Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Tocantins
Reitoria

PLANO DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

HISTÓRICO DE VERSÕES

Data	Versão	Descrição
22/11/2023	1	Elaboração do plano de gestão de segurança da informação no IFTO.

1. INTRODUÇÃO

Um plano de gestão de segurança da informação é um documento estratégico que detalha as políticas, processos, procedimentos, programas e ações de controle necessários para garantir a proteção, confidencialidade, integridade e disponibilidade das informações e dados sensíveis e de defesa contra ameaças cibernéticas no âmbito do IFTO.

Este documento visa mitigar ameaças e vulnerabilidades de privacidade e segurança da informação, estabelecer controles adequados para garantir maior proteção de dados e promover uma cultura de privacidade e segurança da informação em todo o IFTO. Este plano considera ameaças internas e externas, avalia riscos, define responsabilidades e implementa medidas de segurança para salvaguardar ativos de informação críticos para o instituto.

O plano de gestão de segurança da informação consiste em um processo contínuo para estabelecer um sistema de gestão de segurança da informação contemplando as fases: estabelecer, implementar e operar, monitorar e analisar criticamente e manter e melhorar a segurança da informação dentro do IFTO. O documento foi elaborado a partir de boas práticas apresentadas no *framework* de Privacidade e Segurança da Informação divulgado pela Secretaria de Governo Digital (SGD, 2023), normas 27001 e 27002 publicada pela ISO/IEC (ABNT, 2022a; ABNT, 2022b) e Controles CIS apresentados pelo *Center for Internet Security* (CIS, 2023).

1.1. Escopo

O escopo deste documento contempla medidas de controle para garantir privacidade e segurança da informação para os recursos

operacionais e comunicação disponibilizados pela área de Tecnologia da Informação no âmbito do IFTO.

1.2. **Objetivos**

Este plano tem como objetivo criar um ambiente seguro no qual o IFTO possa operar, proteger seus ativos de informação e garantir que as informações críticas estejam disponíveis, íntegras e confidenciais, contribuindo para a confiabilidade, conformidade e eficiência geral das operações do IFTO.

1.3. **Abrangência**

O plano abrange a definição de políticas, normas, medidas de segurança, procedimentos, atividades e ferramentas a serem adotadas pelo IFTO nos próximos anos visando a privacidade e segurança das informações relacionadas aos recursos, sistemas operacionais, aplicações, *softwares*, sistemas de informações, aplicativos e serviços de TI.

1.4. **Benefícios esperados**

Com a execução do plano de gestão de segurança da informação espera-se obter os seguintes benefícios:

a) proteção dos ativos de informação;

b) melhorar os controles de privacidade e segurança da informação adotados pelo IFTO;

c) promover a conformidade com a legislação vigente (leis, decretos, instruções normativas, portarias, políticas, normas, entre outros);

d) melhorar as estratégias de monitoramento e controle de privacidade e segurança da informação;

e) evitar o vazamento de informações e proteger os dados sensíveis do IFTO;

f) ajudar a reduzir os riscos de ataques cibernéticos e falhas de segurança;

g) melhorar a confiança dos sistemas tecnológicos desenvolvidos e mantidos pelo IFTO;

h) estabelecer procedimentos para detecção, notificação e resposta a incidentes de segurança da informação;

i) garantir a proteção e privacidade dos dados dos usuários;

j) ampliar a confiabilidade e proteção de sistemas de informação contra os principais ataques que podem resultar em incidentes de segurança da informação;

k) garantir a continuidade de negócios; e

l) disseminar a cultura de privacidade e segurança da informação no IFTO.

2. **DEFINIÇÕES**

Para melhor compreender os termos, acrônimos e abreviações referentes à temática segurança da informação foram utilizados os conceitos apresentados no glossário de segurança da informação (BRASIL, 2021), nas normas ABNT 27001 (ABNT, 2022a), 27002 (ABNT, 2022b), 27005 (ABNT, 2019), 31000 (ABNT, 2018).

a) ameaça: qualquer evento que explore vulnerabilidades. Causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização;

b) análise de riscos: uso sistemático de informações visando a identificação e estimativa das fontes de risco;

c) avaliação de riscos: processo global da análise de risco e da valoração do risco;

d) autenticidade: propriedade de estar associado a uma determinada pessoa, entidade ou processo; permite a validação de identidade de usuários e sistemas;

e) autenticidade: propriedade de estar associado a uma determinada pessoa, entidade ou processo; Permite a validação de identidade de usuários e sistemas;

f) ataque: qualquer ação que comprometa a segurança de uma organização;

g) ativo: qualquer elemento que tenha valor para a organização e para os seus negócios. Alguns exemplos: banco de dados, *softwares*, equipamentos (computadores, notebooks e servidores), elementos de redes (roteadores, *switches* entre outros), pessoas, processos e serviços;

h) confidencialidade: propriedade de não estar disponível ou acessível para pessoas, entidades ou processos não autorizados;

i) controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso aos meios de tecnologia oferecidos;

j) CSI: Comitê de Segurança da Informação;

k) diretriz: descrição que orienta o que deve ser feito e como para se alcançarem objetivos estabelecidos nas políticas;

l) disponibilidade: propriedade de estar disponível e utilizável diante da demanda de uma entidade devidamente autorizada;

m) ETIR: grupo de agentes públicos com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da administração pública federal, em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação do órgão ou da entidade. Anteriormente era chamada de

Equipe de Tratamento de Incidentes de Rede;

n) evento: ocorrência identificada de um estado de rede, serviço ou sistema que indique uma possível falha da política de segurança ou falha das salvaguardas, ou mesmo uma situação até então desconhecida que pode se tornar relevante em termos de segurança;

o) evento de segurança da informação: ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da Política de Segurança da Informação, ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação;

p) gerenciamento de riscos: atividades coordenadas para dirigir e controlar uma organização, no que se refere aos riscos. Normalmente inclui a avaliação do risco, o tratamento do risco, a aceitação do risco e a comunicação do risco;

q) gerenciamento de incidentes: processo responsável pela gestão do ciclo de vida de todos os incidentes. Seu propósito é restaurar a operação normal do serviço de TI o mais rápido possível e que o impacto no negócio seja minimizado;

r) impacto: consequência avaliada de um evento em particular;

s) informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

t) incidente: evento ou série de eventos indesejados ou inesperados que provavelmente comprometerão as operações da empresa ou ameaçam a segurança da informação. Uma interrupção não planejada (imprevista) de um serviço ou redução na qualidade de um serviço. Qualquer evento que cause ou possa causar uma interrupção ou uma redução da qualidade do serviço prestado. Como exemplo de incidente tem-se: indisponibilidade de internet, queima de componentes eletrônicos em servidor, *bug* de sistema ou problemas de impressão;

u) incidente de segurança: um ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação como por exemplo ataques cibernéticos;

v) integridade: propriedade de salvaguardar a precisão e completude dos ativos;

x) não repúdio: propriedade de garantir que uma pessoa ou entidade participante numa dada operação jamais possa negar essa participação;

plano de trabalho: instrumento tático de diagnóstico e planejamento da implementação dos controles de privacidade e de segurança da informação;

w) política de segurança da informação: Documento que declara o comprometimento da direção e estabelece o enfoque da organização para gerenciar a segurança da informação;

y) privacidade: direito à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, nos termos do inciso X do art. 5 da Constituição da República Federativa do Brasil de 1988;

z) processo: qualquer atividade utilizando recursos e gerenciamento para promover a transformação de entradas em saídas;

a1) segurança da informação: ações que objetivam assegurar a preservação da confidencialidade, integridade e disponibilidade da informação. Além disso, outras propriedades, como autenticidade, responsabilização, não repúdio e confiabilidade podem também estar envolvidas;

b1) vulnerabilidade: qualquer fraqueza que possa ser explorada e comprometer a segurança de sistemas ou informações. Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. São falhas que permitem o surgimento de deficiências na segurança geral do computador ou da rede; e

c1) Usuário: pessoa que utiliza sistemas e/ou demais recursos de tecnologia da informação e comunicação do IFTO.

3. SEGURANÇA DA INFORMAÇÃO

A gestão de segurança da informação é um conjunto de processos, metodologias, procedimentos desenvolvidos e implementados para garantir a confidencialidade, integridade e disponibilidade das informações atuando contra acessos não autorizados, mau uso, divulgações indevidas, cópias não autorizadas, destruição ou alterações. Ela envolve a implementação de políticas, procedimentos, práticas e tecnologias com o propósito de garantir que os dados e informações críticas de uma organização sejam protegidos de maneira eficaz, reduzindo riscos e garantindo a integridade e a confiabilidade desses ativos.

As atividades e responsabilidades sobre questões relacionadas à segurança da informação dos recursos de processamento da informação, inclusive dos recursos de computação em nuvem no âmbito do IFTO são definidas conforme a Instrução Normativa PR/SGD nº 1, de 27 de maio de 2020 e Portaria SGD/MGI nº 852, de 28 de março de 2023, Lei nº 13.709/2018 e Política de Segurança da Informação do IFTO.

3.1. Estrutura organizacional de segurança da informação

A estrutura de gestão de segurança da informação no IFTO é formada da seguinte forma:

a) Gestor de Tecnologia da Informação: dentre outras atribuições, nos termos da Portaria nº 778, de 4 de abril de 2019, responsável por planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, considerando a cadeia de suprimentos relacionada à solução;

b) Gestor de Segurança da Informação: dentre outras atribuições, nos termos da Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional, da Presidência da República - GSI/PR, responsável por planejar, implementar e melhorar continuamente os controles de segurança da informação em ativos de informação;

c) Encarregado pelo Tratamento de Dados Pessoais: dentre outras atribuições, nos termos do art. 41, §2º, da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD), responsável por conduzir o diagnóstico de privacidade, bem como orientar, no que couber, os gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis;

d) Responsável pela Unidade Controle Interno: atuará no apoio, supervisão e monitoramento das atividades desenvolvidas pela primeira linha de defesa prevista pela Instrução Normativa CGU nº 3, de 9 de junho de 2017;

e) Comitê de Segurança da Informação: grupo de pessoas formado por representantes das áreas finalísticas e assessoram a implementação das ações de segurança da informação, constituem grupos de trabalhos para tratar temas e propor soluções específicas sobre segurança da informação, participam da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação; e

f) Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação: composta preferencialmente por servidores públicos civis ocupantes de cargo efetivo ou militares de carreira, com capacidade técnica compatível com as atividades dessa equipe. A atuação da equipe será regida por normativos, padrões e procedimentos técnicos exarados pelo Centro de Tratamento e Resposta de Incidentes Cibernéticos do governo, sem prejuízo das demais metodologias e padrões conhecidos.

3.2. Sistema de Gestão de Segurança da Informação

O sistema de gestão de segurança da informação (SGSI-IFTO) do IFTO utiliza como referência a norma ISO/IEC/ABNT 27001:2022 (ABNT, 2022a). A figura 1 apresenta as 4 (quatro) fases a serem executadas continuamente pelo IFTO para garantir a privacidade e segurança da informação como também a conformidade com a legislação pertinente.

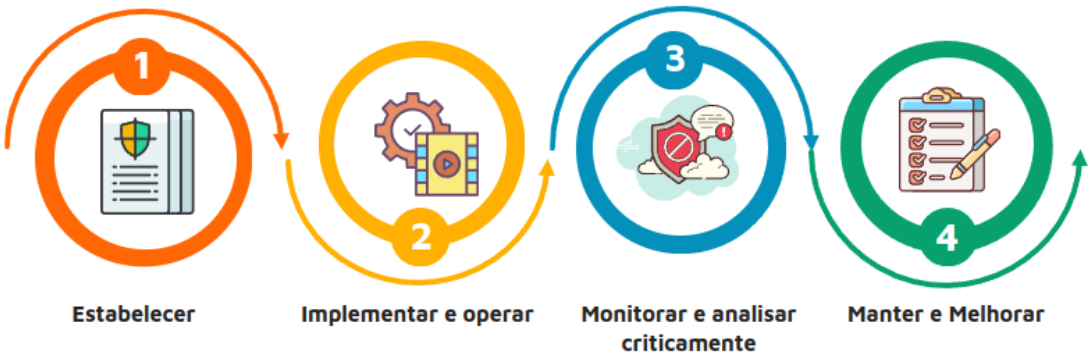

Figura 1 - Fases do SGSI-IFTO

O SGSI-IFTO apresentado na figura 1, utilizado pelo IFTO inclui uma abordagem para proteger a informação de acordo com os princípios e atributos de confidencialidade, disponibilidade, integridade,

responsabilidade, autenticidade e criticidade. Ele envolve vários processos organizacionais dentre eles: classificação da informação, gestão de riscos de segurança da informação, gestão de resposta a incidentes cibernéticos, controle de acesso à informação, gestão de ativos de tecnologia da informação, conscientização, educação e treinamento em segurança da informação dentre outros processos.

O SGSI-IFTO é uma abordagem estratégica criada a partir das necessidades e objetivos, requisitos de segurança, processos organizacionais e tamanho do IFTO. Ela permite o entendimento dos requisitos de segurança da informação e a necessidade de estabelecer uma política e objetivos para a segurança da informação. Também possibilita a implementação e operação de controles para gerenciar os riscos de segurança da informação no contexto dos riscos de negócio. Esta abordagem permite o monitoramento crítico e análise crítica do desempenho e eficácia do SGSI e a melhoria contínua baseada em medições objetivas.

3.3. Processos e programa de gestão de segurança da informação

Na execução do plano de gestão de privacidade e segurança da informação vários processos e programa que compõem o Sistema de Gestão de Segurança da Informação (SGSI-IFTO) estão interrelacionados de forma a possibilitar a gestão de segurança da informação integrada aos demais processos organizacionais. A figura 2 apresenta resuimidamente alguns dos processos relacionados à privacidade e segurança da informação.

Figura 2 - Processos e programa que compõem o SGSI-IFTO

A figura 2 apresenta os processos e programa que compõe o SGSI-FTO. Para cada processo e programa existem medidas de controles a serem implementadas para assegurar a disponibilidade, integridade,

confidencialidade e a autenticidade da informação no âmbito do IFTO.

3.4. Controles de privacidade e segurança da informação

A gestão de segurança da informação envolvem os controles de privacidade e segurança da informação definidos pelo *Center for Internet Security* (CIS, 2023). Estes controles envolvem rotinas para gestão de ativos da informação, classificação da informação, riscos de segurança da informação, acesso à informação, auditoria de logs, incidentes de segurança da informação, gestão contínua de vulnerabilidades, proteção e recuperação de dados e educação de usuários. A figura 3 apresenta de forma resumida os controles que compõem a privacidade de dados no IFTO.

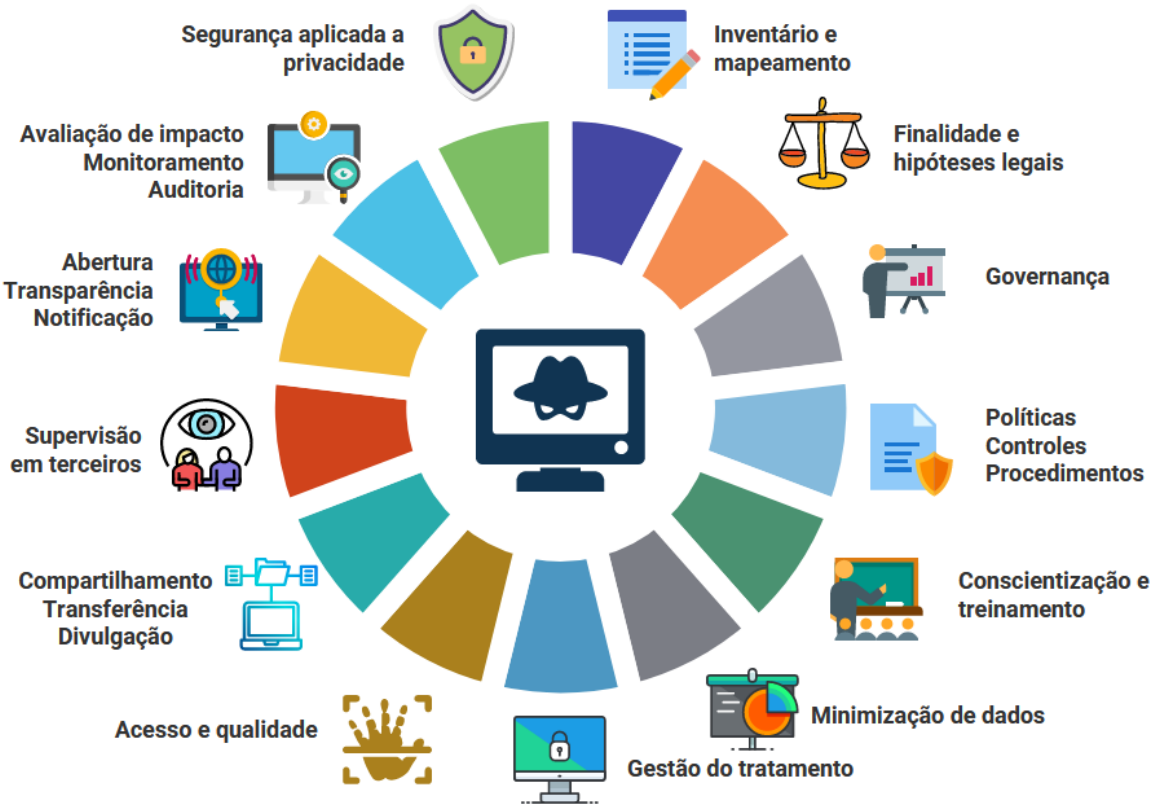

Figura 3 - Controles de Privacidade

O detalhamento dos controles de privacidade apresentados na figura 3 consta no anexo I deste documento. A figura 4 apresenta de forma resumida os controles que compõem a segurança da informação no IFTO.

Figura 4 - Controles de Segurança da Informação

O detalhamento dos controles apresentados na figura 4 consta no anexo I deste documento. Estes controles seguem a recomendação do *Center for Internet Security* (CIS, 2023) e Norma ANBT/ISO/IEC 27002:2022 (ABNT, 2022b).

3.5. Framework de Privacidade e Segurança da Informação

Para a implementação de ações relacionadas aos controles de privacidade e segurança da informação, o IFTO utiliza o Programa de Privacidade e Segurança da Informação (PPSI) definido na Portaria SGD/MGI Nº 852, de 28 de março de 2023 (BRASIL, 2023). A figura 5 apresenta o framework utilizado pelo IFTO.

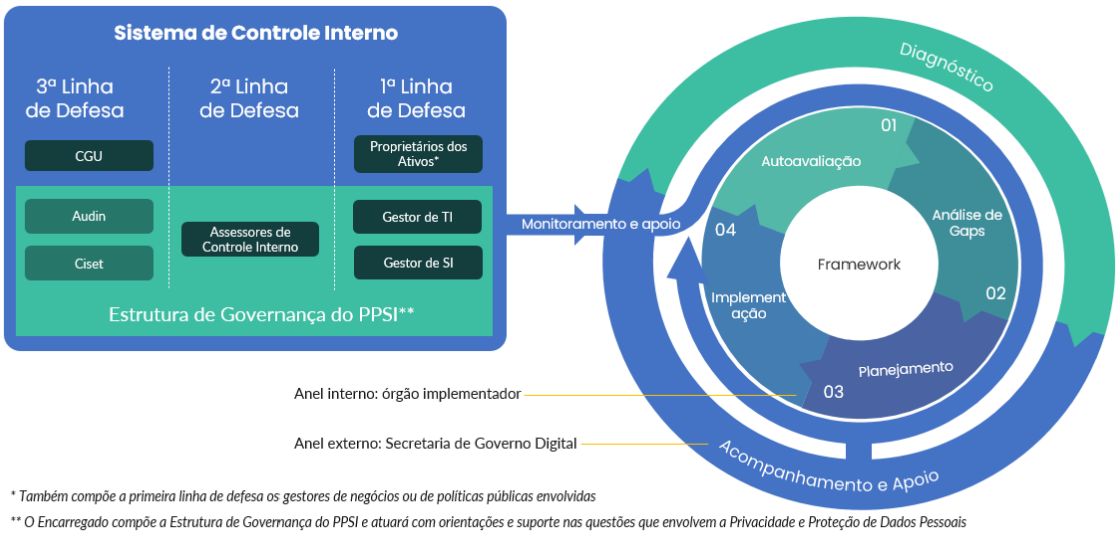

Figura 5 - Framework de privacidade e segurança da informação (BRASIL, 2023)

A figura 5 resume a metodologia utilizada para a implementação do *framework* de privacidade e segurança da informação no âmbito do IFTO. A metodologia é composta por 4 (quatro) etapas: autoavaliação, análise de *gaps,* planejamento e implementação.

3.6. Plano de gestão de segurança da informação

O plano de gestão de segurança da informação é composto por 12 (doze) etapas iterativas e incrementais. Estas etapas envolvem diversas temáticas: monitoramento de ameaças e vulnerabilidades, desenvolvimento de políticas, programas, normas, processos, planos, contratos e procedimentos, treinamento e conscientização, implementação de controles técnicos, monitoramento e detecção de incidentes, privacidade de dados, gestão de fornecedores e terceiros, gestão da segurança da rede, auditorias e revisões, conformidade regulatória, resposta a incidentes e melhoria contínua. A figura 6 apresenta de forma resumida as etapas que são utilizadas pelo IFTO para gerir a segurança da informação.

Figura 6 - Plano de gestão de segurança da informação

As etapas do plano de gestão de segurança da informação apresentadas na figura 6 foram definidas a partir das boas práticas utilizadas no mercado para a privacidade e segurança da informação. Grande parte das medidas e controles a serem utilizadas pelo IFTO são recomendadas pelo *Center for Internet Security* (CIS, 2023) e Norma ANBT/ISO/IEC 27002:2022 (ABNT, 2022b).

3.4.1. Monitoramento de ameaças e vulnerabilidades

Etapa responsável por identificar as ameaças potenciais aos sistemas e dados do IFTO com também as possíveis vulnerabilidades em sistemas, softwares e aplicativos utilizados pelo IFTO. A fase avalia as vulnerabilidades que podem ser exploradas e determina o impacto e probabilidade de ocorrência de cada ameaça identificada. Nesta etapa são realizadas as atividades:

a) avaliação de impactos à proteção de dados;

b) identificação e análise de riscos de privacidade e segurança da informação;

c) identificação e análise de vulnerabilidades; e

d) avaliação dos alertas de segurança da informação emitidos pelas organizações que atuam com privacidade e segurança da informação.

3.4.2. Desenvolvimento de políticas, programas, normas, processos, planos e contratos

Etapa responsável por estabelecer políticas, programas, normas, processos, planos e contratos referentes à controle de acesso, gestão de ativos, registro de *logs* de auditoria, gestão de backups, gestão de vulnerabilidades, gestão de mudanças, recuperação de dados dentre outras atividades essenciais para garantir a privacidade e segurança da informação. Nesta etapa são realizadas as atividades:

a) elaboração de políticas sobre segurança da informação;

b) elaboração do programas, tais como: testes de invasão, conscientização, educação e treinamento em segurança da Informação;

c) elaboração de normas complementares sobre segurança da informação;

d) elaboração de processos de gestão de segurança da informação;

e) elaboração de planos para gestão de processos relacionados à segurança da informação; e

f) estabelecimento de contratos para prestação de serviços, aquisição de *hardwares e softwares* e capacitações envolvendo segurança da informação.

3.4.3. Conscientização, educação e treinamento

Etapa responsável por realizar por ações de conscientização, educação e treinamento em segurança da informação. Nesta etapa são realizadas as atividades:

a) elaboração de estratégias para realização de campanhas de conscientização, educação e treinamento sobre a importância da segurança da informação;

b) realização de ações de conscientização sobre segurança da informação por meio de divulgação de materiais eletrônicos e impressos;

c) treinamentos com usuários sobre práticas seguras de privacidade e

proteção de dados de forma presencial e online; e

c) disponibilização de materiais educativos sobre segurança da informação através dos canais de comunicação oficiais do IFTO.

3.4.4. Configuração de infraestrutura de rede

Etapa responsável por configurar, dispositivos de rede, servidores, *firewalls,* ferramentas e aplicações para a implementação dos controles de privacidade e segurança da informação. Nesta etapa são realizadas as atividades:

a) configuração de infraestrutura adequada para a privacidade e segurança da informação;

b) manutenção preventiva e corretiva de *hardware e software* relacionados a rede de computadores, tais como servidores, switches, firewalls, access points; e

d) implementação de atualizações de segurança para recursos de redes, sistemas operacionais, sistemas de informação e *softwares*.

3.4.5. Implementação de controles de segurança

Etapa responsável por realizar a implementação de controles de segurança da informação, tais como: criptografia para proteger dados confidenciais em trânsito e em repouso, implementação de *softwares* proteção de equipamentos e redes dentre outras atividades. Nesta etapa são realizadas as atividades:

a) implementação de criptografia nos recursos, sistemas operacionais, sistemas de informação e aplicativos;

b) instalação e configuração de antivírus nos ativos institucionais;

c) instalação e configuração de sistemas prevenção e detecção de intrusão; e

d) instalação e configuração de controles de proteção relacionados ao uso de sistemas operacionais e *softwares* institucionais.

3.4.6. Implementação de controles de privacidade

Etapa responsável por realizar a implementação de controles de privacidade. Nesta etapa são realizadas as atividades:

a) identificação e classificação dados pessoais e sensíveis para garantir seu tratamento adequado; e

b) configuração de mecanismos de controle de acesso a dados sensíveis.

3.4.7. Gestão de fornecedores e terceiros

Etapa responsável por gerenciar contratos com empresas fornecedoras de *softwares*, *hardwares* e serviços especializados em privacidade e segurança da informação. Esta etapa faz a avaliação da segurança da informação de fornecedores e parceiros de negócios. Nesta etapa é realizada a atividade:

a) estabelecimento de acordos contratuais que garantam a conformidade com os padrões de segurança e privacidade do IFTO.

3.4.8. Gestão de incidentes de segurança da informação

Etapa responsável pela implementação de ferramentas de monitoramento de incidentes de segurança da informação para identificar atividades suspeitas ou não autorizadas. Nesta etapa são realizadas as atividades:

a) definição dos procedimentos para detecção, análise, contenção, resposta e documentação sobre incidentes de segurança da informação; e

b) definição dos documentos para registro das atividades realizadas.

3.4.9. Gestão de continuidade de negócios

Etapa responsável pela implementação de soluções para continuidade de negócios. Nesta etapa são realizadas as atividades:

a) definição dos procedimentos para a gestão de continuidade de negócios; e

b) definição dos documentos para registro das atividades realizadas.

3.4.10. Auditorias e revisões

Etapa responsável pela condução de auditorias sobre os controles de privacidade e segurança da informação com a finalidade de avaliar se as ações realizadas são suficientes para assegurar a confiabilidade, autenticidade, disponibilidade no contexto do IFTO. Nesta etapa é realizada a atividade:

a) validação prática das políticas, programas, planos, processos, controles e procedimentos operacionais.

3.4.11. Conformidade regulatória

Etapa responsável pela garantia de que o plano de gestão de segurança da informação esteja em conformidade com regulamentos de privacidade, como o GDPR, LGPD, CCPA, entre outros. Nesta etapa são realizadas as atividades:

a) avaliações de conformidade utilizando como parâmetros as recomendações da legislação pertinente à privacidade e segurança da

informação; e

b) elaboração de relatórios de conformidade exigidos por regulamentações específicas.

3.4.12. Melhoria contínua

Etapa responsável por realizar a análise crítica dos resultados obtidos através da execução das etapas anteriores. Nesta etapa são realizadas as atividades:

a) revisão das políticas, programa, processos, normas, planos, procedimentos, contratos, acordos envolvendo privacidade e segurança da informação de acordo com a legislação pertinente à administração pública federal; e

b) adaptação do plano de gestão de privacidade e segurança da informação de acordo com as ameaças cibernéticas, vulnerabilidades, tecnologias e regulamentos.

4. PAPÉIS E RESPONSABILIDADES

Os papéis e responsabilidades para a execução do plano de gestão de segurança da informação no IFTO são definidos com base na Instrução Normativa nº 1, de 27 de maio de 2020 e a Portaria SGD/MGI nº 852, de 28 de março de 2023.

5. MATRIZ RACI

A matriz RACI apresentada na tabela 1 é utilizada para definir com clareza as atribuições, papéis e responsabilidades de cada colaborador nas atividades do processo. A sigla RACI significa, em inglês: *responsible, accountable, consulted e informed.*

a) ***responsible (responsável):*** pessoa, função ou unidade organizacional responsável pela execução de uma atividade no âmbito de um processo;

b) ***accountable (responsabilizado):*** dono da atividade, deverá fornecer os meios para que a atividade possa ser executada, e será responsabilizado caso a atividade não alcance os seus objetivos; Cada atividade só pode possuir um a*ccountable*;

c) ***consulted (consultado):*** pessoas que deverão ser consultadas durante a execução da atividade; As informações levantadas junto a essas pessoas tornam-se entradas para a execução da atividade;

d) ***informed (informado):*** pessoas que serão informadas acerca do progresso da execução da atividade.

Tabela 1 - Matriz de responsabilidades

Etapa	AA	CSI	GSI	ETIR	STI	U

Monitoramento de ameaças e vulnerabilidades.	A	C	C	C	R	I
Desenvolvimento de políticas, programas, normas, processos, planos e contratos.	A	C	C	R	C	I
Conscientização, educação e treinamento.	A	C	R	C	C	I
Configuração da infraestrutura da rede.	A	C	C	C	R	I
Implementação de controles de segurança.	A	C	C	C	R	I
Implementação de controles de privacidade.	A	C	C	C	R	I
Gestão de fornecedores e terceiros.	A	C	C	C	R	I
Gestão de incidentes de segurança da informação.	A	C	C	C	R	I
Gestão de continuidade de negócios.	A	C	C	C	R	I
Auditorias e revisões.	A	C	C	R	C	I
Conformidade regulatória.	A	C	C	R	C	I
Melhoria contínua.	A	C	C	R	C	I

Fonte: Diretoria de Tecnologia da Informação

Legenda:

AA: Alta Administração

CSI: Comitê de Segurança da Informação.

GSI: Gestor de Segurança da Informação.

ETIR: Equipe de Tratamento de Incidente de Segurança da Informação.

STI: Setor de Tecnologia da Informação (Diretoria de Tecnologia da Informação e setores de TI das unidades do IFTO).

U: Usuário

6. INDICADOR DE DESEMPENHO

As atividades de segurança da informação dos recursos de processamento da informação, inclusive dos recursos de computação em nuvem serão monitoradas e constantemente medidas através de indicador de desempenho. Esse indicador tem como objetivo acompanhar a eficácia do processo, identificando tendências, falhas e oportunidades de correções, promovendo sempre a melhoria contínua. A tabela 2 apresenta o indicador de desempenho do processo.

Tabela 2 - Indicador de desempenho

Indicador	Número de controles de segurança da informação gerenciados durante o ano.
Objetivo	Aumentar o número de controles de segurança da informação gerenciados durante o ano.
Periodicidade	Anual.
Fonte	Diretoria de Tecnologia da Informação.

Fórmula	Somatório de controles de segurança da informação gerenciados durante o ano.
Meta	Aumentar o número de controles de privacidade e segurança da informação aplicados durante o ano.

Fonte: Diretoria de Tecnologia da Informação

7. PRÁTICAS RECOMENDADAS

Para as atividades de privacidade e gestão da segurança dos recursos de processamento da informação, inclusive dos recursos de computação em nuvem sejam executadas com eficiência foram estabelecidas as seguintes práticas a serem observadas:

1. A instituição deve elaborar políticas, programas, normas, processos, procedimentos e controles inerentes à gestão da privacidade e segurança dos recursos de processamento da informação, inclusive dos recursos de computação em nuvem.

2. A instituição deve executar atividades de gestão de privacidade segurança dos recursos de processamento da informação, inclusive dos recursos de computação em nuvem.

3. A instituição deve gerenciar (inventariar e controlar) os dispositivos conectados em sua rede.

4. A instituição deve gerenciar (inventariar e controlar) os *softwares* instalados nos dispositivos conectados em sua rede.

5. A instituição deve gerenciar vulnerabilidades técnicas em seus ativos de *software*, de *hardware* e de rede críticos para o negócio.

6. A instituição deve implementar configurações seguras em seus ativos de *software*, *hardware* e de rede críticos para o negócio.

7. A instituição deve manter, monitorar e analisar *logs* de auditoria dos ativos de *software, de hardware* e de rede críticos para o negócio.

8. A instituição deve aplicar controles compensatórios para o uso de privilégios administrativos em seus ativos de *software*, de *hardware* e de rede críticos para o negócio.

9. A instituição deve implementar defesas contra *malware* (ex. vírus) e outras ameaças cibernéticas (ex. *phishing*).

10. A instituição deve limitar e controlar o uso de portas, protocolos e serviços de rede nas conexões de sua rede interna com a internet e outras redes externas.

11. A instituição deve implementar defesa de perímetro das conexões de sua rede interna com a internet e outras redes externas.

12. A instituição deve implementar cópias regulares de segurança (*backup*) das informações em meio digital, conforme as melhores práticas e as necessidades de negócio, incluindo a realização periódica de testes de recuperação das informações.

13. A instituição deve executar regularmente testes de segurança em seu ambiente de TI (detecção de vulnerabilidades e testes de penetração).

14. A instituição deve implementar controles de acesso físicos e lógicos à informação e aos ativos associados à informação que são por ela gerenciados ou custodiados, com vistas a proteger adequadamente a confidencialidade das informações não públicas e a integridade e a disponibilidade das informações consideradas críticas para o negócio.

15. A instituição deve instituir uma política, princípios, objetivos, diretrizes, principais atividades e responsabilidades relativas ao processo de gestão de privacidade e segurança da informação.

16. A instituição deve avaliar periodicamente o desempenho e a conformidade do processo de gestão de privacidade e segurança da informação e promover eventuais ajustes necessários.

8. **REFERÊNCIAS**

ABNT. NBR 16167, de 4 de maio de 2013. **Estabelece as diretrizes básicas para classificação, rotulação e tratamento das informações de acordo com sua sensibilidade e criticidade para a organização, visando o estabelecimento de níveis adequados de proteção.** (ABNT, 2013). Brasil, 2013.

BRASIL. **Norma Complementar 20/IN01/DSIC/GSIPR, de 15 de julho de 2014.** Estabelece as diretrizes de Segurança da Informação e Comunicações para instituição do processo de tratamento da informação, envolvendo todas as etapas do ciclo de vida da informação, no âmbito da Administração Pública Federal, direta e indireta**.** (BRASIL , 2014).

ABNT. NBR ISO/IEC 27032. Tecnologia da Informação. **Técnicas de segurança: diretrizes para segurança cibernética.** (ABNT, 2015). Brasil, 2015.

ABNT. NBR ISO/IEC 27017. Tecnologia da Informação. **Técnicas de segurança. Código de prática para controles de segurança da informação com base ABNT NBR ISO/IEC 27002 para serviços em nuvem.** (ABNT, 2016). Brasil, 2016.

ABNT. NBR ISO/IEC 27004:2017. **Tecnologia da Informação. Técnicas de Segurança: Sistemas de gestão da segurança da informação: monitoramento, medição, análise e avaliação.** (ABNT, 2017). Brasil, 2017.

BRASIL. Gabinete de Segurança Institucional. Secretaria de Coordenação de Sistemas. Departamento de Segurança da Informação e Comunicações. **Norma complementar 14/IN01/DSIC/SCS/GSIPR. Princípios, diretrizes e responsabilidades relacionados à segurança da informação para o tratamento da informação em ambiente de computação em nuvem.** Brasil, 2018. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/42764/9/Norma%20Complementar_14_R01_%20Seguranca%20da%20Informacao%20-Nuvem.pdf Acesso em: 03 jan. 2021.

ABNT. NBR ISO/IEC 27005:2019. **Tecnologia da informação. Técnicas de segurança: Gestão de riscos de segurança da informação.** (ABNT, 2019a). Brasil, 2019.

ABNT. NBR ISO/IEC 27701. Técnicas de Segurança. **Extensão da ABNT NBR/ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação: requisitos e diretrizes.** (ABNT, 2019b). Brasil, 2019.

ABNT. NBR ISO/IEC 27003:2020. **Tecnologia da informação. Técnicas de segurança: Sistemas de gestão da segurança da informação. Orientações.** (ABNT, 2020). Brasil, 2020.

ABNT. NBR ISO/IEC 27007. **Segurança da Informação, segurança cibernética e proteção da privacidade: diretrizes para auditoria de sistemas de gestão de segurança da informação.** (ABNT, 2021). Brasil, 2021.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Portaria **Nº 93, de 18 de outubro de 2021: Glossário de segurança da informação.** (BRASIL, 2021).

ABNT. NBR ISO/IEC 27001:2022. **Segurança da informação, segurança cibernética e proteção à privacidade: sistemas de gestão da segurança da informação. Requisitos.** (ABNT, 2022a). Brasil, 2022.

ABNT. NBR ISO/IEC 27002:2022. **Segurança da informação, segurança cibernética e proteção à privacidade de segurança. Controles de segurança da informação.** (ABNT, 2022b). Brasil, 2022.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Instrução Normativa Nº 1, de 27 de maio de 2020. Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.** Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215. Acesso em: 06 set. de 2023.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Instrução Normativa Nº 3, de 28 de maio de 2021. Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.** Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-gsi/pr-n-3-de-28-de-maio-de-2021-322963172. Acesso em: 06 de set. 2023.

BRASIL. Presidência de República. Ministério da Gestão e da inovação em serviços públicos. **Guia do framework de privacidade e segurança da informação. Programa de privacidade e segurança da informação.** Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf Acesso em: 17 abr. 2023.

CENTER FOR INTERNET SECURITY, INC. **Controles CIS Versão 8.** Disponível em: https://www.cisecurity.org/controls/v8/ (CIS, 2023). Acesso em 20/12/2021 às 09:54.

ANEXO I
PLANO DE TRABALHO

A área de TI do IFTO tem utilizado nos últimos anos como

referência para a gestão de privacidade e segurança da informação os controles de segurança definidos pelo *Center for Internet Security* (CIS, 2023) e normas ABNT 27001 (ABNT, 2022a) e 27002 (ABNT, 2022b). Estes controles possibilitam aumentar o nível de maturidade em relação ao processo de gestão de segurança da informação como também são mecanismos de defesa cibernética. Atualmente nem todos os controles estão implantados, pois estão em fase de estudo de viabilidade técnica.

Os controles de privacidade e segurança da informação *Critical Security Controls* são práticas recomendadas no mercado formuladas por grupo de especialistas em TI que utilizam informações coletadas de ataques reais e suas defesas eficazes. Estas práticas fornecem orientação específica e um caminho claro para que as organizações atinjam os objetivos e metas descritos por várias estruturas legais, regulamentares e políticas (CIS, 2023). As próximas seções detalham os controles para a execução de atividades de gestão de segurança dos recursos de processamento da informação, inclusive dos recursos de computação em nuvem que serão utilizados pelo IFTO nos próximos anos.

1. Controles de Segurança

1.1. Inventário e controle de ativos corporativos

Este controle é responsável por gerenciar ativamente (inventariar, rastrear e corrigir) todos os ativos da empresa (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos de rede; dispositivos não informáticos / IoT - Internet das Coisas; e servidores) conectados à infraestrutura fisicamente, virtualmente, remotamente, e aqueles em ambientes de nuvem, para saber com precisão a totalidade de ativos que precisam ser monitorados e protegidos dentro da empresa. Isso também apoiará a identificação de ativos não autorizados e não gerenciados para remover ou corrigir.

Segundo a norma ABNT 27002 (ABNT, 2022b) convém que todos os ativos sejam inventariados e tenham um proprietário responsável. Para CIS (CIS, 2023), a instituição deve ter gestão ativa (inventariar, rastrear e corrigir) de todos os ativos corporativos (dispositivos de usuário final, incluindo portáteis e móveis, dispositivos de rede, dispositivos não computacionais; internet das coisas (IoT) e servidores conectados fisicamente à infraestrutura, virtualmente, remotamente e aqueles em ambientes de nuvem, para saber com precisão a totalidade dos ativos que precisam ser monitorados e protegidos dentro da instituição.

Para CIS (2023) a gestão do controle de todos os ativos corporativos exerce papel crítico no monitoramento de segurança, resposta a incidentes, backup e recuperação de sistemas. As empresas devem saber quais dados são essenciais para elas, e a gestão adequada de ativos ajudará a identificar os ativos corporativos que mantém ou gerenciam esses dados críticos, para que os controles de segurança apropriados possam ser aplicados. No IFTO este controle é gerenciado

através de várias soluções de tecnologia da informação, como por exemplo a ferramenta GLPI, software de gerenciamento de serviços baseado em tecnologias de código aberto.

1.1.1. **Procedimentos e ferramentas**

1. Inventário de ativos de corporativos de TI;

2. Definir os proprietários dos ativos;

3. Classificação da informação;

4. Varredura ativa e descoberta de vulnerabilidades na rede por meio de ferramentas de varredura de rede (*logs*, registros de plataforma corporativa (sistemas, portais, VPN, IDS, IPS, DPI, MDM).

1.1.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotadas para o inventário e controle de ativos corporativos. Dentre elas tem-se as atividades apresentadas na tabela 1.

Tabela 1 - Atividades para o inventário e controle de ativos corporativos

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramenta de Apoio
Estabelecer e manter um inventário detalhado de ativos corporativos.	Dispositivo	Identificar	Semanalmente	GLPI ZABBIX PFSENSE
Endereçar ativos não autorizados.	Dispositivo	Responder	Semanalmente	PFSENSE
Utilizar uma ferramenta de descoberta ativa para identificar ativos conectados à rede.	Dispositivo	Detectar	Semanalmente	NMAP NESSUS
Usar o *Dynamic Host Configuration Protocol* (DHCP) para atualizar o inventário de ativos corporativos.	Dispositivo	Identificar	Diariamente	PFSENSE
Usar uma ferramenta de descoberta passiva para	Dispositivo	Detectar	Semanalmente	NMAP NESSUS

identificar ativos conectados à rede corporativa.				

1.2. Inventário e controle de ativos de software

Segundo CIS (2023) este controle é responsável pela gestão ativa (inventariar, rastrear e corrigir) de todos os *softwares* (sistemas operacionais e aplicações) na rede para que apenas o *software* autorizado seja instalado e possa ser executado, e que o *software* não autorizado e não gerenciado seja encontrado e impedido de ser instalado ou executado.

1.2.1. **Procedimentos e ferramentas**

1. Lista de permissões;

2. Ferramenta de inventário de software.

1.2.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotadas para o inventário e controle de ativos de *software*. Dentre elas tem-se as atividades apresentadas na tabela 2.

Tabela 2 - Atividades para o inventário e controle de ativos de software

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramenta de Apoio
Estabelecer e manter um inventário detalhado de *softwares* licenciados instalados em ativos corporativos.	Aplicações	Identificar	Semestralmente	-

Assegurar que apenas o *software* com suporte atualmente suportado seja designado como autorizado no inventário de software para ativos corporativos.	Aplicações	Identificar	Mensalmente	-
Assegurar que o software não autorizado seja retirado do uso em ativos corporativos ou receba uma exceção documentada.	Aplicações	Responder	Mensalmente	-
Utilizar ferramentas de inventário de *software*, quando possível, em todo o IFTO para automatizar a descoberta e documentação do *software* instalado.	Aplicações	Detectar	Diariamente	-
Usar controles técnicos, como a lista de permissões de aplicativos, para garantir que apenas software autorizado possa executar ou ser acessado.	Aplicações	Proteger	Semestralmente	-
Usar controles técnicos para garantir que apenas bibliotecas de *software* autorizadas, como arquivos .dll,	Aplicações	Proteger	Semestralmente	-

.ocx, .so, etc. específicos, tenham permissão para carregar em um processo do sistema. Bloquear o carregamento de bibliotecas não autorizadas em um processo do sistema.				
Usar controles técnicos, como assinaturas digitais e controle de versão, para garantir que apenas scripts autorizados, como arquivos .ps1, .py, etc. específicos, tenham permissão para executar. Bloquear a execução de scripts não autorizados.	Aplicações	Proteger	Semestralmente	-

1.3. Proteção de dados

Este controle é responsável por utilizar processos e controles técnicos para identificar, classificar, manusear, reter e descartar dados com segurança (BRASIL, 2023; CIS, 2023). Para CIS (2023) os dados devem ser gerenciados de maneira adequada em todo o seu ciclo de vida. O IFTO deve desenvolver um processo de gestão de dados que inclua um *framework* de gestão de dados, diretrizes de classificação de dados e requisitos para proteção, manuseio, retenção e descarte de dados.

A instituição deve desenvolver processos e controles técnicos para identificar, classificar, manusear com segurança, reter e descartar dados. Segundo a ABNT 27002 (ABNT, 2022b) deve-se assegurar que a informação receba um nível adequado de proteção. A informação deve ser classificada para indicar a necessidade, prioridades e o nível esperado de proteção quando do tratamento da informação (ABNT, 2013).

A implementação do controle de proteção de dados pode

ajudar a proteger uma infinidade de informações em uma rede corporativa, incluindo Informações de Identificação pessoais. A área de TI utiliza várias soluções para proteção de dados, como por exemplo: *firewalls*, antivírus, criptografia entre outros.

1.3.1. **Procedimentos e ferramentas**

1. Processo de gerenciamento de dados;
2. Inventário ou mapeamento de dados;
3. Lista de controle de acesso a dados;
4. Esquema de classificação de dados;
5. Fluxo de dados de documentos.

1.3.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotados para a proteção de dados. Dentre elas tem-se as atividades apresentadas na tabela 3.

Tabela 3 - Atividades para a proteção de dados

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramenta de Apoio
Estabelecer e manter um processo de gestão de dados.	Dados	Identificar	Anualmente	SEI
Estabelecer e manter um inventário de dados.	Dados	Identificar	Anualmente	SEI
Configurar listas de controle de acesso a dados com base na necessidade de um usuário.	Dados	Proteger	-	-
Reter os dados de acordo com o processo de gerenciamento de dados da empresa. A retenção de dados deve incluir cronogramas mínimo e máximo.	Dados	Proteger	-	-
Eliminar os dados com segurança	Dados	Proteger	-	-

conforme descrito no processo de gerenciamento de dados da empresa. Certificar-se de que o processo e o método de descarte sejam proporcionais à sensibilidade dos dados.				
Criptografar os dados em dispositivos do usuário final contendo dados confidenciais. Implementações de exemplo podem incluir: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	Dispositivos	Proteger	-	-
Estabelecer e manter um esquema geral de classificação de dados para a empresa. As empresas podem usar rótulos, como “Sensível”, “Confidencial” e “Público”, e classificar seus dados de acordo com esses rótulos. Revisar e atualizar o esquema de classificação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta proteção.	Dados	Identificar	-	-
Documentar fluxos de dados do documento. A documentação do fluxo de dados inclui	Dados	Identificar	Anualmente	SEI

fluxos de dados do provedor de serviços e deve ser baseada no processo de gerenciamento de dados da empresa. Revisar e atualizar a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam afetar esta proteção.				
Criptografar dados em mídia removível.	Dados	Proteger	-	-
Criptografar dados confidenciais em trânsito. Implementações de exemplo podem incluir: Transport Layer Security (TLS) e Open Secure Shell (OpenSSH).	Dados	Proteger	-	-
Criptografar dados confidenciais em repouso em servidores, aplicativos e bancos de dados que contenham dados sensíveis. A criptografia da camada de armazenamento, também conhecida como criptografia do lado do servidor, atende ao requisito mínimo desta proteção. Métodos de criptografia adicionais podem incluir criptografia de camada de aplicativo, também	Dados	Proteger	-	-

conhecida como criptografia do lado do cliente, em que o acesso ao (s) dispositivo (s) de armazenamento de dados não permite o acesso aos dados de texto simples.				
Segmentar o processamento e armazenamento de dados com base na sensibilidade dos dados. Não processar dados sensíveis em ativos corporativos destinados a dados de menor sensibilidade.	Rede	Proteger	-	-
Implementar uma ferramenta automatizada, como uma ferramenta de prevenção de perda de dados (DLP) baseada em host, para identificar todos os dados confidenciais armazenados, processados ou transmitidos por meio de ativos da empresa, incluindo aqueles situados no local ou em um provedor de serviços remoto, e atualizar o inventário de dados sensíveis do IFTO.	Dados	Proteger	-	-
Registrar o acesso a dados confidenciais, incluindo modificação e descarte.	Dados	Detectar	-	-

1.4. Configuração segura de ativos corporativos e *software*

Este controle é responsável por estabelecer e manter a configuração segura de ativos institucionais (dispositivos de usuário final, incluindo portáteis e móveis, dispositivos de rede, dispositivos não computacionais/IoT, servidores e software (sistemas operacionais e aplicações). Para CIS (2023) a instituição deve estabelecer e manter a configuração segura de ativos corporativos (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos de rede; dispositivos não computacionais/IoT; e servidores) e *software* (sistemas operacionais e aplicações). A partir da classificação de riscos dos dados, os ativos corporativos e *softwares* são configurados.

1.4.1. **Procedimentos e ferramentas**

1. Determine a classificação de risco dos dados manipulados/armazenados no ativo corporativo (por exemplo, risco alto, moderado, baixo).

2. Crie um *script* de configuração de segurança que defina as configurações de segurança do sistema para atender aos requisitos para proteger os dados usados no ativo corporativo. Use benchmarks, como os descritos anteriormente nesta seção.

3. Instale o *software* básico do sistema operacional.

4. Aplique o sistema operacional e os *patches* de segurança apropriados.

5. Instale os pacotes, ferramentas e utilitários de *software* de aplicação apropriados.

6. Aplique as atualizações apropriadas.

7. Instale *scripts* de customização locais nesta imagem.

8. Execute o *script* de segurança para definir o nível de segurança apropriado.

9. Execute uma ferramenta compatível com o SCAP para registrar/pontuar a configuração do sistema da imagem do *baseline*.

10. Execute um teste de garantia de qualidade de segurança.

11. Salve esta imagem de base em um local seguro.

1.4.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotadas para configuração segura de ativos corporativos e *software*. Dentre elas tem-se as atividades apresentadas na tabela 4.

Tabela 4 - Atividades para configuração segura de ativos corporativos e *software*

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramenta de Apoio

Estabelecer e manter um processo de configuração segura para ativos corporativos (dispositivos de usuário final, incluindo dispositivos portáteis e móveis, não computacionais / IoT e servidores) e software (sistemas operacionais e aplicativos). Revisar e atualizar a documentação anualmente ou quando ocorrerem mudanças significativas no IFTO que possam impactar esta medida de segurança.	Aplicações	Proteger	Anualmente	-
Estabelecer e manter um processo de configuração segura para infraestrutura de rede. Revisar e atualizar a documentação anualmente ou quando ocorrerem mudanças significativas no IFTO que possam afetar esta medida de segurança.	Rede	Proteger	Anualmente	-
Configurar o bloqueio automático de sessão em ativos corporativos após um período definido de inatividade.	Usuários	Proteger	-	-
Implementar e gerenciar um firewall nos servidores, onde houver suporte. Implementações de exemplo incluem um firewall virtual, firewall do sistema operacional ou um agente de firewall	Dispositivo	Proteger	-	Windows Defender PFSENSE

de terceiros.				
Implementar e gerenciar um firewall baseado em host ou uma ferramenta de filtragem de porta em dispositivos de usuário final, com uma regra de negação padrão que elimina todo o tráfego, exceto os serviços e portas que são explicitamente permitidos.	Dispositivo	Proteger	-	Windows Defender PFSENSE
Gerenciar com segurança ativos e software corporativos. Implementações de exemplo incluem gerenciamento de configuração por meio de infraestrutura controlada por versão como código e acesso a interfaces administrativas em protocolos de rede seguros, como Secure Shell (SSH) e *Hypertext Transfer Protocol* Secure (HTTPS). Não usar protocolos de gerenciamento inseguros, como Telnet (Teletype Network) e HTTP, a menos que seja operacionalmente essencial.	Rede	Proteger	-	-
Gerenciar contas padrão em ativos e software corporativos, como root, administrador e outras contas de fornecedores pré-configuradas. Implementações de exemplo podem incluir: desativar contas padrão ou torná-las inutilizáveis.	Usuários	Proteger	-	-

Desinstalar ou desativar serviços desnecessários em ativos e software corporativos, como um serviço de compartilhamento de arquivos não utilizado, módulo de aplicativo da web ou função de serviço.	Dispositivo	Proteger	-	-
Configurar servidores DNS confiáveis em ativos corporativos. As implementações de exemplo incluem: configuração de ativos para usar servidores DNS controlados pela empresa e/ou servidores DNS confiáveis acessíveis externamente.	Dispositivo	Proteger	-	DNS IFTO DNS Google
Impor o bloqueio automático de dispositivo seguindo um limite predeterminado de tentativas de autenticação local com falha em dispositivos portáteis de usuário final, quando compatível.	Dispositivo	Responder	-	Active Directory
Impor capacidade de limpeza remota nos dados nos dispositivos portáteis de usuário final de propriedade do IFTO quando for considerado apropriado, como dispositivos perdidos ou roubados, ou quando um indivíduo não oferecer mais suporte ao IFTO.	Dispositivo	Proteger	-	-
Separar espaços de trabalho corporativos em dispositivos móveis	Dispositivo	Proteger	-	-

de usuário final, onde houver suporte.				

1.5. Gestão de contas

Controle responsável por usar processos e ferramentas para atribuir e gerenciar autorização de credenciais para contas de usuário, incluindo contas de administrador, contas de serviço para ativos e *softwares* institucionais (BRASIL, 2023). A instituição deve usar processos e ferramentas para atribuir e gerenciar autorização de credenciais para contas de usuário, incluindo contas de administrador, bem como contas de serviço, de ativos corporativos e *software* (CIS, 2023).

O gerenciamento de contas é aplicável a todos os aplicativos, dispositivos e serviços. Todos os usuários precisarão de uma conta para acessar aplicativos, dispositivos e provedores de serviços internos ou externos. O registro e o monitoramento de contas são componentes críticos das operações de segurança. O IFTO deve desenvolver políticas de senha adequadas e orientações para não reutilizar senhas.

As contas devem ser rastreadas. Qualquer conta que esteja inativa deve ser desabilitada e eventualmente removida do sistema. Deve haver auditorias periódicas para garantir que todas as contas ativas sejam rastreadas para usuários autorizados do ativo corporativo. Os usuários devem usar aplicações de gestão de senhas para armazenar com segurança suas senhas e devem ser instruídos a não mantê-las em planilhas ou arquivos de texto em seus computadores. O IFTO utiliza o SUAP para o gerenciamento de contas de usuários.

1.5.1. **Procedimentos e ferramentas**

1. Desenvolver um programa abrangente de gestão de acesso e identidades (*Identity and Access Management - IAM*);

2. Identificar e rastrear contas administrativas ou de alto privilégio e contas de serviço;

3. Auditoria periódicas.

1.5.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotadas para a gestão de contas. Dentre elas tem-se as atividades apresentadas na tabela 5.

Tabela 5 - Atividades para gestão de contas

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramer de Apoi

Estabelecer e manter um inventário de todas as contas gerenciadas no IFTO.	Identificar	Trimestralmente.	Active Directory	
Usar senhas exclusivas para todos os ativos institucionais.	Usuários	Proteger	-	Active Directory
Excluir ou desabilitar quaisquer contas inativas após um período determinado de inatividade, quando houver suporte.	Usuários	Responder	-	Active Directory
Restringir os privilégios de administrador a contas de administrador dedicadas em ativos corporativos. Realizar atividades gerais de computação, como navegação na Internet, e-mail e uso do pacote de produtividade, a partir da conta primária não privilegiada do usuário.	Usuários	Proteger	-	Active Directory
Estabelecer e manter um inventário de contas de serviço.	Usuários	Identificar	-	Active Directory
Centralizar o gerenciamento de contas por meio de um diretório ou serviço de identidade.	Usuários	Proteger	-	Active Directory

1.6. Gestão do controle de acesso

Controle responsável por usar processos e ferramentas para criar, atribuir, gerenciar e revogar credenciais de acesso e privilégios para contas de usuário, administrador e serviço para ativos e software institucionais (BRASIL, 2023). O controle de gerenciamento de acesso destina-se a gerenciar grande parte do processo de autenticação e autorização, desde como um usuário acessa um dispositivo até a revogação de credenciais e privilégios de acesso.

A instituição deve usar processos e ferramentas para criar,

atribuir, gerenciar e revogar credenciais de acesso e privilégios para contas de usuário, administrador e serviço para ativos e software corporativos. Para a norma ABNT 27002 (ABNT, 2022b) a instituição deve assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação (ABNT, 2013). Esta prática é responsável pelo controle de acesso à informação e aos ativos associados à informação.

1.6.1. **Procedimentos e ferramentas**

1. Procedimento forma de registro e cancelamento de usuários;
2. Gerenciamento de senha de usuário;
3. Gerenciamento de acesso privilegiado;
4. Inventariar e rastrear contas de serviço;
5. Listas de processos em execução.

1.6.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotadas para a gestão do controle de acesso. Dentre elas tem-se as atividades apresentadas na tabela 6.

Tabela 6 - Atividades para gestão de contas

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramenta de Apoio
Estabelecer e seguir um processo, de preferência automatizado, para conceder acesso aos ativos do IFTO mediante nova contratação, concessão de direitos ou mudança de função de um usuário.	Usuários	Proteger	-	Active Directory SUAP
Estabelecer e seguir um processo, de preferência automatizado, para revogar o acesso aos ativos do IFTO, por meio da desativação de contas imediatamente após o encerramento, revogação de direitos ou mudança de função de um usuário. Desativar contas, em vez de excluí-las, pode ser necessário para preservar as trilhas de auditoria.	Usuários	Proteger	-	Active Directory SUAP

Exigir que todas as aplicações corporativas ou de terceiros expostas externamente apliquem o MFA quando houver suporte.	Usuários	Proteger	Revisar e atualizar anualmente	E-mail. Federação CAFe GOV.BR
Exigir MFA para acesso remoto à rede.	Usuários	Proteger	-	-
Exigir MFA para todas as contas de acesso administrativo, onde houver suporte, em todos os ativos do IFTO, sejam gerenciados no local ou por meio de um provedor terceirizado.	Usuários	Proteger	-	-
Estabelecer e manter um inventário dos sistemas de autenticação e autorização do IFTO, incluindo aqueles hospedados no local ou em um provedor de serviços remoto.	Usuários	Identificar	Anualmente	-
Centralizar o controle de acesso para todos os ativos da empresa por meio de um serviço de diretório ou provedor de SSO, onde houver suporte.	Usuários	Proteger	-	-
Definir e manter o controle de acesso baseado em funções, determinando e documentando os direitos de acesso necessários para cada função dentro da empresa para cumprir com sucesso suas funções atribuídas. Realizar análises de controle de acesso de ativos corporativos para validar se todos os privilégios estão autorizados.	Dados	Proteger	Anualmente	-

1.7. Gestão contínua de vulnerabilidades

Controle responsável por desenvolver um plano para avaliar e rastrear vulnerabilidades continuamente em todos os ativos dentro da infraestrutura do IFTO, a fim de remediar e minimizar a janela de oportunidade para atacantes. Monitorar as fontes públicas e privadas

para novas informações sobre ameaças e vulnerabilidades.

Segundo Brasil (2023) este controle é voltado ao monitoramento de possíveis vulnerabilidades em softwares ou hardwares usados pela instituição. Abrange processos para tomada de decisões com ações proativas e correções naquilo que possa comprometer a privacidade, incluindo ações defensivas.

A instituição deve desenvolver um plano para avaliar e rastrear vulnerabilidades continuamente em todos os ativos corporativos dentro da infraestrutura da instituição, a fim de remediar e minimizar a janela de oportunidade para atacantes. Deve-se monitorar fontes públicas e privadas para novas informações sobre ameaças e vulnerabilidades. A área de TI realiza a gestão contínua de vulnerabilidades por meio de *softwares* livres.

1.7.1. **Procedimentos e ferramentas**

1. Ferramentas de varredura de vulnerabilidades.

2. Processo de garantia de qualidade para verificar as atualizações de configuração ou *patches* implementados corretamente em todos os ativos.

1.7.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotadas para a gestão contínua de vulnerabilidades. Dentre elas tem-se as atividades apresentadas na tabela 7.

Tabela 7 - Atividades para gestão contínua de vulnerabilidades

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramenta de Apoio
Estabelecer e manter um processo de gestão de vulnerabilidade documentado para ativos corporativos.	Aplicações	Proteger	Anualmente	SEI
Estabelecer e manter uma estratégia de remediação baseada em risco documentada em um processo de remediação, com revisões mensais ou mais frequentes.	Aplicações	Responder	Mensalmente	SEI
Executar atualizações do sistema operacional em	Aplicações	Proteger	Mensalmente	Rundeck Playlist Windows Update

ativos corporativos por meio do gerenciamento automatizado de *patches.*				
Executar a gestão automatizada de *patches* de aplicações.	Aplicações	Proteger	Mensalmente	
Realizar varreduras automatizadas de vulnerabilidade de ativos corporativos internos. Realizar varreduras autenticadas e não autenticadas, usando uma ferramenta de varredura de vulnerabilidade compatível com SCAP.	Aplicações	Identificar	Trimestralmente	Nessus Wazuh
Executar varreduras de vulnerabilidade automatizadas de ativos corporativos expostos externamente usando uma ferramenta de varredura de vulnerabilidade compatível com SCAP.	Aplicações	Identificar	Mensalmente	Nessus Wazuh
Corrigir as vulnerabilidades detectadas no software por meio de processos e ferramentas.	Aplicações	Responder	Mensalmente	-

1.8. Gestão de registros de auditoria

Controle responsável por coletar, alertar, analisar e reter *logs* de eventos com o objetivo de ajudar a detectar, compreender ou se recuperar de um ataque (BRASIL, 2023). A instituição deve coletar, alertar, analisar e reter *logs* de auditoria de eventos que podem ajudar a

detectar, compreender ou se recuperar de um ataque (CIS, 2023).

1.8.1. **Procedimentos e ferramentas**

1. Servidor de *logs* centralizado;
2. Avaliação periódicas de *logs*.

1.8.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotadas para a gestão de registros de auditoria. Dentre elas tem-se as atividades apresentadas na tabela 8.

Tabela 8 - Atividades para gestão de registros de auditoria

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramenta de Apoio
Estabelecer e manter um processo de gerenciamento de registro de auditoria que defina os requisitos de registro do IFTO. No mínimo, tratar da coleta, revisão e retenção de *logs* de auditoria para ativos corporativos.	Rede	Proteger	Anualmente	-
Coletar *logs* de auditoria.	Rede	Detectar	Diariamente	-
Garantir o armazenamento adequado do registro de auditoria.	Rede	Proteger	Diariamente	-
Padronizar a sincronização de tempo.	Rede	Proteger	Diariamente	Active Directory
Coletar *logs* de auditoria detalhados.	Rede	Detectar	-	-
Coletar *logs* de auditoria de consulta DNS em ativos corporativos, quando apropriado e suportado.	Rede	Detectar	-	-

Coletar *logs* de auditoria de requisição de URL em ativos corporativos, quando apropriado e suportado.	Rede	Detectar	-	-
Coletar *logs* de auditoria de linha de comando.	Dispositivo	Detectar	-	-
Centralizar, na medida do possível, a coleta e retenção de *logs* de auditoria nos ativos corporativos.	Rede	Detectar	-	-
Reter os *logs* de auditoria em ativos corporativos.	Rede	- Proteger	-	-
Realizar análises de *logs* de auditoria para detectar anomalias ou eventos anormais que possam indicar uma ameaça potencial.	Rede	Detectar	-	-
Coletar *logs* do provedor de serviços, quando houver suporte.	Dados	Detectar	-	-

1.9. Proteções de e-mail e navegador Web

Controle responsável por melhorar as proteções e detecções de vetores de ameaças de e-mail e web, pois são oportunidades para atacantes manipularem o comportamento humano por meio do engajamento direto (BRASIL, 2023; CIS, 2023).

A instituição deve melhorar as proteções e detecções de vetores de ameaças de e-mail e web, pois são oportunidades para atacantes manipularem o comportamento humano por meio do engajamento direto.

1.9.1. **Procedimentos e ferramentas**

1. Habilitar filtros de conteúdo e ativar os bloqueadores de pop-up;

2. Assinar serviços de filtragem de DNS para bloquear tentativas de acesso a esses sites no nível da rede;

3. Treinar e encorajar o comportamento correto;

4. Ferramenta de filtragem de spam e verificação de *malware* no *gateway* de e-mail reduz o número de e-mails e anexos maliciosos que chegam à rede corporativa.

1.9.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotadas para proteções de e-mail e navegador web. Dentre elas tem-se as atividades apresentadas na tabela 9.

Tabela 9 - Atividades para proteções de e-mail e navegador web

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramenta de Apoio
Garantir o uso apenas de navegadores e clientes de e-mail suportados plenamente.	Aplicações	Proteger	-	-
Usar serviços de filtragem de DNS em todos os ativos corporativos para bloquear o acesso a domínios mal-intencionados conhecidos.	Rede	Proteger	-	-
Impor e atualizar filtros de URL baseados em rede para limitar um ativo corporativo de se conectar a sites potencialmente maliciosos ou não aprovados.	Rede	Proteger	-	-
Restringir extensões de cliente de e-mail e navegador desnecessárias ou não autorizadas.	Aplicações	Proteger	-	Google
Implementar o DMARC.	Rede	Proteger	-	Servidor DNS

Bloquear tipos de arquivo desnecessários que tentem entrar no *gateway* de e-mail do IFTO.	Rede	Proteger	-	-
Implantar e manter proteções *antimalware* de servidor de e-mail, como varredura de anexos e/ou *sandbox.*	Rede	Proteger	-	-

1.10. Defesas contra *malware*

Controle responsável por impedir ou controlar a instalação, disseminação e execução de aplicações, códigos ou scripts maliciosos em ativos da organização (BRASIL, 2023). Para CIS (2023) a instituição deve impedir ou controlar a instalação, disseminação e execução de aplicações, códigos ou *scripts* maliciosos em ativos corporativos. Segundo a ABNT 27002 (ABNT, 2022b) convém que os usuários estejam conscientes dos perigos do código malicioso e que os gestores, onde apropriado, implantem controles para prevenir, detectar e remover código malicioso e controlar códigos móveis (ABNT, 2013).

1.10.1. **Procedimentos e ferramentas**

1. Atualizações automatizadas de proteção contra *malware*;
2. Coleta centralizada dos *logs*;
3. Política para proibição de softwares não autorizados.

1.10.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotadas para defesas contra *malware*. Dentre elas tem-se as atividades apresentadas na tabela 10.

Tabela 10 - Atividades para defesas contra *malware*

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramenta de Apoio
Instalar e manter um software anti-*malware* em todos os ativos corporativos.	Dispositivo	Detectar	-	-

Configurar atualizações automáticas de assinatura anti-*malware* em todos os ativos corporativos.	Dispositivo	Proteger	-	-
Desabilitar a funcionalidade de execução e reprodução automática para mídias removíveis.	Dispositivo	Proteger	-	-
Configurar a varredura anti-*malware* automática de mídia removível.	Dispositivo	Detectar	-	-
Habilitar recursos anti-exploração.	Dispositivo	Proteger	-	-
Gerenciar o software anti-*malware* de maneira centralizada.	Dispositivo	Proteger	-	-
Usar software anti-*malware* baseado em comportamento.	Dispositivo	Detectar	-	-

1.11. Recuperação de dados

Controle responsável por criar e manter práticas de recuperação de dados que sejam capazes de restaurar os ativos da organização para um estado pré-incidente ou o estado mais confiável possível (BRASIL, 2023). A instituição deve estabelecer e manter práticas de recuperação de dados suficientes para restaurar ativos corporativos dentro do escopo para um estado pré-incidente e confiável.

1.11.1. **Procedimentos e ferramentas**

1. Processo de gestão de dados;
2. Procedimentos de recuperação de dados;
3. Procedimentos de restauração de dados.

1.11.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotadas para

recuperação de dados. Dentre elas tem-se as atividades apresentadas na tabela 11.

Tabela 11 - Atividades para recuperação de dados

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramenta de Apoio
Estabelecer e manter um processo de recuperação de dados.	Dados	Recuperar	Anualmente	-
Executar *backups* automatizados de ativos corporativos.	Dados	Recuperar	Semanalmente	-
Proteger os dados de recuperação com controles equivalentes dos dados originais.	Dados	Proteger	-	-
Estabelecer e manter uma instância isolada de dados de recuperação.	Dados	Recuperar	-	-
Testar os dados de recuperação.	Dados	Recuperar	Trimestralmente	-

1.12. Gestão de infraestrutura de redes

Controle responsável por estabelecer, implementar e gerenciar ativamente (rastreie, reporte e corrija) os dispositivos de rede, a fim de evitar que atacantes explorem serviços de rede e pontos de acesso vulneráveis (BRASIL, 2023). A instituição deve estabelecer, implementar e gerenciar ativamente (rastrear, reportar, corrigir) os dispositivos de rede, a fim de evitar que atacantes explorem serviços de rede e pontos de acesso vulneráveis (CIS, 2023). A aplicação deste controle visa a garantir que a infraestrutura de rede seja mantida e configurada adequadamente durante todo o seu ciclo de vida.

1.12.1. **Procedimentos e ferramentas**

1. Monitorar versões e configurações de infraestrutura em busca de vulnerabilidades;

2. Diagrama de arquitetura de segurança.

1.12.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotadas para gestão de infraestrutura de redes. Dentre elas tem-se as atividades apresentadas na tabela 12.

Tabela 12 - Atividades para gestão de infraestrutura de redes

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramenta de Apoio
Assegurar que a infraestrutura de rede seja mantida atualizada.	Rede	Proteger	Mensalmente	-
Estabelecer e manter uma arquitetura de rede segura.	Rede	Proteger	-	-
Gerenciar infraestrutura de rede com segurança.	Rede	Proteger	-	-
Estabelecer e manter diagrama(s) de arquitetura.	Rede	Identificar	Diariamente	ZABBIX
Centralizar a autenticação, autorização e auditoria (AAA) de rede.	Rede	Proteger	-	-
Usar protocolos de comunicação e gestão de rede seguros.	Rede	Proteger	-	-
Assegurar que os dispositivos remotos utilizem uma VPN e esteja se conectando a uma infraestrutura AAA do IFTO.	Dispositivo	Proteger	-	-
Estabelecer e manter recursos de computação dedicados para todo o trabalho administrativo.	Dispositivo	Proteger	-	-

1.13. Monitoramento e defesa da rede

Controle responsável por implementar processos e

ferramentas para que a organização estabeleça o monitoramento e a defesa de rede contra ameaças de segurança em toda a sua infraestrutura de rede e base de usuários (BRASIL, 2023). A instituição deve operar processos e ferramentas para estabelecer e manter monitoramento e defesa de rede abrangente contra ameaças de segurança em toda a infraestrutura de rede corporativa e base de usuários (CIS, 2023). Para a norma ABNT 27001 (ABNT, 2022a) a instituição deve garantir a proteção das informações em redes e a proteção da infraestrutura de suporte.

1.13.1. **Procedimentos e ferramentas**

1. Controles de rede;
2. Segurança dos serviços de rede;
3. Processo de monitoramento contínuo;
4. Relatório de atividades;
5. Procedimentos de resposta;
6. Registros de auditoria;
7. Monitoramento do uso do sistema;
8. Registro de *log* de administrador e operador;
9. Registro de falhas;
10. Sincronização dos relógios;
11. Revisões semanais de *logs* de auditoria;
12. Ferramentas de correlação de *logs* de auditoria;
13. Ferramentas automatizadas de análise de *log*.

1.13.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotadas para monitoramento e defesa de rede. Dentre elas tem-se as atividades apresentadas na tabela 13.

Tabela 13 - Atividades para monitoramento e defesa da rede

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramenta de Apoio
Centralizar o alerta de eventos de segurança.	Rede	Detectar	-	-
Implantar solução de detecção de intrusão baseada em host.	Dispositivo	Detectar	-	-

Implantar uma solução de detecção de intrusão de rede.	Rede	Detectar	-	-
Realizar filtragem de tráfego entre segmentos de rede.	Rede	Proteger	-	-
Gerenciar controle de acesso para ativos remotos.	Dispositivo	Proteger	-	-
Coletar logs de fluxo de tráfego da rede.	Rede	Detectar	-	-
Implantar solução de prevenção de intrusão baseada em host.	Dispositivo	Proteger	-	-
Implantar uma solução de prevenção de intrusão de rede.	Rede	Proteger	-	-
Implantar controle de acesso no nível de porta.	Dispositivo	Proteger	-	-
Executar filtragem da camada de aplicação.	Rede	Proteger	-	-
Ajustar limites de alerta de eventos de segurança.	Rede	Detectar	Mensalmente	-

1.14. Conscientização sobre segurança e treinamento de competências

Controle responsável por implantar e manter um programa de conscientização de segurança que possa influenciar e conscientizar o comportamento dos colaboradores, tornando-os devidamente qualificados e assim atingir o objetivo de reduzir riscos de segurança cibernética da organização (BRASIL, 2023). A aplicação deste controle destina-se a garantir que os colaboradores recebam treinamento de segurança direcionado para suas funções e responsabilidades específicas levando

em consideração o treinamento através da lente de conscientização de privacidade.

Segundo CIS (2023) a instituição deve estabelecer e manter um programa de conscientização de segurança para influenciar o comportamento da força de trabalho para ser consciente em segurança e devidamente qualificada para reduzir os riscos de segurança cibernética para a empresa. Para a norma ABNT 27002 (ABNT, 2022b) convém que todos os funcionários da organização e, onde pertinente, fornecedores e terceiros recebam treinamento apropriados em conscientização, e atualizações regulares nas políticas e procedimentos organizacionais, relevantes para as suas funções (ABNT, 2013).

1.14.1. **Procedimentos e ferramentas**

1. Programa de conscientização e treinamento de segurança da informação.

1.14.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotadas para monitoramento e defesa de rede. Dentre elas tem-se as atividades apresentadas na tabela 14.

Tabela 14 - Atividades para conscientização sobre segurança e treinamento de competências

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramenta de Apoio
Estabelecer e manter um programa de conscientização de segurança.	N/A	Proteger	Anualmente	-
Treinar membros da força de trabalho para reconhecer ataques de engenharia social, como *phishing*, pretexto e uso não autorizado.	N/A	Proteger	-	-
Treinar membros da força de trabalho nas melhores práticas de autenticação.	N/A	Proteger	-	-
Treinar a força de trabalho nas melhores práticas de tratamento de dados.	N/A	Proteger	-	-

Treinar membros da força de trabalho sobre as causas da exposição não intencional de dados.	N/A	Proteger	-	-
Treinar membros da força de trabalho no reconhecimento e comunicação de incidentes de Segurança.	N/A	Proteger	-	-
Treinar a força de trabalho sobre como identificar e comunicar se o seus ativos corporativos estão faltando atualizações de segurança.	N/A	Proteger	-	-
Treinar a força de trabalho sobre os perigos de se conectar e transmitir dados corporativos em redes inseguras.	N/A	Proteger	-	-
Conduzir treinamento de competências e conscientização de segurança para funções específicas.	N/A	Proteger	-	-

1.15. Gestão de provedor de serviços

Controle responsável por garantir a proteção das informações, sistemas e processos críticos da organização a partir de um processo para avaliar os provedores de serviços que operem e mantenham estes ativos da organização. Este processo deve avaliar os provedores de serviços que mantêm dados sensíveis, ou são responsáveis por plataformas ou processos de TI críticos de uma empresa, para garantir que esses provedores estejam protegendo essas plataformas e dados de forma adequada (BRASIL, 2023).

1.15.1. **Procedimentos e ferramentas**

1. *Checklists* ISO 27001/Controles CIS;
2. Inventário de provedores de serviços.

1.15.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotadas para gestão de provedor de serviços. Dentre elas tem-se as atividades apresentadas na tabela 15.

Tabela 15 - Atividades para gestão de provedor de serviços

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramenta de Apoio
Estabelecer e manter um inventário de provedores de serviços.	N/A	Identificar	Anualmente	SEI
Estabelecer e manter uma política de gestão de provedores de serviços.	N/A	Identificar	Anualmente	SEI
Classificar provedores de serviços.	N/A	Identificar	Anualmente	SEI
Garantir que os contratos do provedor de serviços incluam requisitos de segurança.	N/A	Proteger	Anualmente	SEI
Avaliar provedores de serviços.	N/A	Identificar	Anualmente	SEI
Monitorar provedores de serviços.	Dados	Detectar	Anualmente	SEI
Descomissionar com segurança os provedores de serviços.	Dados	Proteger	Anualmente	SEI

1.16. Segurança de aplicações

A instituição deve gerenciar o ciclo de vida da segurança de *software* desenvolvido, hospedado ou adquirido internamente para prevenir, detectar e corrigir os pontos fracos de segurança antes que possam afetar a empresa (CIS, 2023).

1.16.1. **Procedimentos e ferramentas**

1. *Checklists* ISO 27001/Controles CIS;
2. Processo de gestão de vulnerabilidades;
3. Processo de software.

1.16.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotadas para segurança de aplicações. Dentre elas tem-se as atividades apresentadas na tabela 16.

Tabela 16 - Atividades para segurança de aplicações

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramenta de Apoio
Estabelecer e manter um processo seguro de desenvolvimento de aplicações.	Aplicações	Proteger	Anualmente	-
Estabelecer e manter um processo para aceitar e endereçar vulnerabilidades de software.	Aplicações	Proteger	Anualmente	-
Executar análise de causa raiz em vulnerabilidades de segurança.	Aplicações	Proteger	-	-
Estabelecer e gerenciar um inventário de componentes de *software* de terceiros.	Aplicações	Proteger	-	-
Usar componentes de software de terceiros atualizados e confiáveis.	Aplicações	Proteger	-	-
Estabelecer e manter um sistema de classificação de gravidade e processo para vulnerabilidades de aplicações.	Aplicações	Identificar	-	-
Usar modelos de configurações de segurança padrão para infraestrutura de aplicações.	Aplicações	Proteger	-	-
Separar sistemas de produção e não	Aplicações	Proteger	-	Ambiente de desenvolvimento de software

produção.				
Treinar desenvolvedores em conceitos de segurança de aplicações e codificação segura.	Aplicações	Proteger	-	-
Aplicar princípios de design seguro em arquiteturas de aplicações.	Aplicações	Proteger	-	-
Aproveitar os módulos ou serviços controlados para componentes de segurança de aplicações.	Aplicações	Proteger	-	-
Implementar verificações de segurança em nível de código.	Aplicações	Proteger	-	-
Realizar teste de invasão de aplicação.	Aplicações	Proteger	-	
Conduzir aplicações de modelagem de ameaças.	Aplicações	Proteger	-	-

1.17. Gestão de respostas a incidentes

A instituição deve estabelecer um programa para desenvolver e manter uma capacidade de resposta a incidentes (por exemplo, políticas, planos, procedimentos, funções definidas, treinamento e comunicações) para preparar, detectar e responder rapidamente a um ataque.

1.17.1. **Procedimentos e ferramentas**

1. Processo de gestão de incidentes de segurança da informação.

1.17.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotadas para gestão de respostas a incidentes. Dentre elas tem-se as atividades apresentadas na tabela 17.

Tabela 17 - Atividades para gestão de respostas a incidentes

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramenta de Apoio
Designar pessoal para gerenciar tratamento de incidentes.	N/A	Responder	Revisar e atualizar anualmente	Processo de gerenciamento de incidentes de segurança da informação
Estabelecer e manter informações de contato para relatar incidentes de segurança.	N/A	Identificar	Revisar e atualizar anualmente	Processo de gerenciamento de incidentes de segurança da informação
Estabelecer e manter um processo corporativo para relatar incidentes.	N/A	Identificar	Revisar e atualizar anualmente	Processo de gerenciamento de incidentes de segurança da informação
Estabelecer e manter um processo de resposta a incidentes.	N/A	Identificar	Revisar e atualizar anualmente	Processo de gerenciamento de incidentes de segurança da informação
Atribuir funções e responsabilidades chave.	N/A	Identificar	Revisar e atualizar anualmente	Processo de gerenciamento de incidentes de segurança da informação
Definir mecanismos de comunicação durante a resposta a incidentes.	N/A	Responder	Revisar e atualizar anualmente	Processo de gerenciamento de incidentes de segurança da informação. Central de Serviços no SUAP.
Conduzir exercícios de resposta a incidentes rotineiros.	N/A	Recuperar	Revisar e atualizar anualmente	-
Conduzir análises pós-incidente.	N/A	Recuperar	Revisar e atualizar anualmente	-
Estabelecer e manter limites de incidentes de segurança.	N/A	Recuperar	Revisar e atualizar anualmente	-

1.18. Testes de invasão

A instituição deve testar a eficácia e a resiliência dos ativos corporativos por meio da identificação e exploração de fraquezas nos controles (pessoas, processos e tecnologia) e da simulação dos objetivos e ações de um atacante.

1.18.1. **Procedimentos e ferramentas**

1. Programa de Teste de Invasão.

1.18.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotadas para testes de invasão. Dentre elas tem-se as atividades apresentadas na tabela 18.

Tabela 18 - Atividades para testes de invasão

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramenta de Apoio
Estabelecer e manter um programa de teste de invasão.	N/A	Identificar	Revisar e atualizar anualmente	-
Realizar testes de invasão externos periódicos.	Rede	Identificar	Revisar e atualizar anualmente	Nmap Wireshark Metasploit
Corrigir as descobertas do teste de invasão.	Rede	Recuperar	Revisar e atualizar anualmente	-
Validar as medidas de segurança.	Rede	Proteger	Revisar e atualizar anualmente	-
Realizar testes de invasão internos periódicos.	N/A	Proteger	Revisar e atualizar anualmente	-

1.19. Política de Segurança da Informação

Segundo a norma ABNT 27002 (ABNT, 2022b) a instituição deve estabelecer uma clara orientação da política de segurança da informação alinhada com os objetivos do negócio e demonstrar apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de sua política de segurança da informação (ABNT, 2022b). O IFTO deve prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentos pertinentes.

1.19.1. **Procedimentos e ferramentas**

1. Política de segurança da informação;

2. Normas complementares sobre segurança da informação;

3. Análise crítica da política de segurança da informação.

1.19.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotadas em relação a política de segurança da informação. Dentre elas tem-se as atividades apresentadas na tabela 19.

Tabela 19 - Atividades relacionadas à política de segurança da informação

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramenta de Apoio
Publicar a política de segurança da informação.	N/A	Identificar	Revisar e atualizar anualmente	Portal Institucional
Análise crítica da política de segurança da informação.	N/A	Identificar	Revisar e atualizar anualmente	SEI

1.20. Organização da segurança da informação

A instituição deve gerenciar a segurança da informação dentro da organização.

1.20.1. **Procedimentos e ferramentas**

1. Definição de atribuições e responsabilidades pela segurança da informação;

2. Coordenação da segurança da informação.

1.20.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotadas em relação a organização da segurança da informação. Dentre elas tem-se as atividades apresentadas na tabela 20.

Tabela 20 - Atividades relacionadas à organização da segurança da informação

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramenta de Apoio
Papéis e responsabilidades pela SI.	N/A	Identificar	Revisar e atualizar anualmente	Política de Segurança da Informação

Comitê de Segurança da Informação.	N/A	Identificar	Revisar e atualizar anualmente	Portaria
Acordos de confidencialidade.	N/A	Identificar	Revisar e atualizar anualmente	SEI
Acordos de nível de serviços.	N/A	Identificar	Revisar e atualizar anualmente	SEI

1.21. Segurança em recursos humanos

Para a norma ABNT 27002 a instituição deve assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis e reduzir o risco de furto ou roubo, fraude ou mau uso de recursos. A instituição deve definir claramente todas as responsabilidades pela segurança da informação (ABNT, 2022b).

1.21.1. **Procedimentos e ferramentas**

1. Atribuir papéis e responsabilidades para a segurança da informação;

2. Matriz RACI.

1.21.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotadas em relação à segurança em recursos humanos. Dentre elas tem-se as atividades apresentadas na tabela 21.

Tabela 21 - Atividades relacionadas à segurança em recursos humanos

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramenta
Estabelecer o Comitê de Segurança da Informação.	N/A	Identificar	Revisar e atualizar anualmente	SEI (Portaria)
Definir papéis e responsabilidades para a privacidade e segurança da informação.	N/A	Identificar	Revisar e atualizar anualmente	SEI (Portaria)

1.22. Segurança física e do ambiente

A instituição deve prevenir o acesso físico não autorizado,

danos e interferências com as instalações e informações da organização. Para a norma ABNT 27002 convém que as instalações de processamento da informação críticas ou sensíveis sejam mantidas em áreas seguras, protegidas por perímetros de segurança definidos, com barreiras de segurança e controles de acesso apropriados. Convém que a proteção oferecida seja compatível com os riscos identificados (ABNT, 2022b).

1.22.1. **Procedimentos e ferramentas**

1. Perímetros de segurança (paredes, portões controlados por cartões, alarmes, fechaduras, portas corta-fogo);

2. Controles apropriados de entrada e saída de visitantes;

3. Proteção contra incêndios, enchentes, terremotos, explosões, perturbações da ordem pública e outras formas de desastres naturais;

4. Proteção de equipamentos contra ameaças físicas e do meio ambiente;

5. Proteção contra intempéries da natureza;

6. Manutenção de equipamentos;

7. Proteção de equipamentos usados fora das dependências do IFTO;

8. Proteção de equipamentos móveis;

9. Reutilização e alienação segura de equipamentos;

10. Autorização prévia para retirada de equipamentos.

1.22.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotadas em relação à segurança física e do ambiente. Dentre elas tem-se as atividades apresentadas na tabela 22.

Tabela 22 - Atividades relacionadas à segurança física e do ambiente

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramenta de Apoio
Definir o perímetro de segurança física.	N/A	Proteger	Revisar e atualizar anualmente	-
Definir controles de entrada física.	N/A	Proteger	Revisar e atualizar anualmente	-
Segurança em escritórios, salas e instalações.	N/A	Proteger	Revisar e atualizar anualmente	-
Proteção contra ameaças externas e do meio ambiente.	N/A	Proteger	Revisar e atualizar anualmente	-
Trabalhando em áreas seguras.	N/A	Proteger	Revisar e atualizar anualmente	-

Acesso do público, áreas de entrega e de carregamento.	N/A	Proteger	Revisar e atualizar anualmente	-

1.23. Segurança de equipamentos

A instituição deve impedir perdas, danos, furto ou roubo, ou comprometimento de ativos e interrupção das atividades da organização.

1.23.1. **Procedimentos e ferramentas**

1. Instalação e proteção do equipamento;
2. Utilidades;
3. Segurança do cabeamento;
4. Manutenção dos equipamentos;
5. Segurança de equipamentos fora das dependências da organização;
6. Reutilização e alienação segura de equipamentos;
7. Remoção de propriedade.

1.23.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotadas em relação à segurança de equipamentos. Dentre elas tem-se as atividades apresentadas na tabela 23.

Tabela 23 - Atividades relacionadas à segurança de equipamentos

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramenta de Apoio
Proteção do local de instalação de equipamentos.	N/A	Proteger	Revisar e atualizar anualmente	-
Estabilização de energia elétrica.	N/A	Proteger	Revisar e atualizar anualmente	-
Proteção do cabeamento estruturado.	N/A	Proteger	Revisar e atualizar anualmente	-
Manutenção corretiva e preventiva de equipamentos.	N/A	Proteger	Revisar e atualizar anualmente	-
Proteção de equipamentos para uso fora das dependências	N/A	Proteger	Revisar e atualizar anualmente	-

da organização.				
Descarte seguro da mídia.	N/A	Proteger	Revisar e atualizar anualmente	-
Norma sobre retirada de equipamento do local de instalação.	N/A	Proteger	Revisar e atualizar anualmente	Norma de uso de recursos computacionais

1.24. Gerenciamento das operações e comunicações

A instituição deve garantir a operação segura e correta dos recursos de processamento da informação. Para a norma ABNT 27002 convém que os procedimentos e responsabilidade pela gestão e operação de todos os recursos de processamento das informações sejam definidos, documentados, mantidos atualizados e disponíveis a todos os usuários que dele necessitem (ABNT, 2022b).

1.24.1. **Procedimentos e ferramentas**

1. Procedimentos e responsabilidades operacionais;
2. Documentação dos procedimentos de operação;
3. Gestão de mudanças;
4. Segregação de funções;
5. Separação dos recursos de desenvolvimento, teste e de produção;
6. Gerenciamento de serviços terceirizados;
7. Entrega de serviços;
8. Monitoramento e análise crítica de serviços terceirizados;
9. Gerenciamento de mudanças para serviços terceirizados;
10. Gestão de capacidade;
11. Aceitação de sistemas.

1.24.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotadas em relação ao gerenciamento das operações e comunicações. Dentre elas tem-se as atividades apresentadas na tabela 24.

Tabela 24 - Atividades relacionadas ao gerenciamento das operações e comunicações

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramenta de Apoio

Documentar, manter atualizados e disponíveis a todos os usuários os procedimentos de operações.	N/A	Identificar	Revisar e atualizar anualmente	Google Drive Portal Institucional
Controlar mudanças nos recursos de processamento da informação e sistemas.	N/A	Proteger	Revisar e atualizar anualmente	-
Segregar as funções para a Segurança da Informação.	N/A	Proteger	Revisar e atualizar anualmente	Programa de privacidade e segurança da informação
Separar recursos de desenvolvimento, teste e produção.	N/A	Proteger	Revisar e atualizar anualmente	Ambiente de homologação de sistemas
Implementar, executar e manter acordos de nível de serviços.	N/A	Proteger	Revisar e atualizar anualmente	Catálogo de Serviços de TI
Monitorar e analisar criticamente os serviços terceirizados.	N/A	Proteger	Revisar e atualizar anualmente	Checklist de execução contratual
Gerenciar mudanças.	N/A	Proteger	Revisar e atualizar anualmente	Processo de gerenciamento de mudanças
Gestão de capacidade.	N/A	Proteger	Revisar e atualizar anualmente	-
Estabelecer critérios de aceitação para novos sistemas, atualizações e novas versões.	N/A	Proteger	Revisar e atualizar anualmente	Processo de Software

1.25. Manuseio de mídias

A instituição deve prevenir contra divulgação não autorizada, modificação, remoção ou destruição aos ativos e interrupções das atividades do negócio.

1.25.1. **Procedimentos e ferramentas**

1. Gerenciamento de mídias removíveis;

2. Descarte seguro de mídias;

3. Tratamento da informação;

4. Segurança da documentação dos sistemas.

1.25.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotadas em relação ao manuseio de mídias. Dentre elas tem-se as atividades apresentadas na tabela 25.

Tabela 25 - Atividades relacionadas ao manuseio de mídias

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramenta de Apoio
Implementar gerenciamento de mídias removíveis.	N/A	Proteger	-	-
Definir procedimento formal para descarte seguro de mídias.	N/A	Proteger	-	SEI
Estabelecer procedimentos para o tratamento e o armazenamento de informações contra a divulgação não autorizada ou uso indevido.	N/A	Proteger	-	-
Proteger documentação de sistemas contra acessos não autorizados.	N/A	Proteger	-	Criptografia

1.26. Troca de informações

A instituição deve manter a segurança na troca de informações e softwares internamente à organização e com quaisquer entidades externas.

1.26.1. **Procedimentos e ferramentas**

1. Políticas e procedimentos para troca de informações;

2. Acordos para a troca de informações;

3. Mídias em trânsito;

4. Mensagens eletrônicas;

5. Sistemas de informações do negócio.

1.26.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotadas em relação à troca de informações. Dentre elas tem-se as atividades apresentadas na tabela 26.

Tabela 26 - Atividades relacionadas à troca de informações

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramenta de Apoio
Estabelecer e formalizar políticas, procedimentos e controles para proteger a troca de informações em todos os tipos de recursos de comunicação.	N/A	Identificar	Revisar e atualizar anualmente	SEI
Estabelecer acordos para a troca de informações e softwares entre a organização e entidades externas.	N/A	Identificar	Revisar e atualizar anualmente	Acordos de Cooperação Técnica
Proteger informações contra acesso não autorizado, uso impróprio ou alteração indevida durante o transporte externos aos limites físicos da organização.	N/A	Identificar	Revisar e atualizar anualmente	*Log* de acessos Criptografia
Desenvolver e implementar políticas e procedimentos para proteger as informações associadas com a interconexão de sistemas de informações do negócio.	N/A	Identificar	Revisar e atualizar anualmente	Controle de acesso

1.27. Controle de acesso à rede

A instituição deve prevenir acesso não autorizado aos serviços de rede.

1.27.1. **Procedimentos e ferramentas**

1. Autorização de uso de serviços de rede;
2. Métodos de autenticação de usuários remotos;
3. Identificação de equipamentos em redes;
4. Proteção de portas de configuração e diagnóstico remotos;
5. Segregação de redes;
6. Controle de conexão de rede;
7. Controle de roteamento de rede.

1.27.2. **Medidas de segurança**

Existem diversas medidas que podem ser adotadas em relação ao controle de acesso à rede. Dentre elas tem-se as atividades apresentadas na tabela 27.

Tabela 27 - Atividades relacionadas ao controle de acesso à rede

Descrição	Tipo de Ativo	Função de Segurança	Periodicidade	Ferramenta de Apoio
Definir política de uso dos serviços de rede.	N/A	Identificar	Revisar e atualizar anualmente	Norma de uso de recursos computacionais
Definir métodos de autenticação para controlar o acesso de usuários remotos.	N/A	Proteger	Revisar e atualizar anualmente	Active Directory
Definir métodos de identificação automática de equipamentos como um meio de autenticar conexões vindas de localizações e equipamentos específicos.	N/A	Identificar	Revisar e atualizar anualmente	Servidor DHCP
Definir métodos para controle de acessos físicos e lógico para diagnosticar e configurar portas.	N/A	Identificar	Revisar e atualizar anualmente	Servidor Firewall
Definir métodos de segregação de redes para grupos de	N/A	Identificar	Revisar e atualizar anualmente	Configuração de VLANs

serviços de informação, usuários e sistemas de informação.				
Definir métodos para controle de conexão de rede de acordo com a política de controle de acesso e os requisitos das aplicações.	N/A	Identificar	Revisar e atualizar anualmente	Servidor Firewall
Implementar controle de roteamento na rede para assegurar que as conexões de computador e fluxos de informação não violem a política de controle de acesso das aplicações do negócio.	N/A	Identificar	Revisar e atualizar anualmente	Servidor Firewall

ANEXO II
PREVISÃO ORÇAMENTÁRIA

Para a execução do plano de privacidade e segurança da informação estima-se previsão orçamentária apresentada na tabela abaixo:

Ação de Segurança	Previsão Orçamentária
Atualização de infraestrutura física de servidores.	R$ 721.933,63
Aquisição de solução de antivírus.	R$ 388.900,00
Aquisição de solução de backup.	R$ 210.000,00
PREVISÃO DE INVESTIMENTO	**R$ 1.320.833,63**

Documento assinado eletronicamente por **Fabiana Ferreira Cardoso**, **Gestora de Segurança da Informação**, em 19/12/2023, às 11:00, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Kleyton Matos Moreira**, **Diretor**, em 22/12/2023, às 14:56, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ifto.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2222423** e o código CRC **221428D5**.

Avenida Joaquim Teotônio Segurado, Quadra 202 Sul, ACSU-SE 20, Conjunto 1, Lote 8 - Plano Diretor Sul — CEP 77020-450 Palmas/TO — (63) 3229-2200
portal.ifto.edu.br — reitoria@ifto.edu.br

Referência: Processo nº 23235.023730/2023-25 SEI nº 2222423