentos de risco específicos
2. **Desenvolvimento de Conteúdo**
    - Criação de material adaptado à realidade do setor educacional
    - Desenvolvimento de estudos de caso baseados em situações reais
    - Tradução de termos técnicos para linguagem acessível
3. **Implementação**
    - Treinamentos presenciais para gestores
    - Módulos online para todos os servidores
    - Campanhas visuais nos ambientes de trabalho
    - Simulações de phishing para testar resposta dos servidores
4. **Avaliação e Reforço**
    - Testes de conhecimento periódicos
    - Reconhecimento de comportamentos seguros
    - Módulos de reforço trimestrais
    - Adaptação contínua baseada em novos riscos identificados

### 6.2.3 Resultados e Lições Aprendidas

- Redução de 85% em incidentes relacionados a engenharia social
- Aumento significativo em reportes de tentativas de phishing
- Importância da adaptação do material ao contexto específico do órgão
- Eficácia de abordagens positivas em vez de foco apenas em consequências negativas
- Necessidade de renovação contínua das estratégias de comunicação

## 6.3 Melhores Práticas para o Serviço Público Brasileiro

Com base nas experiências de implementação das normas ISO 27000 em diferentes órgãos públicos brasileiros, podem-se extrair as seguintes melhores práticas:

### 6.3.1 Planejamento e Governança

- Obter patrocínio explícito da alta administração desde o início
- Estabelecer formalmente papéis e responsabilidades por instrumento normativo interno
- Alinhar iniciativas de segurança da informação com planejamento estratégico institucional
- Integrar requisitos de segurança em processos de contratação desde a concepção
- Estabelecer métricas claras para mensurar efetividade das iniciativas

### 6.3.2 Implementação Técnica

- Adotar abordagem gradual, começando por controles fundamentais
- Considerar limitações de infraestrutura tecnológica no planejamento
- Priorizar automação de controles para reduzir dependência de ações manuais
- Implementar verificações de conformidade técnica em processos contínuos
- Desenvolver capacidade interna para reduzir dependência de consultores externos

### 6.3.3 Aspectos Culturais e Humanos

- Comunicar benefícios da segurança da informação em termos de serviços aos cidadãos
- Envolver representantes de diferentes áreas nas decisões de segurança

- Reconhecer e valorizar comportamentos seguros demonstrados por servidores
- Adaptar linguagem técnica para diferentes públicos internos
- Estabelecer canais acessíveis para reportar preocupações e incidentes

**Dica para Implementação:** Para órgãos públicos com recursos limitados, é recomendável:

1. Começar com uma avaliação simplificada de riscos para identificar áreas críticas
2. Implementar controles básicos com alto impacto e baixo custo (ex.: política de senhas fortes, conscientização)
3. Buscar compartilhamento de experiências com outros órgãos semelhantes
4. Desenvolver capacidades internas gradualmente através de treinamentos específicos
5. Utilizar ferramentas de código aberto quando apropriado para reduzir custos de implementação

# Capítulo 7

# Conclusão e Próximos Passos

## 7.1 Principais Benefícios da Implementação das Normas ISO 27000

A implementação das normas ISO/IEC 27001, 27002 e 27005 no serviço público brasileiro traz benefícios significativos:

- **Proteção de Dados Sensíveis**: Salvaguarda de informações de cidadãos e da administração pública
- **Conformidade Legal**: Base sólida para atendimento à LGPD e outras regulamentações
- **Gestão Eficaz de Riscos**: Identificação e tratamento metódico de ameaças à segurança
- **Melhoria na Prestação de Serviços**: Maior disponibilidade e confiabilidade de sistemas públicos
- **Otimização de Recursos**: Alocação mais eficiente de investimentos em segurança
- **Cultura Organizacional**: Desenvolvimento de consciência sobre responsabilidades de segurança
- **Confiança Institucional**: Fortalecimento da credibilidade do órgão perante a sociedade

## 7.2 Desafios Persistentes

Apesar dos benefícios, alguns desafios persistem na implementação das normas ISO 27000 no setor público:

- **Restrições Orçamentárias**: Limitações de recursos para investimentos em segurança
- **Infraestrutura Legada**: Sistemas antigos com limitações técnicas de segurança
- **Capacitação Técnica**: Necessidade de desenvolvimento contínuo de competências especializadas
- **Resistência à Mudança**: Dificuldades culturais na adoção de novas práticas de trabalho
- **Complexidade Normativa**: Necessidade de harmonizar múltiplos requisitos regulatórios
- **Descontinuidade Administrativa**: Mudanças de gestão que afetam a continuidade de projetos

## 7.3 Tendências e Desenvolvimentos Futuros

Para os próximos anos, algumas tendências importantes devem ser consideradas no planejamento de segurança da informação no serviço público:

- **Expansão do Governo Digital**: Crescimento de serviços públicos online com novos desafios de segurança
- **Inteligência Artificial**: Uso de IA tanto para proteção quanto como vetor potencial de ameaças
- **Regulamentações Adicionais**: Evolução contínua do arcabouço legal de proteção de dados e segurança
- **Segurança em Nuvem**: Migração crescente de sistemas para ambientes em nuvem pública ou híbrida
- **Cibersegurança Colaborativa**: Compartilhamento de informações sobre ameaças entre órgãos públicos
- **Identidade Digital**: Expansão de sistemas de identidade digital cidadã com novos requisitos de proteção

## 7.4 Recomendações Finais para Servidores Públicos

1. **Adotar Mentalidade de Riscos**: Incorporar considerações de segurança da informação em todas as atividades
2. **Buscar Capacitação Contínua**: Manter-se atualizado sobre ameaças emergentes e melhores práticas
3. **Promover Colaboração**: Trabalhar em conjunto com equipes de segurança da informação e proteção de dados
4. **Documentar Decisões**: Registrar justificativas para decisões relacionadas a segurança da informação
5. **Compartilhar Experiências**: Contribuir para a comunidade de prática em segurança no setor público
6. **Aplicar Proporcionalidade**: Implementar controles proporcionais aos riscos identificados
7. **Manter Vigilância Contínua**: Estar atento a sinais de potenciais incidentes de segurança

A segurança da informação no serviço público não é apenas uma questão técnica ou de conformidade, mas um componente essencial da missão de servir ao cidadão com eficiência, integridade e confiabilidade.

**Informação Importante**

**Lembre-se dos três pilares fundamentais da segurança da informação:**

- **Confidencialidade**: Garantir que a informação seja acessível apenas a quem tem autorização
- **Integridade**: Assegurar que a informação permaneça precisa e completa
- **Disponibilidade**: Garantir que a informação esteja acessível quando necessária

Equilibrar esses três pilares é essencial para uma abordagem eficaz de segurança da informação no contexto do serviço público brasileiro.

# Capítulo 8

# Referências e Recursos Adicionais

## 8.1 Normas Técnicas

- ABNT NBR ISO/IEC 27001:2022 - Requisitos para sistemas de gestão de segurança da informação
- ABNT NBR ISO/IEC 27002:2022 - Código de prática para controles de segurança da informação
- ABNT NBR ISO/IEC 27005:2019 - Gestão de riscos de segurança da informação
- ABNT NBR ISO/IEC 27701:2019 - Extensão da ISO/IEC 27001 e ISO/IEC 27002 para gestão da privacidade da informação
- ABNT NBR ISO/IEC 27017:2015 - Controles de segurança para serviços em nuvem
- ABNT NBR ISO/IEC 27018:2019 - Proteção de dados pessoais em nuvens públicas
- ABNT NBR ISO/IEC 27036:2013 - Segurança da informação para relações com fornecedores
- ABNT NBR ISO 31000:2018 - Gestão de riscos - Diretrizes
- ABNT NBR ISO 22301:2020 - Segurança e resiliência - Sistemas de gestão de continuidade de negócios

## 8.2 Legislação e Normativos Brasileiros

- Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD)
- Lei nº 12.527/2011 - Lei de Acesso à Informação (LAI)
- Lei nº 14.129/2021 - Lei de Governo Digital
- Decreto nº 9.637/2018 - Política Nacional de Segurança da Informação
- Decreto nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética
- Instrução Normativa GSI/PR nº 1/2020 - Diretrizes de segurança da informação para órgãos do Poder Executivo Federal
- Resolução CGD nº 2/2020 - Política de Governança Digital no âmbito federal
- Normas Complementares do GSI/PR (NC 01 a NC 22)
- Acórdãos do TCU sobre segurança da informação (1.603/2008, 1.233/2012, 3.051/2014, entre outros)

## 8.3 Publicações e Guias Técnicos

- CERT.br - Cartilha de Segurança para Internet - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
- CTI.BR - Guia de Boas Práticas de Segurança para a Internet - Comitê Gestor da Internet no Brasil
- GSI/PR - Guia de Boas Práticas em Segurança da Informação para o Governo Federal
- NIST Special Publication 800-53 - Security and Privacy Controls for Information Systems and Organizations
- NIST Cybersecurity Framework - Framework for Improving Critical Infrastructure Cybersecurity
- ENISA - Guidelines for SMEs on the security of personal data processing
- CIS Controls - Center for Internet Security Critical Security Controls

- COBIT 2019 - Control Objectives for Information and Related Technologies

## 8.4 Recursos Educacionais

- ENAP - Cursos de capacitação em segurança da informação para servidores públicos
- SERPRO e DATAPREV - Material educacional sobre segurança da informação
- CEGSIC/UnB - Curso de Especialização em Gestão da Segurança da Informação e Comunicações
- Governo Digital - Plataforma de cursos online sobre segurança da informação e proteção de dados
- TCU - Cartilhas e guias sobre governança e segurança da informação
- ANPD - Guias orientativos sobre proteção de dados pessoais na administração pública

## 8.5 Portais e Comunidades

- Portal do Governo Digital - `https://www.gov.br/governodigital`
- Portal da ANPD - `https://www.gov.br/anpd`
- CTIR.Gov - Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal
- Portal da Transparência - `https://www.portaltransparencia.gov.br`
- Comunidade de TIC do SISP - Sistema de Administração dos Recursos de Tecnologia da Informação
- Rede Nacional de Ensino e Pesquisa (RNP) - Centro de Atendimento a Incidentes de Segurança (CAIS)

**Dica para Servidores Públicos:** Além dos recursos listados acima, é recomendável participar de grupos de discussão e comunidades de prática em segurança da informação específicos para o setor público, como os fóruns do SISP e grupos técnicos coordenados pelo GSI/PR, onde é possível compartilhar experiências e desafios com outros órgãos.

# Capítulo 9

# Apêndices

## 9.1 Apêndice A - Glossário de Termos

| Termo | Definição |
|---|---|
| Ativo de informação | Qualquer componente (informação, software, hardware, serviço, pessoa) que tenha valor para a organização |
| Ameaça | Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização |
| Confidencialidade | Propriedade de que a informação não esteja disponível ou revelada a pessoas, entidades ou processos não autorizados |
| Controle | Medida que modifica o risco; inclui políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais |
| Disponibilidade | Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada |
| Incidente de segurança | Evento único ou série de eventos de segurança da informação indesejados ou inesperados, que têm probabilidade significativa de comprometer as operações do negócio |
| Integridade | Propriedade de salvaguarda da exatidão e completeza de ativos |
| Não repúdio | Capacidade de provar a ocorrência de um evento ou ação alegada e suas entidades originárias |
| Resiliência | Capacidade de adaptação de uma organização em um ambiente complexo e em constante mudança |

| | |
|---|---|
| Risco | Efeito da incerteza sobre os objetivos, caracterizado pela referência a eventos potenciais, suas consequências e à probabilidade de ocorrência |
| SGSI | Sistema de Gestão de Segurança da Informação; parte do sistema de gestão global, baseado na abordagem de risco do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação |
| Tratamento de riscos | Processo para modificar o risco através da aplicação de controles |
| Vulnerabilidade | Fragilidade de um ativo ou controle que pode ser explorada por uma ou mais ameaças |

## 9.2 Apêndice B - Modelos de Documentos

### 9.2.1 B.1 - Modelo Simplificado de Política de Segurança da Informação

**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**

**1. OBJETIVO**

Estabelecer diretrizes e princípios de segurança da informação para proteção dos ativos de informação do [NOME DO ÓRGÃO], garantindo a confidencialidade, integridade, disponibilidade e autenticidade das informações.

**2. ABRANGÊNCIA**

Esta política aplica-se a todos os servidores, colaboradores, estagiários, consultores, prestadores de serviço e demais usuários que tenham acesso às informações e recursos de tecnologia da informação do [NOME DO ÓRGÃO].

**3. PRINCÍPIOS**

- As informações devem ser protegidas de acordo com seu valor, sensibilidade e criticidade;
- A gestão de segurança da informação deve estar alinhada às estratégias e objetivos institucionais;
- As responsabilidades pela segurança da informação devem ser claramente definidas;
- A gestão de riscos deve ser realizada de forma contínua;
- A conscientização e capacitação em segurança da informação são essenciais para a efetividade desta política.

**4. DIRETRIZES GERAIS**

- Classificação da Informação: As informações devem ser classificadas de acordo com seu grau de sensibilidade e criticidade.
- Controle de Acesso: O acesso às informações deve ser concedido conforme o princípio do privilégio mínimo.
- Uso Aceitável: Os recursos de TI devem ser utilizados exclusivamente para fins institucionais.
- Gestão de Incidentes: Todos os incidentes de segurança devem ser reportados e tratados adequadamente.
- Conformidade: Todas as ações devem estar em conformidade com a legislação vigente, em especial a LGPD.
- Continuidade de Negócios: Planos de continuidade devem ser estabelecidos para os processos críticos.

**5. RESPONSABILIDADES**

### 9.2.2 B.2 - Matriz Simplificada de Avaliação de Riscos

**MATRIZ DE AVALIAÇÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO**

| Ativo | Ameaça | Vulnerabilidade | Controles Existentes |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

| Probabilidade | Impacto | Nível de Risco | Tratamento | Controles Recomendados |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |

**Instruções de preenchimento:**

- **Ativo:** Identifique o ativo de informação (sistema, banco de dados, equipamento, etc.)
- **Ameaça:** Descreva a ameaça potencial (ex.: acesso não autorizado, vazamento de dados)
- **Vulnerabilidade:** Indique as vulnerabilidades que podem ser exploradas
- **Controles Existentes:** Liste os controles já implementados
- **Probabilidade:** Estime a probabilidade (Alta, Média, Baixa)
- **Impacto:** Avalie o impacto potencial (Alto, Médio, Baixo)
- **Nível de Risco:** Determine o nível conforme a matriz (Crítico, Alto, Médio, Baixo)
- **Tratamento:** Indique a estratégia (Mitigar, Aceitar, Evitar, Compartilhar)
- **Controles Recomendados:** Sugira controles adicionais referenciando a ISO 27002

### 9.2.3 B.3 - Modelo de Plano de Ação para Implementação

**PLANO DE AÇÃO PARA IMPLEMENTAÇÃO DO SGSI**

| ID | Ação | Responsável | Início | Término | Status |
|---|---|---|---|---|---|
| 1 | Estabelecer comitê de segurança da informação | | | | |
| 2 | Desenvolver política de segurança da informação | | | | |
| 3 | Realizar inventário de ativos de informação | | | | |
| 4 | Implementar metodologia de avaliação de riscos | | | | |
| 5 | Definir plano de tratamento de riscos | | | | |
| 6 | Selecionar e implementar controles prioritários | | | | |
| 7 | Estabelecer métricas e indicadores do SGSI | | | | |
| 8 | Desenvolver programa de conscientização | | | | |
| 9 | Implementar processo de gestão de incidentes | | | | |
| 10 | Realizar auditoria interna do SGSI | | | | |
| 11 | Conduzir análise crítica pela direção | | | | |
| 12 | Estabelecer processo de melhoria contínua | | | | |

**Recursos necessários:**

- 
- 
- 

**Premissas:**

*Segurança da Informação no Serviço Público*

- 
- 

**Restrições:**

- 

## 9.3 Apêndice C - Lista de Verificação Mensal de Segurança da Informação

**CHECKLIST MENSAL DE SEGURANÇA DA INFORMAÇÃO**

**Instruções:** Marque "Sim", "Não"ou "N/A"(Não Aplicável) para cada item. Para itens marcados como "Não", registre a não conformidade e defina uma ação corretiva.

### 1. Documentos e Dados Sensíveis

| Item | Sim | Não | N/A |
|---|---|---|---|
| 1.1 Documentos sensíveis não são deixados expostos sobre a mesa | | | |
| 1.2 Documentos físicos sensíveis são armazenados em gavetas ou armários seguros | | | |
| 1.3 Documentos descartados são triturados ou destruídos adequadamente | | | |
| 1.4 Mídias removíveis (DVDs, pen drives) contendo dados sensíveis estão guardadas em local seguro | | | |

### 2. Segurança no Computador e Navegador

| Item | Sim | Não | N/A |
|---|---|---|---|
| 2.1 Computador é bloqueado (Ctrl+Alt+Del ou Win+L) ao ausentar-se da estação de trabalho | | | |
| 2.2 Sistema operacional e navegadores estão atualizados | | | |
| 2.3 Não há software não autorizado instalado no computador | | | |
| 2.4 Antivírus está ativo e atualizado | | | |
| 2.5 Firewall está ativado | | | |

### 3. E-mails e Comunicação Segura

| Item | Sim | Não | N/A |
|---|---|---|---|
| 3.1 E-mails de origem desconhecida não são abertos | | | |
| 3.2 Links em e-mails suspeitos não são clicados | | | |
| 3.3 E-mails contendo informações sensíveis são marcados como confidenciais | | | |
| 3.4 Dados pessoais sensíveis são compartilhados apenas com criptografia | | | |
| 3.5 Remetente de e-mail é verificado antes de | | | |

**Informação Importante**

Este checklist deve ser adaptado à realidade específica de cada órgão público, considerando sua estrutura, capacidade técnica e níveis de risco. Recomenda-se que os servidores realizem esta verificação mensalmente, documentando os resultados para identificação de tendências e oportunidades de melhoria.

## 9.4 Apêndice D - Mapeamento entre Controles ISO 27002 e Requisitos da LGPD

| **Artigo LGPD** | **Requisito** | **Controles ISO 27002 relacionados** | **Prioridade** |
|---|---|---|---|
| Art. 46 | Medidas de segurança técnicas e administrativas para proteger dados pessoais | 5.1 - Políticas de segurança 5.23 - Gestão de vulnerabilidades 8.3 - Controle de acesso 8.24 - Criptografia | Alta |
| Art. 46 §1º | Padrões técnicos mínimos | Toda a norma ISO 27002 fornece estes padrões | Alta |
| Art. 47 | Segurança desde a concepção | 5.7 - Segurança no desenvolvimento 5.8 - Segurança no ciclo de vida | Alta |
| Art. 48 | Comunicação de incidentes | 5.24 - Gestão de incidentes 6.8 - Relatório de eventos de segurança | Alta |
| Art. 49 | Sistemas seguros e com registro de acesso | 8.5 - Autenticação da informação 8.15 - Registro de eventos | Alta |
| Art. 6, III | Necessidade | 5.14 - Classificação da informação 8.10 - Deleção da informação | Média |
| Art. 6, VII | Prevenção | 5.4 - Avaliação de riscos 5.5 - Tratamento de riscos | Alta |
| Art. 6, VIII | Não discriminação | 5.35 - Proteção de PII (informações pessoais identificáveis) | Média |
| Art. 6, IX | Responsabilização e prestação de contas | 5.1 - Políticas de segurança 5.2 - Funções e responsabilidades | Alta |
| Art. 6, X | Transparência | 5.16 - Definição de requisitos de SI 5.34 - Acordos de compartilhamento | Média |

| | | | |
|---|---|---|---|
| Art. 18 | Direitos dos titulares | 5.22 - Transferência de informação 8.9 - Gestão dos direitos de acesso privilegiados | Alta |
| Art. 38 | Relatório de impacto à proteção de dados pessoais | 5.4 - Avaliação de riscos 5.5 - Tratamento de riscos | Alta |
| Art. 50 | Governança em privacidade | 5.1 - Políticas de segurança 5.2 - Funções e responsabilidades | Alta |

Este mapeamento é indicativo e deve ser adaptado ao contexto específico de cada órgão público. A implementação dos controles deve ser precedida por uma análise de riscos conforme a ISO 27005, considerando-se os dados tratados, os sistemas utilizados e o contexto operacional da instituição.

## 9.5 Índice Remissivo