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

PLANO DE CONTINUIDADE DE NEGÓCIOS

EM SEGURANÇA DA INFORMAÇÃO

TECNOLOGIA DA INFORMAÇÃO

HISTÓRICO DE VERSÕES

Data	Versão	Descrição
22/04/2021	1	Elaboração do Plano de Continuidade de Negócios em Segurança da Informação (PCNSI).
19/12/2023	2	Revisão periódica do PCNSI.
26/12/2024	3	Revisão periódica do PCNSI.
08/04/2025	4	Aprovação do PCNSI no CGTI.

1. INTRODUÇÃO

A segurança da informação é um pilar fundamental para o funcionamento eficiente e confiável de qualquer organização, especialmente em instituições de ensino, que lidam com dados sensíveis de estudantes, professores, técnicos administrativos, prestadores de serviços, voluntários e parceiros educacionais. Nesse contexto, o Plano de Continuidade de Negócios em Segurança da Informação (PCNSI) do Instituto Federal de Educação, Ciência e Tecnologia do Tocantins (IFTO) surge como uma ferramenta estratégica para garantir a proteção, a disponibilidade e a integridade das informações, em situações de crise, como desastres naturais, ataques cibernéticos ou falhas operacionais.

O PCNSI é um recurso indispensável para assegurar que o IFTO possa manter suas operações críticas em funcionamento, minimizando impactos negativos em caso de interrupções. Esta ferramenta estratégica que não apenas protege o instituto contra riscos e ameaças cibernéticas, mas também fortalece sua capacidade de manter a excelência acadêmica e operacional, em cenários adversos. O PCNSI é importante em razão:

1. Proteção de dados sensíveis: instituições de ensino armazenam uma vasta quantidade de informações confidenciais, como dados pessoais, registros acadêmicos, pesquisas científicas e informações financeiras. O PCNSI garante que esses dados estejam protegidos contra acessos não autorizados, vazamentos ou perdas, preservando a privacidade e a confiança da comunidade acadêmica.

2. Minimização de riscos e impactos: em um cenário de crise, como um ataque cibernético ou uma falha de infraestrutura, o PCNSI fornece diretrizes claras para a recuperação rápida e eficiente dos sistemas e serviços. Isso reduz o tempo de inatividade, evitando prejuízos financeiros, acadêmicos e reputacionais.

3. Conformidade com legislações e normas: o IFTO está sujeito a regulamentações como a Lei Geral de Proteção de Dados (LGPD) e Instrução Normativa GSI/PR nº 3 de 28 de maio de 2021. O PCNSI auxilia no cumprimento dessas exigências, demonstrando o compromisso da instituição com a segurança da informação e a responsabilidade no tratamento de dados.

Portanto, o PCNSI não apenas protege os dados e sistemas, mas também fortalece a resiliência do IFTO, permitindo que ele cumpra sua missão mesmo diante de adversidades. A adoção desse instrumento estratégico reforça a credibilidade, a transparência e a sustentabilidade e prepara o IFTO para enfrentar os desafios do presente e do futuro, garantindo a continuidade de suas atividades e a proteção de seu patrimônio informacional.

2. OBJETIVOS

O objetivo geral do PCNSI é garantir a continuidade das operações críticas do IFTO, protegendo seus ativos de informação e minimizando os impactos de incidentes que possam comprometer a disponibilidade, integridade e confidencialidade dos dados. O PCNSI visa assegurar que o IFTO esteja preparado para prevenir, responder e recuperar-se de interrupções, mantendo a qualidade dos serviços educacionais e a confiança da comunidade. Para isso foram definidos os seguintes objetivos específicos:

a) identificar e priorizar processos críticos: mapear os processos, sistemas e serviços essenciais para o funcionamento do IFTO, como matrículas, vestibular, registros acadêmicos, sistemas de ensino online e infraestrutura de TIC;

b) proteger ativos de informação: implementar medidas de segurança para garantir a confidencialidade, integridade e disponibilidade dos dados sensíveis, como informações pessoais de estudantes, professores, técnicos administrativos, prestadores de serviços, voluntários e fornecedores;

c) prevenir e mitigar riscos: identificar possíveis ameaças, como ataques cibernéticos, desastres naturais ou falhas operacionais, e estabelecer ações preventivas para reduzir sua probabilidade e impacto;

d) estabelecer procedimentos de resposta a incidentes: definir protocolos claros para proteger, responder e recuperar ativos de informação de forma ágil e eficiente;

e) garantir a recuperação rápida de sistemas e serviços: criar planos de recuperação de desastres para restaurar sistemas críticos e serviços essenciais no menor tempo possível após uma interrupção;

f) promover a conscientização e capacitação: realizar treinamentos e campanhas de conscientização para a comunidade, reforçando boas práticas em segurança da informação e o papel de cada indivíduo na proteção dos dados;

g) assegurar conformidade com legislações e normas: garantir que a instituição esteja em conformidade com leis, instruções normativas, decretos, portarias e normas sobre segurança da informação; e

h) testar e melhorar continuamente o PCNSI: realizar testes e simulações periódicas do PCNSI para identificar pontos de melhoria e garantir sua eficácia em situações reais.

3. **ESCOPO**

3.1 Abrangência Organizacional

O PCNSI abrange incidentes de segurança da informação que possam comprometer a integridade, confidencialidade e disponibilidade das informações do IFTO. Isso inclui as seguintes atividades críticas:

a) administração acadêmica: matrículas, registros de alunos, histórico escolar, calendários acadêmicos;

b) gestão financeira: folha de pagamento, orçamentos, contratos e pagamentos;

c) gestão de infraestrutura tecnológica: servidores, redes, sistemas de informação, aplicações, sistemas de armazenamento, dispositivos de segurança (*firewalls*, antivírus) e serviços em nuvem computacional, plataformas de ensino a distância e bancos de dados;

d) assistência estudantil, ensino, pesquisa, extensão e inovação: dados de processos seletivos, estágios, convênios, projetos de extensão, pesquisas científicas, propriedade intelectual, projetos acadêmicos;

e) comunicação e relacionamento: site institucional e e-mail institucional; e

f) bibliotecas e acervos digitais: bases de dados, publicações digitais e repositórios institucionais.

3.2 Processos e Serviços Críticos

O PCNSI define ações para prevenir, proteger, responder e recuperar processos e serviços institucionais essenciais para o funcionamento do IFTO, como:

a) matrículas e rematrículas: garantir a continuidade dos processos de inscrição e registro de estudantes no sistema acadêmico;

b) aulas e avaliações online: manter a disponibilidade de plataformas de ensino a distância (EAD) e sistemas de avaliação;

c) gestão de dados pessoais: proteger informações de estudantes, professores, técnicos administrativos, prestadores de serviços, voluntários e fornecedores, em conformidade com a LGPD;

d) sistemas de gestão de documentos eletrônicos: proteger documentos institucionais;

e) sistemas de gestão administrativa: proteger dados de projetos de ensino, pesquisa e extensão, dados financeiros, contratos, estágios, convênios, programas assistenciais;

f) comunicação institucional: assegurar a continuidade de portais, e-mails institucionais e sistemas de informação; e

g) Infraestrutura tecnológica: manter a conectividade e o acesso à internet para atividades acadêmicas e administrativas.

3.3 Ativos de Informação

O PCNSI abrange ativos de informação críticos, incluindo:

a) dados sensíveis: informações pessoais, registros acadêmicos, dados financeiros, saúde etc;

b) sistemas e aplicativos: sistemas de gestão acadêmica e administrativa, sistemas de bibliotecas, ferramentas de EAD;

c) infraestrutura física e lógica: servidores, redes, data centers, dispositivos de armazenamento; e

d) documentos eletrônicos: planos de gestão, contratos, convênios, programas assistenciais, projetos, políticas institucionais, portarias, ofícios, relatórios de gestão etc.

3.4 Cenários de Interrupção

Existem diversos cenários de interrupção que podem afetar a disponibilidade, integridade e confidencialidade dos dados e sistemas institucionais. Este PCNSI considera vários cenários que podem impactar a continuidade dos negócios em segurança da informação, como por exemplo:

a) ataque de *ransomware*: sequestro de dados institucionais, incluindo registros acadêmicos, administrativos e financeiros, exigindo resgate para liberação;

b) vazamento de dados sensíveis: exposição de informações de estudantes, professores, técnicos administrativos, prestadores de serviços, voluntários, fornecedores, parceiros educacionais, entre outros devido a falhas de segurança ou ataques *hackers;*

c) *phishing* e engenharia social: roubo de credenciais por meio de e-mails fraudulentos e manipulação de usuários para obtenção de acesso indevido;

d) ataques de negação de serviço distribuído (DDoS): sobrecarga nos servidores, tornando plataformas acadêmicas (EAD, portais internos) inacessíveis;

e) acesso não autorizado a sistemas de informação (intrusão): exploração de vulnerabilidades em sistemas e serviços, podendo comprometer bases de dados e serviços essenciais;

f) falha em equipamentos (servidores, *switches*, roteadores): pane em infraestrutura essencial, impossibilitando acesso a registros acadêmicos e administrativos;

g) erro humano: configurações erradas, alteração/exclusão acidental de dados ou uso indevido de sistemas críticos;

h) problemas de rede e conectividade: interrupção de internet que afeta sistemas de ensino remoto, e-mails institucionais e plataformas acadêmicas;

i) corrupção de dados: arquivos e bancos de dados comprometidos por falhas técnicas, *bugs* de *software* ou processos mal executados;

j) falha em sistemas de autenticação: problemas em sistemas de login que impedem o acesso a sistemas de informação, serviços de TI e plataformas de ensino e gestão;

k) incêndios, enchentes e terremotos: danos físicos ao data center, servidores e infraestrutura de TI;

l) tempestades e raios: falhas elétricas que podem danificar equipamentos críticos;

m) calor excessivo ou falha no resfriamento: superaquecimento de servidores levando à paralisação de sistemas;

n) falha no sistema de contingência de energia elétrica/queda de energia prolongada: falta de eletricidade afetando servidores, roteadores e dispositivos de conectividade;

o) falha de *nobreaks* e geradores: equipamentos de contingência que não funcionam corretamente, agravando o impacto da interrupção;

p) desabastecimento de Internet ou telefonia: falha no fornecimento de serviços essenciais para comunicação e suporte remoto;

q) indisponibilidade de serviços em nuvem (SaaS, IaaS, PaaS): provedores de tecnologia (Google, Huawei, etc.) enfrentam falhas ou ataques;

r) falha em contratos de suporte técnico: dependência de empresas terceirizadas para suporte de TI sem um plano de contingência eficiente;

s) ataques ou problemas em parceiros acadêmicos: instituições conveniadas ou instituições parceiras (RNP) comprometidas podem afetar operações conjuntas;

t) greves e paralisações: impacto nas operações devido a paralisações de servidores da TI ou da administração;

u) falta de treinamento em segurança da informação: usuários vulneráveis a golpes, erros operacionais e práticas inseguras;

v) uso indevido de sistemas institucionais: acesso não autorizado por estudantes, professores, técnicos administrativos, prestadores de serviços, voluntários ou fornecedores devido à falta de controle de acesso adequado;

w) não conformidade com LGPD (Lei Geral de Proteção de Dados): vazamentos ou manuseio inadequado de dados podem gerar multas e processos judiciais;

x) quebra de contratos e parcerias: interrupção de serviços que afetam acordos com outras instituições e órgãos reguladores;

y) descarte incorreto de documentos ou dispositivos eletrônicos;

z) reputação e perda de credibilidade: problemas recorrentes podem afetar a confiança de estudantes, professores, técnicos administrativos, prestadores de serviços, voluntários, fornecedores, sociedade no IFTO;

a1) vírus de computador/*malware*; e

b1) falha em sistemas de informação (*software*).

3.5 Partes Interessadas Envolvidas

As partes interessadas envolvidas que podem ser impactadas pela execução do PCNSI são:

a) comunidade acadêmica: estudantes, professores, técnicos administrativos, prestadores de serviços, voluntários, fornecedores, parceiros educacionais e sociedade;

b) equipe de TI: profissionais responsáveis pela infraestrutura e segurança da informação, desenvolvimento de sistemas, suporte e manutenção de usuários;

c) gestores e administradores: líderes de setores críticos, como administração acadêmica e financeira;

d) parceiros e fornecedores: empresas terceirizadas que fornecem serviços de TI e hospedagem de dados como por exemplo RNP; e

e) órgãos reguladores: entidades governamentais e fiscalizadoras, como o Ministério da Educação (MEC) e a Autoridade Nacional de Proteção de Dados (ANPD).

3.6 Exclusões

Para evitar ambiguidades, **não** está incluído no PCNSI do IFTO:

a) processos ou sistemas que não são críticos para a operação do IFTO;

b) ativos de informação que não possuem impacto significativo em caso de interrupção; e

c) cenários de risco extremamente improváveis ou de baixo impacto.

3.7 Recursos Necessários

A implementação do PCNSI demanda uma combinação equilibrada de recursos humanos, tecnológicos, financeiros e operacionais. Com a alocação adequada desses recursos, o IFTO estará preparado para enfrentar incidentes e interrupções garantindo a continuidade de suas operações, protegendo seus ativos de informação e mantendo a confiança da comunidade.

3.7.1 Recursos Humanos

Para a elaboração, execução e manutenção do PCNSI são necessários os seguintes recursos humanos:

a) alta gestão: representado pelo Comitê de Segurança da Informação. Grupo de pro-reitores, diretores, gerentes e coordenadores responsáveis por setores críticos do IFTO (administração, assistência estudantil, ensino, extensão, pesquisa). Este grupo de pessoas gerenciam os processos considerados críticos para o instituto, tais como: processo seletivo, matrícula, assistência estudantil, pós-graduação, projetos, convênios, estágios, dentre outros;

b) equipe de segurança da Informação: profissionais especializados em infraestrutura de serviços e sistemas de informação. Estas pessoas são responsáveis por identificar riscos, avaliar o impacto da ameaça, implementar controles e medidas de segurança e monitorar as ameaças e vulnerabilidades;

c) equipe de TI: administradores de sistemas, redes e banco de dados e técnicos de tecnologia da informação. Estas pessoas são responsáveis por garantir que a infraestrutura tecnológica esteja segura;

d) equipe jurídica: profissionais especializados na legislação brasileira, responsáveis por garantir a conformidade com as leis, instruções normativas, decretos, portarias e outras regulamentações;

e) equipe de gestão de pessoas: profissionais responsáveis por disponibilizar treinamentos para capacitação de usuários sobre boas práticas em segurança da informação; e

f) equipe de comunicação institucional: profissionais responsáveis por comunicar as ações do PCNSI.

3.7.2 Recursos Tecnológicos

Para que o PCNSI possa alcançar os resultados esperados é necessário ter recursos tecnológicos para suportar os controles e as medidas de segurança da informação. Dentre eles tem-se:

a) ferramentas de segurança: *firewalls*, sistemas de detecção e prevenção de intrusões (IDS/IPS), antivírus, softwares para detecção e resposta a ameaças cibernéticas, soluções de criptografia para proteção de dados sensíveis dentre outros;

b) sistemas de *backup* e recuperação: softwares para gerenciamento de *backup* automatizado e armazenamento seguro de dados, preferencialmente em locais físicos distintos (*on-premises* e na nuvem computacional) e soluções de recuperação de desastres para restaurar sistemas críticos rapidamente;

c) monitoramento e análise: sistemas de monitoramento contínuo de redes e servidores para detectar anomalias e incidentes em tempo real e ferramentas de análise de *logs* e gestão de eventos de segurança (SIEM);

d) infraestrutura de redundância: servidores e dispositivos de rede redundantes para garantir a disponibilidade de sistemas críticos e conexões de internet alternativas para evitar interrupções; e

e) plataformas de comunicação segura: sistemas de e-mail, mensagens e videoconferência com criptografia e autenticação robusta.

3.7.3 Recursos Financeiros

A implementação do PCNSI requer investimentos para aquisição de tecnologias, treinamentos e manutenção de infraestrutura de segurança da informação. Dentre os recursos financeiros necessários incluem:

a) orçamento para aquisição de tecnologias: compra de *softwares* de segurança, licenças e serviços de computação em nuvem;

b) custos com consultoria e treinamento: contratação de especialistas para auxiliar na elaboração e implementação do Plano de Gestão de Segurança da Informação. Cursos e *workshops* para capacitação da equipe e conscientização da comunidade acadêmica e administrativa;

c) investimento em infraestrutura tecnológica: modernização de data centers, redes e sistemas para suportar a implementação dos controles e medidas de segurança e continuidade; e

d) reserva para emergências: definir recursos orçamentários para cobrir despesas imprevistas, como recuperação de desastres ou resposta a incidentes graves.

3.7.4 Recursos Operacionais

Além dos recursos humanos, tecnológicos e financeiros, é necessário estruturar processos, políticas e procedimentos para garantir a operacionalização do PCNSI. Isso inclui:

a) políticas e procedimentos: definir políticas e normas de segurança da informação, planos de resposta a incidentes e procedimentos de recuperação de desastres;

b) plano de comunicação: definir estratégias para comunicação interna e externa durante incidentes, incluindo canais de contato e fluxos de informação;

c) testes e simulações: elaborar planos de testes para execução de exercícios práticos de continuidade, como simulações de ataques cibernéticos ou desastres naturais; e

d) gestão de terceiros: celebrar contratos e acordos com fornecedores de serviços de TI, nuvem computacional e segurança para garantir alinhamento com o PCNSI.

3.7.5 Recursos de Infraestrutura Física

O IFTO deverá considerar a seguinte infraestrutura física para o PCNSI:

a) data center seguro: infraestrutura física (sala de equipamentos) com controle de acesso, sistemas de refrigeração, *nobreaks* e grupo gerador de energia;

b) locais alternativos para operação: espaços físicos (campus) ou virtuais (nuvem computacional) para continuidade das operações em caso de indisponibilidade da sede principal; e

c) proteção contra desastres naturais: medidas como sistemas de combate a incêndios, sistemas de para raios, proteção contra enchentes e estruturas resistentes a desastres.

3.7.6 Recursos de Governança e Gestão

Para garantir a eficácia do PCNSI, é essencial estabelecer uma estrutura de governança, que inclui:

a) Comitê de Segurança da Informação: grupo responsável por supervisionar a implementação, revisão e melhoria contínua das ações previstas nos planos de ação;

b) indicadores de desempenho (KPIs): métricas para avaliar a eficácia do plano, como tempo de recuperação (RTO) e ponto de recuperação (RPO); e

c) auditorias e revisões periódicas: processos para avaliar a conformidade do PCNSI com as melhores práticas e regulamentações nacionais e internacionais.

4. PAPÉIS E RESPONSABILIDADES

O PCNSI do IFTO envolve diversos atores com papéis definidos para garantir a resiliência da infraestrutura de TIC, a proteção de dados administrativos, acadêmicos e a continuidade das operações educacionais. Dentre os atores tem-se:

4.1 Alta Administração

Representada pelo Comitê de Segurança da Informação. Grupo de pessoas responsáveis pelo processo de tomada de decisão em relação ao PCNSI. No contexto deste plano tem as seguintes responsabilidades:

a) aprovar investimentos em segurança da informação e continuidade de negócios; e

b) aprovar os planos de ação para prevenção e detecção de ameaças cibernéticas e recuperação de desastres.

4.2 Equipe de Segurança da Informação

Representada pela Equipe de Tratamento e Resposta a Incidentes Cibernéticos. Grupo de pessoas responsável por coordenar as respostas a incidentes envolvendo segurança da informação, tomar decisões estratégicas e garantir a aplicação do PCNSI. No contexto deste plano tem as seguintes responsabilidades:

a) monitorar e identificar ameaças cibernéticas e falhas de segurança da informação;

b) realizar a análise de impacto no negócio;

c) definir e revisar estratégias de continuidade de negócios em segurança da informação;

d) elaborar e atualizar os planos de ação para a continuidade de negócios em segurança da informação conjuntamente com as coordenações de TI;

e) receber, analisar e responder às notificações e às atividades relacionadas a incidentes de segurança em redes de computadores;

f) desenvolver as atividades de prevenção, tratamento e resposta a incidentes de segurança da informação;

g) realizar treinamentos e conscientização sobre segurança digital; e

h) monitorar ameaças cibernéticas e vulnerabilidades em serviços e sistemas de informação.

4.3 Equipe de TI

Grupo de pessoas responsável por executar os controles e medidas de segurança para mitigar falhas e restaurar a operação dos sistemas e serviços de TIC. No contexto deste plano tem as seguintes responsabilidades:

a) diagnosticar e corrigir falhas de segurança da informação em sistemas críticos;

b) restaurar *backups* e garantir a integridade dos dados após incidentes;

c) aplicar *patches* e atualizações de segurança em servidores e dispositivos;

d) monitorar continuamente a infraestrutura e detectar possíveis ameaças; e

e) prover suporte técnico para estudantes, professores, técnicos administrativos, prestadores de serviços, voluntários e fornecedores durante crises tecnológicas.

4.4 Equipe Jurídica

Grupo de pessoas responsável por assegurar a conformidade do PCNSI com as leis e regulações aplicáveis. No contexto deste plano tem as seguintes responsabilidades:

a) avaliar riscos legais e regulatórios em caso de vazamento de dados ou incidentes de segurança;

b) assegurar que o IFTO cumpra com a legislação sobre acesso à informação, segurança e proteção de dados;

c) gerenciar a comunicação com órgãos reguladores, como a Autoridade Nacional de Proteção de Dados (ANPD); e

d) definir procedimentos legais para mitigar impactos jurídicos e proteger a reputação institucional.

4.5 Equipe de gestão de pessoas

Grupo de pessoas responsável por definir e ofertar cursos de capacitação para usuários sobre segurança digital. No contexto deste plano tem as seguintes responsabilidades:

a) contratar cursos de capacitação em segurança da informação.

4.6 Equipe de Comunicação Institucional

Grupo de pessoas responsável por coordenar a comunicação com estudantes, professores, técnicos administrativos, prestadores de serviços, voluntários, fornecedores, sociedade e a mídia durante incidentes de segurança da informação. No contexto deste plano tem as seguintes responsabilidades:

a) criar e divulgar comunicados internos e externos em caso de crise;

b) garantir que as informações oficiais sejam claras e coerentes;

c) controlar a narrativa para minimizar impactos negativos à reputação do IFTO; e

d) manter contato com a imprensa e gerir crises de imagem.

4.7 Responsável pelo Setor de TI na unidade

Pessoa designada para responder pelas ações executadas pela área de TI na unidade do IFTO em relação ao PCNSI. No contexto deste plano tem as seguintes responsabilidades:

a) planejar a execução dos controles de segurança da informação em sua unidade;

b) garantir a implementação, manutenção e atualização de soluções de segurança da informação;

c) supervisionar e responder à falhas críticas na infraestrutura de TI de sua unidade;

d) coordenar a resposta a ataques cibernéticos e vazamentos de dados em sua unidade; e

e) coordenar auditorias e avaliações de riscos e ameaças relacionadas a sua unidade.

4.8 Administrador de Redes

Pessoa responsável por garantir que a infraestrutura física e lógica da unidade do IFTO seja resiliente e segura. No contexto deste plano tem as seguintes responsabilidades:

a) monitorar ameaças e vulnerabilidade do data centers e redes de comunicação da unidade para evitar interrupções;

b) garantir redundância de serviços e sistemas de informação de sua unidade;

c) supervisionar a prestação de serviços de provedores de serviços terceirizados (nuvem, segurança, conectividade); e

d) gerenciar as estratégias de backup e recuperação de dados dos serviços e sistemas de informação.

4.9 Usuários

Pessoa responsável por colaborar com a detecção de possíveis incidentes de segurança da informação. No contexto deste PCNSI tem as seguintes responsabilidades:

a) utilizar credenciais e acessos a serviços e sistemas de informação institucionais com responsabilidade;

b) relatar tentativas de *phishing*, acessos indevidos ou falhas nos sistemas;

c) seguir boas práticas de segurança digital (uso de senhas fortes, autenticação multifator, etc.);

d) participar de treinamentos e simulações de incidentes; e

e) Obedecer as normas de segurança da informação publicadas pelo IFTO.

5. ANÁLISE DE IMPACTO NO NEGÓCIO

A análise de impacto no negócio visa identificar e avaliar os impactos que incidentes ou falhas de segurança podem ter nas operações e serviços essenciais da organização. No contexto do IFTO envolve entender os efeitos de eventos como vazamentos de dados, ataques cibernéticos, falhas de sistemas ou interrupções na infraestrutura de TI.

Esta atividade envolve avaliar os danos que uma interrupção nos serviços ou a perda de dados pode causar às operações do IFTO. Dentre os diversos impactos identificados tem-se:

a) acadêmico: prejuízo nas aulas, perda de materiais de ensino e pesquisa, interrupção do aprendizado online;

b) financeiro: custos com reparação de danos, perda de reputação que pode levar à diminuição de matrículas ou repasses financeiros pelo governo federal, penalidades por não conformidade com normas de privacidade e proteção de dados;

c) regulatório: multas ou sanções por não conformidade com legislações como a Lei Geral de Proteção de Dados (LGPD) no Brasil;

d) reputacional: perda de confiança entre estudantes, professores, técnicos administrativos, prestadores de serviços, voluntários, fornecedores, parceiros educacionais e sociedade; e

e) operacional: atraso na execução das atividades administrativas e acadêmicas.

5.1 Atividades críticas de negócio

Para que o IFTO possa prestar serviços educacionais, são executados diversos processos organizacionais, os quais envolvem atividades críticas realizadas em sistemas de informação. A Tabela 1 apresenta os processos e ativos de informação classificados como *críticos* para o PCNSI. Essa classificação foi elaborada com base em entrevistas realizadas com *stakeholders*, levando em consideração o impacto potencial e o tempo máximo de inatividade tolerável.

Tabela 1 - Processos e ativos de informação críticos para o IFTO

Processo Crítico	Ativo de Informação	Criticidade	RPO	RTO	Impacto				
					Acadêmico	Financeiro	Regulatório	Reputacional	Operacional
Comunicação Interna e Externa.	E-mail Institucional	alta	8 hs	8 hs	Alto	Médio	Médio	Alto	Alto
Impressão e digitalização de documentos.	Outsourcing de Impressão	alta	8 hs	8 hs	Médio	Baixo	Baixo	Baixo	Alto
Ensino Remoto.	Moodle	alta	8 hs	8 hs	Alto	Indefinido	Alto	Alto	Alto

Comunicação Interna e Externa.	Portal Institucional	alta	8 hs	8 hs	Alto	Indefinido	Indefinido	Alto	Alto
Publicação de artigos científicos.	Sistema de submissão de artigos científicos	alta	8 hs	8 hs	Alto	Indefinido	Indefinido	Alto	Alto
Seleção de Estudantes.	Sistema de Gestão de Processo Seletivo	alta	8 hs	8 hs	Alto	Alto	Alto	Alto	Alto
Gestão acadêmica (matrícula, histórico escolar e diploma) e administrativa (financeiro, contratos, frotas, almoxarifado, compras, licitações).	Sistema Unificado de Administração Pública (SUAP)	alta	8 hs	8 hs	Alto	Alto	Alto	Alto	Alto
Gestão de processos e documentos eletrônicos.	SEI	alta	8 hs	8 hs	Alto	Alto	Alto	Alto	Alto
Gestão de Bibliotecas.	SOPHIA	alta	8 hs	8 hs	Alto	Indefinido	Indefinido	Alto	Alto
Gestão de Redes.	Firewall	alta	8 hs	8 hs	Alto	Alto	Alto	Alto	Alto
Gestão de Projetos de Pesquisas.	Portal Integra	alta	8 hs	8 hs	Alto	Indefinido	Indefinido	Alto	Alto
Gestão de Concursos.	Sistema de Gestão de Concursos	alta	8 hs	8 hs	Alto	Indefinido	Indefinido	Alto	Alto
Gestão de Eleições.	Votações Eletrônicas	alta	8 hs	8 hs	Indefinido	Indefinido	Indefinido	Alto	Alto
Gestão de Usuários de Sistemas.	Sistema de Autenticação de Usuários	alta	8 hs	8 hs	Alto	Alto	Alto	Alto	Alto
Acesso a Banco de Dados.	Banco de Dados Institucional	alta	8 hs	8 hs	Alto	Alto	Alto	Alto	Alto

Fonte: Diretoria de Tecnologia da Informação (IFTO)

Os sistemas de informação, recursos e serviços de TIC que sustentam os processos organizacionais críticos do IFTO, conforme apresentados na tabela 1, poderão ser atualizados ou modificados em função do contexto interno e externo do instituto. A tabela 2 exibe a priorização desses sistemas e serviços de TIC para o restabelecimento das operações normais. Essa hierarquização foi definida com base em critérios de criticidade, dependência e relevância estratégica.

Tabela 2 - Priorização de restabelecimento de sistemas e serviços de TIC

Prioridade	Sistemas/Serviços de TIC	Criticidade	Interdependência
1	Firewall.	Alta	Link de Internet Principal Link de Internet Secundário
2	Sistema de Autenticação de Usuários.	Alta	Firewall
3	SUAP.	Alta	Firewall Sistema de Autenticação de Usuários
4	Sistema Eletrônico de Informações.	Alta	Firewall Sistema de Autenticação de Usuários
5	Moodle.	Alta	Firewall Sistema de Autenticação de Usuários
6	Portal Institucional.	Alta	Firewall Sistema de Autenticação de Usuários

7	Portal Integra.	Alta	Firewall
8	Sophia.	Alta	Firewall
9	Sistemas Internos.	Alta	Internet Sistema de Autenticação de Usuários
10	Sistema de submissão de artigos científicos	Alta	Internet
11	Sistema de Gestão do Processo Seletivo.	Alta	Internet
12	Sistema de Gestão de Concursos.	Alta	Internet
13	Revista Sitio Novo.	Alta	Internet
14	E-mail Institucional.	Alta	Internet Sistema de Autenticação de Usuários
15	Impressão e digitalização de documentos.	Alta	Rede cabeada Rede Wi-Fi Sistema de Autenticação de Usuários
16	Votações Eletrônicas.	Alta	Internet

Fonte: Diretoria de Tecnologia da Informação (IFTO)

A priorização de sistemas e serviços de TIC, apresentada na tabela 2, foi estabelecida com base no cenário vigente durante a elaboração do PCNSI. Todos os sistemas de informação e serviços de TIC listados foram classificados como críticos e receberam prioridade elevada, devido ao seu caráter essencial para a execução dos processos organizacionais nas áreas administrativas e acadêmicas do IFTO. Ressalta-se, contudo, que essa análise poderá ser revisada, caso ocorram mudanças significativas no contexto interno ou externo do instituto ao longo do tempo.

Portanto, a Análise de Impacto no Negócio para o PCNSI configura-se como um processo contínuo e dinâmico, que possibilita ao IFTO identificar riscos e planejar a continuidade de suas operações estratégicas. Essa atividade assegura a proteção dos ativos críticos e a capacidade de recuperação ágil em caso de incidentes de segurança, garantindo a resiliência institucional.

6. AVALIAÇÃO DE RISCOS E AMEAÇAS DE SEGURANÇA DA INFORMAÇÃO

A avaliação de riscos e ameaças à segurança da informação no IFTO é um processo estratégico para identificar, analisar e mensurar riscos que possam comprometer:

a) a integridade, confidencialidade e disponibilidade dos ativos de TI; e

b) os serviços essenciais às operações institucionais.

Como etapa fundamental do PCNSI, esse processo garante que o Instituto esteja preparado para responder eficientemente a incidentes que afetem suas atividades críticas. Os principais riscos e ameaças considerados no plano são:

1. Vazamento de Dados Pessoais

a) Descrição: Exposição não autorizada de dados pessoais de alunos, professores, técnicos administrativos, prestadores de serviços, voluntários, fornecedores e parceiros educacionais (ex: CPF, endereços, históricos acadêmicos);

b) Causas: ataques cibernéticos, falhas de configuração, falhas de sistemas, erros humanos, dispositivos perdidos/roubados e acesso indevido por colaboradores ou terceiros;

c) Probabilidade: alta;

d) Consequências: exposição de dados sensíveis, violação da LGPD;

e) Impactos: perda de confiança dos estudantes, servidores e comunidade, multas por descumprimento da LGPD, danos à reputação da instituição e processos judiciais;

f) Ações preventivas: políticas de clara de segurança da informação e proteção de dados, criptografia de dados, treinamento regular, *firewalls* e sistemas de detecção de intrusão (IDS/IPS), controle rígido de acesso à dados pessoais e monitoramento contínuo de acesso à dados pessoais; e

g) Ações de contingência: notificação imediata, bloqueio de acessos, plano de comunicação de crise e atualização de sistemas.

2. Ataques Cibernéticos

a) Descrição: invasões maliciosas, como *ransomware, phishing, malware* ou DDoS (ataques de negação de serviço);

b) Causas: falhas de segurança, sistema desatualizado, falta de atualizações de software e falta de conscientização dos usuários;

c) Probabilidade: alta;

d) Consequências: interrupção de sistemas, sequestro de dados (ransomware);

e) Impactos: paralisação das operações, perda de dados, perda de confiança dos estudantes, servidores e comunidade e custos de recuperação e danos à imagem da instituição;

f) Ações preventivas: atualizações automáticas, *firewalls* e sistemas de detecção de intrusão (IDS/IPS), autenticação multifator, atualização contínua de vulnerabilidades de sistemas, realização de *pentest*, monitoramento contínuo de *logs* de acesso, treinamento de usuários sobre segurança digital, política de *backup* diário e criptografado, autenticação multifator e monitoramento contínuo de alertas de segurança; e

g) Ações de contingência: isolamento de sistemas, restauração de backups e acionamento de equipe especializada.

3. Acesso Não Autorizado

a) Descrição: uso indevido de sistemas e dados por pessoas não autorizadas, como estudantes, ex-servidores ou *hackers;*

b) Causas: senhas fracas, falta de controle de acesso, credenciais compartilhadas e sistema desatualizado;

c) Probabilidade: alta;

d) Consequências: comprometimento da integridade dos dados acadêmicos (notas, registros), alteração não autorizada em sistemas críticos (matrículas, financeiro), indisponibilidade de serviços devido a ações a ações maliciosas, violação da LGPD, perda de confiança de alunos e pesquisadores, dano à imagem institucional em rankings educacionais, comprometimento de pesquisas científicas, fraudes em processos seletivos e diplomas fraudulentos emitidos;

d) Impactos: roubo de informações, alteração ou exclusão de dados críticos e fraudes;

e) Ações preventivas: *firewalls* e sistemas de detecção de intrusão (IDS/IPS), atualização contínua de vulnerabilidades de sistemas, monitoramento contínuo de logs de acesso, controle de acesso baseada em roles (RBAC), solução de DLP (*Data Loss Prevention*) e monitoramento contínuo de alertas de segurança, treinamento obrigatórios semestrais, programas de conscientização em phishing política de *clean desk,* logs detalhados de todas as transações, revisão trimestral de privilégios (princípio do menor privilégio), dupla aprovação para operação para operações críticas, biometria para acessos restritos, câmeras em salas de servidores, destruição segura de mídias;

g) Ações de contingência: revogação emergencial de credenciais comprometidas, isolamento dos sistemas afetados (quarentena digital), captura forense de logs e evidências digitais, notificação obrigatória à ANPD (caso LGPD), comunicação transparente à comunidade acadêmica e restauração de backups validados, auditoria independente para identificar falhas, revisão de processos e políticas; ações disciplinares conforme regulamento interno e melhorias no sistema baseadas em lições aprendidas.

4. Falhas em Sistemas ou Hardware

a) Descrição: interrupção de serviços devido a falhas em servidores, redes ou dispositivos de armazenamento;

b) Causas: erros de configuração, sobrecarga, falta de manutenção preventiva, desastres naturais (ex.: incêndios, inundações), obsolescência de equipamentos;

c) Probabilidade: alta;

d) Consequências: indisponibilidade de plataformas e corrupção de dados;

e) Impactos: paralisação das atividades acadêmicas e administrativas, atrasos acadêmicos, prejuízos financeiros, perda de informações;

f) Ações preventivas: testes regulares, redundância de sistemas, planos de backup, monitoramento contínuo do desempenho do sistema ou hardware, política de atualização tecnológica, redundância de servidores, manutenção preventiva e *failover; e*

g) Ações de contingência: ativação de sistemas alternativos, priorização de serviços críticos e comunicação transparente.

5. Uso Inadequado de Dispositivos Pessoais

a) Descrição: uso de dispositivos pessoais (ex.: *notebooks, smartphones*) para acessar sistemas institucionais sem segurança adequada;

b) Causas: falta de políticas de BYOD (*Bring Your Own Device*) ou controle sobre dispositivos conectados à rede;

c) Probabilidade: alta;

d) Consequências: vazamento de dados, ataques cibernéticos, perda ou roubo de dispositivos, violação de políticas, comprometimento de redes;

e) Impactos: exposição de dados acadêmicos, financeiros ou pessoais (LGPD), acesso indevido a pesquisas confidenciais, infecção por malware (*ransomware, spyware*), comprometimento de credenciais institucionais (*phishing*), acesso não autorizado a e-mails, sistemas acadêmicos e banco de dados, fraude em matrículas ou emissão de documentos, sanções legais por descumprimento da LGPD, suspensão de acessos ou responsabilização disciplinar, disseminação de vírus na rede institucional e ataques a servidores internos via conexão insegura;

f) Ações preventivas: exigência de senhas fortes e criptografia, instalação obrigatória de antivírus e VPN institucional, autenticação multifator, segmentação de rede (Redes Wi-Fi separadas para dispositivos pessoais e institucionais e firewalls para restringir acessos), treinamento de conscientização (capacitação sobre riscos de Wi-Fi público e phishing e orientações sobre armazenamento seguro de dados), controle de acesso (gerenciamento de dispositivos e revogação remota de acessos em caso de perda/roubo; e

g) Ações de contingência: bloqueio do dispositivo na rede, revogação de credenciais comprometidas, análise forense para identificar vazamentos, notificação aos afetados (se aplicável à LGPD), restauração de backups em caso de perda de dados, atualização de políticas de acesso, auditoria de segurança para identificar falhas, reforço de treinamentos e políticas e implementação de soluções mais robustas (ex.: *Zero Trust*).

6. Engenharia Social e Phishing

a) Descrição: manipulação de servidores, prestadores de serviços e estudantes para obter informações sensíveis ou acesso a sistemas;

b) Causas: falta de treinamento em segurança da informação e despreparo para identificar golpes;

c) Probabilidade: alta;

d) Consequências: vazamento de dados (exposição de dados pessoais (LGPD), registros acadêmicos ou financeiros), acesso não autorizado (invasão a sistemas internos (matrículas, notas, pesquisas), fraudes financeiras (desvio de recursos via falsificação de ordens de pagamento (ex.: cobranças falsas a alunos), comprometimento de sistemas (instalação de malware ou ransomware via anexos infectados), danos reputacionais (perda de credibilidade da instituição perante alunos e parceiros);

e) Impactos: roubo de credenciais, acesso não autorizado a sistemas e vazamento de dados;

f) Ações preventivas: conscientização e treinamento (simulações de phishing, treinamentos obrigatórios (como identificar e-mails suspeitos, nunca compartilhar senhas etc), controles técnicos (filtros anti-*phishing*, autenticação multifator, política de menos privilégio e monitoramento de logs), políticas institucionais; e

g) Ações de contingência: isolar sistemas afetados, revogar acessos temporariamente e redefinir senhas, coletar evidências (logs, e-mail suspeitos) para análise forense, notificar autoridades como ANPD, caso houver vazamento de dados pessoais, comunicar a comunidade, verificar backups para garantir que não houve corrupção de dados, realizar auditorias para identificar falhas no processo, reforçar treinamentos com base nos erros identificados e atualizar políticas.

7. Falta de *Backup* ou *Backup* Inadequado

a) Descrição: perda de dados críticos devido à falta de *backups, backups* mal configurados ou corrupção de cópias de segurança;

b) Causas: falta de políticas de backup, falhas na execução ou teste de *backups;*

c) Probabilidade: alta;

d) Consequências: paralisação de sistemas acadêmicos (matrículas, notas, EAD), interrupção de pesquisas científicas (dados irrecuperáveis), violação da LGPD (multas por perda de dados pessoais), responsabilização civil por danos a alunos ou parceiros, custos elevados para recuperação emergencial de dados, perda de recursos em processos judiciais ou indenizações e desconfiança de alunos e pesquisadores;

e) Impactos: perda permanente de dados e interrupção prolongada das operações e impacto negativo em rankings educacionais;

f) Ações preventivas: realizar *backups* regulares e testar a restauração de dados, simular cenários de desastres e políticas de *backup* diário e criptografado; e

g) Ações de contingência: restaurar a partir da última cópia válida, usar backups off-site se os locais estiverem comprometidos, ajustar frequência de backups e implementar novas tecnologias (backups imutáveis).

8. Vulnerabilidades em Sistemas de Terceiros

a) Descrição: exploração de falhas em sistemas de fornecedores ou parceiros que têm acesso à rede da instituição;

b) Causas: sistema desatualizado, falta de auditoria em contratos e sistemas de terceiros;

c) Probabilidade: alta;

d) Consequências: exposição de dados acadêmicos, financeiros ou de pesquisa via brechas em sistemas terceirizados (ex.: plataformas de EAD, sistemas de pagamento); acesso lateral a sistemas críticos (ex.: invasão via fornecedor de TI com privilégios mal configurados); violação da LGPD (responsabilidade solidária por falhas de terceiros);

e) Impactos: comprometimento da rede institucional, vazamento de dados, ataques à rede interna, interrupção de serviços e danos reputacionais; comprometimento de sistemas dependentes (ex.: interrupção do SUAP devido a falha no provedor de nuvem); perda de confiança de alunos e parceiros devido a incidentes recorrentes;

f) Ações preventivas: exigir certificações (ex.: ISO 27001) e relatórios de auditoria de fornecedores, restringir acessos de terceiros ao estritamente necessário; isolar sistemas acessados por parceiros (ex.: VLAN separada); MFA (Multifator) para todos os acessos externos; monitoramento contínuo sobre alertas para atividades suspeitas de terceiros, revogar credenciais não utilizadas (ex.: após término de contratos); treinamento e conscientização sobre como identificar comportamentos de risco em parceiros (ex.: solicitações incomuns de acesso); capacitação sobre políticas de segurança da instituição; e

g) Ações de contingência: isolar sistemas afetados: bloquear acessos do fornecedor comprometido; coletar evidências: logs de acesso, contratos e comunicações com o parceiro; notificar stakeholders.

9. Uso Indevido de Redes Wi-Fi

a) Descrição: acesso não autorizado à rede Wi-Fi da instituição por pessoas externas;

b) Causas: senhas fracas, falta de criptografia, configurações inadequadas;

c) Probabilidade: alta;

d) Consequências: interceptação de tráfego não criptografado (e-mails, senhas, dados acadêmicos; propagação de malware para dispositivos conectados (ex.: *ransomware*), consumo excessivo de banda (lentidão na rede legítima), criação de redes falsas ("*evil twin*") para phishing de credenciais e responsabilidade por atividades ilegais realizadas via IP da instituição (ex.: *downloads* piratas);

e) Impactos: vazamento de dados, ataques internos, uso indevido de recursos de rede e ataques internos, fraudes e golpes;

f) Ações preventivas: monitorar proativo de redes e sistemas em tempo real; segmentação de redes (apenas para dispositivos institucionais com autenticação forte); redes de visitantes isolada, com limite de banda e acesso restrito, uso de criptografia avançada como por exemplo WPA3-Enterprise (evitar WPA2 ou senhas compartilhadas), uso de VPN para acessar sistemas internos e publicação de norma de uso de recursos computacional, política de controle de acesso e treinamento de usuários; e

g) Ações de contingência: identificar o dispositivo intruso (via logs do roteador/controller Wi-Fi), bloquear MAC address e desconectar o invasor, alterar credenciais (se houve vazamento de senha); verificar se outros dispositivos foram comprometidos, analisar tráfego suspeito (tentativa de acesso a servidores) comunicar à equipe de Ti e gestores.

10. Desastres Naturais ou Acidentes

a) Descrição: danos físicos à infraestrutura de TI devido a incêndios, inundações, quedas de energia ou outros eventos;

b) Causas: falta de planejamento para desastres e infraestrutura inadequada;

c) Probabilidade: alta;

d) Consequências: destruição de servidores, *switches, storages* e equipamentos de rede; indisponibilidade de sistemas críticos (EAD, matrículas, financeiro); danos a discos e *backups* locais não protegidos; custos de reposição de equipamentos e recuperação de dados e atrasos em aulas, pesquisas e processos administrativos;

e) Impactos: perda de hardware, interrupção de serviços, corrupção de dados, prejuízos financeiros e acadêmico;

f) Ações preventivas: configuração de ambiente computacional redundante em nuvem computacional ou em área elevada para evitar inundações, construir paredes resistentes a incêndios e portas blindadas, implantar sistemas de refrigeração e umidade controlada, implantar sensores de temperatura e água (alerta em caso de vazamento), implantar *nobreaks* e geradores de energia para manter sistemas ativos, instalar para-raios e aterramento elétrico adequado; e

g) Ações de contingência: isolar a área afetada (desligar equipamentos, se seguro), acionar brigadistas ou bombeiros (em caso de incêndio); avaliar danos (verificar se há equipamentos recuperáveis e identificar sistemas críticos offline); acionar plano de continuidade (migrar serviços para infraestrutura secundária (nuvem ou site remoto); recuperação de dados (restaurar backups mais recentes, validar integridade dos dados); comunicação (informar à comunidade acadêmica sobre prazos de retorno e notificar autoridades se necessário); reposição de equipamentos (priorizar servidores e *switches* essenciais e negociar prazos curtos com fornecedores); documentar causas e melhorias necessárias e atualizar políticas.

11. Falta de Conscientização e Treinamento

a) Descrição: comportamentos de risco por parte de técnicos administrativos, professores e estudantes, como clicar em links maliciosos ou compartilhar senhas;

b) Causas: falta de treinamentos regulares em segurança da informação;

c) Probabilidade: alta;

d) Consequências: exposição de informações acadêmicas, financeiras ou pessoais (violação da LGPD), acesso não autorizado a notas, matrículas ou pesquisas científicas, *ransomware* criptografando dados institucionais, falsificação de documentos ou solicitações financeiras (ex.: bolsas falsas), perda de credibilidade da instituição perante alunos e parceiros;

e) Impactos: vazamento de dados, invasão de sistemas, infecção por malware, fraudes e danos à reputação;

f) Ações preventivas: programas de educação continuada (simulações de phishing mensais para identificar vulnerabilidades), treinamentos obrigatórios (identificar e-mails falsos; nunca compartilhar senhas, mesmo como colegas ou superiores; uso de autenticação multifator; configuração de filtros anti-*phishing*; monitoramento de alertas para logins suspeitos e auditoria de compartilhamento de credenciais; e

g) Ações de contingência: isolar contas comprometidas, bloquear links ou anexos maliciosos identificados; rastrear origem do incidente, coletar evidências para ações disciplinares.

12. Não Conformidade com a LGPD

a) Descrição: descumprimento das obrigações legais da Lei Geral de Proteção de Dados (LGPD);

b) Causas: não mapeamento de fluxo de dados, armazenamento excessivo de dados, sistemas sem criptografia, acessos privilegiados não controlados, estudantes e servidores não treinados;

c) Probabilidade: alta;

d) Consequências: sanções administrativas, judiciais, operacionais e reputacionais;

e) Impactos: sanções administrativas, indenizações por danos morais, suspensão de sistemas, interrupção de matrículas e avaliações e perda de credibilidade em rankings educacionais;

f) Ações preventivas: definir prazos de retenção para cada categoria, implementar ferramentas de consentimento para captação legal de dados, criptografar dados sensíveis, adotar pseudonimização em pesquisas acadêmicas, implantar sistemas de gestão de acessos com logs auditáveis, alinhar práticas à LGPD e notificar incidentes à ANPD, quando necessário e treinamento de servidores e estudantes sobre segurança digital; e

g) Ações de contingência: acionar plano de resposta a incidentes, comunicar a ANPD, revogar acessos comprometidos, restaurar dados de backups válidos e oferecer suporte jurídico aos afetados.

13. Exposição de Dados em Plataformas de Ensino

a) Descrição: vulnerabilidades em plataformas de ensino a distância (EAD) ou sistemas de gestão acadêmica;

b) Causas: falhas de desenvolvimento (SQL *injection* em formulários de login, *Cross-Site Scripting* (XSS) em fóruns); configurações inseguras (senhas padrão não alteradas, APIs expostas sem autenticação); dependências desatualizadas (plugins de terceiros com vulnerabilidades conhecidas e versões antigas da plataforma de ensino a distância); falta de criptografia (dados trafegando em HTTP, armazenamento de senhas em texto claro); acessos privilegiados (contas de administrador compartilhadas, ex-funcionários com credenciais ativas);

c) Probabilidade: alta;

d) Consequências: exposição de históricos escolares e documentos pessoais, alteração fraudulenta de resultados acadêmicos, ataques DDoS durante períodos de matrícula, roubo de propriedade intelectual acadêmica;

e) Impactos: vazamento de dados acadêmicos, manipulação de notas, interrupção do sistema de informação e pesquisas comprometidas;

f) Ações preventivas: implementar OWASP Top 10 para proteção contra vulnerabilidades web; configurar WAF (*Web Application Firewall*) específico para EAD; desativar serviços e portas não essenciais; adotar MFA (Autenticação Multifator) para todos os usuários; implementar princípio do menor privilégio para contas administrativas; Gerenciar ciclo de vida de credenciais (exclusão imediata ao desligamento); implementar SIEM com regras específicas para tentativas de acesso incomuns, padrões de download massivo de dados; configurar alertas para alterações em notas/históricos; e

g) Ações de contingência: isolar sistemas comprometidos da rede, revogar credenciais potencialmente vazadas, preservar logs para análise forense, notificar autoridades, comunicar-se com usuários afetados, restaurar sistemas a partir de backups validados, realizar *pentest* completo antes do retorno à operação, atualizar políticas com lições aprendidas, oferecer monitoramento de crédito para afetados (em casos de vazamento de dados pessoais).

14. Fraudes e Manipulação de Dados

a) Descrição: alteração fraudulenta de dados acadêmicos (ex: notas, diários, frequências, boletins, histórico escolar e diploma);

b) Causas: controles de acesso fracos em plataformas acadêmicas, APIs desprotegidas permitindo alterações em massa, senhas de professores/funcionários vazadas, uso de credenciais compartilhadas, servidores mal-intencionados com privilégios excessivos,

estudantes com acesso indevido (ex.: irmão gêmeo), ausência de auditoria em alterações, validação manual ineficiente de documentos;

c) Probabilidade: alta;

d) Consequências: processos por falsificação documental, ações civis por danos morais, desvalorização de diplomas legítimos, prejuízos a processos seletivos (vestibulares e concursos), perda de credibilidade do IFTO, custos com investigações forenses;

e) Impactos: jurídico, acadêmico, reputacional e financeiro;

f) Ações preventivas: implementar MFA (Dupla Autenticação) para todos os acessos administrativos, registrar logs imutáveis de todas as alterações (*Blockchain* para diplomas), criar sistemas de aprovação em dupla etapa para mudanças críticas, adotar RBAC (Controle de Acesso Baseado em Função), auditoria trimestral de privilégios, implementar diplomas digitais com QR Code verificável, exigir assinatura digital para históricos escolares, criar portal de verificação pública de autenticidade, monitoramento proativo de alterações em lotes de notas, acessos em horários incomuns, IPS estrangeiros acessando sistemas acadêmicos; e

g) Ações de contingência: congelar todos os acessos administrativos, isolar sistemas afetados para preservação de evidências, notificar reitoria e departamento jurídico, análise forense dos logs de acesso, identificação dos dados alterados e períodos comprometidos, comunicação transparente aos afetados, restauração de dados válidos a partir de backups criptografados, revalidação manual de documentos críticos e processo disciplinar contra envolvidos.

15. Riscos em Dispositivos Móveis

a) Descrição: perda ou roubo de dispositivos móveis (ex: *tablets, notebooks*) com acesso a dados institucionais;

b) Causas: dispositivos sem criptografia ou senha forte; ausência de controle de inventário; transporte inadequado (ex.: deixar *notebook* em carro visível); uso em locais públicos sem supervisão; ausência de rastreamento (GPS) ou *remote wipe*; backup não automatizado;

c) Probabilidade: alta;

d) Consequências: exposição de informações acadêmicas, financeiras ou pessoais (LGPD); login em e-mails e plataformas institucionais salvas; uso de identidade institucional para golpes (ex.: *phishing*); penalidades da ANPD por violação da LGPD e perda de confiança de alunos e parceiros;

e) Impactos: vazamento de dados, acesso não autorizado a sistemas, fraudes, sanções e danos reputacionais;

f) Ações preventivas: cadastro de todos os dispositivos móveis com dados institucionais; identificação do responsável por cada equipamento; *BitLocker* (Windows) ou *FileVault* (Mac) ativados; armazenamento em nuvem com criptografia (ex.: Google Drive); senhas complexas e autenticação multifator (MFA) para acessos; *Remote Wipe* (apagar dados remotamente via Microsoft Intune, Jamf, etc.); treinamentos regulares co,o transportar dispositivos com segurança, nunca salvar senhas em navegadores ou arquivos locais; política de uso aceitável; bloqueio remoto em caso de perda, dados críticos sincronizados em nuvem institucional, nenhum arquivo sensível deve ser armazenado apenas localmente; e

g) Ações de contingência: usar MDM ou ferramentas como microsoft Intune para apagar dados, resetar credenciais de e-mail, sistemas acadêmicos e VPN, registrar boletim de ocorrência em caso de roubo, comunicar a ANPD se houver vazamento de dados pessoais, verificar se houve login suspeito nos sistemas, informar afetados, recuperar arquivos via backup em nuvem, reforçar treinamentos, implementar novas tecnologias.

16. Falha Humana

a) Descrição: exclusão acidental de arquivos ou pastas;

b) Causas: imperícia, formatação incorreta de sistemas, uso inadequado de ferramentas de TI, desconhecimento de procedimentos de *backup*, ausência de confirmação antes de exclusões críticas, permissões excessivas para usuários comuns, *bugs* em interfaces que facilitam exclusões acidentais;

c) Probabilidade: alta;

d) Consequências: históricos escolares, notas e registros de matrícula apagados, paralisação de sistemas críticos (ex.: plataforma EAD), tempo e custo para recuperação manual de dados, descumprimento da LGPD se dados pessoais forem perdidos, estudantes e professores perdem credibilidade na instituição;

e) Impactos: perda de dados acadêmicos, interrupção operacional, retrabalho, riscos legais e danos à confiança;

f) Ações preventivas: disponibilização de mensagens de aviso para confirmação de exclusão, exigir senha administrativa para operações críticas, backup automatizado com várias versões dos arquivos e pastas, aplicar o princípio do menor privilégio para permissão de usuários, realizar a gestão de logs de acesso, realizar treinamento e conscientização sobre como usar lixeiras seguras e simulações; e

g) Ações de contingência: congelar o sistema para evitar sobrescrita, verificar logs para entender o escopo da exclusão; usar a cópia mais recente não corrompida; comunicar estudantes e professores impactados.

17. Falha de Energia

a) Descrição: Interrupção no fornecimento de energia elétrica;

b) Causas: falhas na rede pública (apagões regionais e sobrecarga na rede elétrica), problemas internos (curto-circuito nas instalações e falta de manutenção preventiva), fenômenos naturais (tempestades com raios e enchentes que afetam subestações) e falhas em equipamentos (*nobreaks*/grupos geradores com defeito e fiação elétrica obsoleta);

c) Probabilidade: alta;

d) Consequências: paralisação de atividades presenciais e EAD, corrupção de arquivos não salvos, danos a equipamentos por desligamento abrupto, danos a equipamentos sensíveis, custo com horas extras para recuperação, falha em sistemas de vigilância, problemas em laboratórios com equipamentos sensíveis, atraso em prazos de entrega e comprometimento de pesquisas em andamento;

e) Impactos: perda de dados, interrupção de aulas, prejuízos financeiros, riscos à segurança e impacto acadêmico;

f) Ações preventivas: implementação de infraestrutura elétrica resiliente (*nobreaks* para equipamentos críticos (grupo geradores, servidores, *switches* de rede e sistemas de segurança)); sistemas de alimentação ininterrupta para laboratórios de informática e sala de servidores; verificação trimestral de geradores e *nobreaks*; testes mensal de sistemas de backup; circuitos elétricos segregados para cargas críticas; proteção contra surtos, procedimentos claros para salvar dados e desligar equipamentos; treinamento periódico para equipe técnica; rotas de evacuação com iluminação autônoma, sistema de comunicação alternativo; e

g) Ações de contingência: priorizar alimentação para servidores e infraestrutura de rede e iluminação de emergência, executar procedimentos desligamento seguro, comunicar à comunicação acadêmica sobre a interrupção e previsão de normalização; verificar se há danos aos equipamentos; disponibilizar materiais *offline*; verificar integridade de sistemas antes de religar; priorizar religamento de (infraestrutura de TI, laboratórios críticos e sistemas administrativos); identificar pontos fracos no plano atual e documentar lições aprendidas.

18. Falha de Conectividade

a) Descrição: Interrupção no fornecimento de redes;

b) Causas: falhas na infraestrutura (rompimento de cabos de fibra óptica, danos em equipamentos de rede (*switches*, roteadores)); problemas no provedor (falhas no *backbone* do ISP, interrupção programada sem aviso prévio); ataques cibernéticos (DDoS contra servidores institucionais; comprometimento de dispositivos de rede); falhas humanas (configurações incorretas em equipamentos, desligamento acidental de servidores); eventos climáticos (tempestades que danificam infraestrutura externa e inundações em datacenters);

c) Probabilidade: alta;

d) Consequências: paralisação de atividades remotas e acesso a plataformas de ensino, impossibilidade de acessar sistemas acadêmicos, bibliotecas virtuais, atrasos em processos

administrativos e pesquisas, risco de corrupção em transações interrompidas e descontentamento de alunos e professores;

e) Impactos: interrupção de aula EAD, inacessibilidade de sistemas, perda de produtividade, comprometimento de dados e danos reputacionais;

f) Ações preventivas: redundância de conexão de Link de Internet diferentes (ex.: fibra + rádio), configuração de rede interna resiliente (topologia em anel ou malha para switches e roteadores; equipamentos críticos com fontes redundantes), monitoramento contínuo através de sistemas de detecção de falhas (PRTG, Zabbix ou Nagios para alertas em tempo real e monitoramento de SLA com provedores), realização de testes regulares (simulações semestrais de falhas na rede e verificação de rotas alternativas); implementação de segurança e proteção (firewalls e sistemas anti-DDoS e segmentação de redes para conter falhas); estabelecimento de plano de continuidade (roteadores 4G/5G como backup e servidores críticos com acesso via VPN alternativa); e

g) Ações de contingência: verificar status com o provedor; analisar logs de rede, mudar para o link secundário (backup), priorizar tráfego essencial (EAD, sistemas acadêmicos), informar sobre a falha e estimativa de reparo, implementar soluções temporárias (Hotspot 5G para atividades críticas e redirecionar serviços para nuvem), avaliar impactos (verificar se houve perda de dados e documentar tempo de inatividade), ao restabelecer conexão principal, testar estabilidade antes de retomar operações normais e atualizar equipamentos se necessário, ajustar plano de contingência com lições aprendidas e treinar equipe em novos procedimentos.

19. Violação de Privacidade

a) Descrição: Divulgação de dados pessoais sensíveis;

b) Causas: falhas processuais (compartilhamento indevido em planilhas não criptografadas e envio acidental para destinatários errados), falhas técnicas (configurações incorretas de permissão em sistemas e vulnerabilidades em softwares de gestão acadêmica), ações maliciosas (acesso não autorizado por funcionários ou hackers e venda ilegal de bancos de dados), falta de treinamento (equipe desconhece protocolos de proteção de dados e uso inadequado de ferramentas de comunicação);

c) Probabilidade: média;

d) Consequências: ações judiciais individuais e coletivas, perda de credibilidade da instituição, danos à imagem perante alunos e comunidade, suspensão de sistemas para investigação, custo com auditorias e correções e danos morais a titulares dos dados (estudantes, professores);

e) Impactos: jurídico/regulatório, reputacional, operacional e psicológico;

f) Ações preventivas: uso de criptografia de dados para armazenamento e transmissão com padrões AES-256 ou superior, uso de VPN para acesso remoto; realização de gestão de acessos (controle baseado em função RBAC), logs detalhados de consultas e modificações; uso de ferramentas especializadas (DLP: *data loss prevention* e mascaramento de dados sensíveis em ambientes de teste); definição de fluxos para tratamento de dados sensíveis e mapeamento de bases legais (LGPD Art. 7º); inserção de cláusulas contratuais rígidas sobre proteção de dados e auditorias periódicas em fornecedores; realização de capacitações semestrais sobre LGPD e simulações de vazamentos para testar respostas; e

g) Ações de contingência: investigação imediata, revogação de acessos e ajuste de processos e reparação aos afetados.

A efetiva implementação do PCNSI no IFTO está intrinsecamente vinculada à realização de análises contínuas e minuciosas dos riscos e ameaças potenciais. Essa abordagem proativa não apenas consolida a segurança da informação, como também resguarda os ativos institucionais e preserva a integridade da missão educacional frente a possíveis incidentes tecnológicos ou ameaças cibernéticas.

7. ESTRATÉGIAS DE CONTINGÊNCIA, CONTINUIDADE E RECUPERAÇÃO

O Plano de Continuidade de Negócios em Segurança da Informação do IFTO deve incorporar estratégias abrangentes de contingência, continuidade operacional e recuperação de sistemas, assegurando a manutenção dos serviços educacionais e administrativos mesmo em cenários adversos, como falhas críticas, incidentes cibernéticos

ou situações de desastre. As diretrizes apresentadas nas seções subsequentes foram elaboradas com fundamento nos resultados obtidos por meio da Análise de Impacto ao Negócio, garantindo alinhamento estratégico com as necessidades institucionais.

7.1 Estratégias de Prevenção/Contingência

As estratégias de prevenção e contingência compreendem um conjunto de medidas proativas e reativas, destinadas tanto à redução da probabilidade de ocorrência de incidentes quanto à mitigação de seus possíveis impactos. Para assegurar a continuidade dos negócios do IFTO, foram estabelecidas as diretrizes apresentadas na tabela 3, as quais contemplam:

Tabela 3 - Estratégias de prevenção/contingência

Estratégia	Medida de segurança	Responsável pela Execução
Preparação.	-Instalar de equipamentos de segurança, como extintores, alarmes e saídas de emergência. -Garantir que as instalações físicas, como data centers e áreas com equipamentos de TI, estejam protegidas contra desastres naturais, incêndios e intrusões. -Garantir que servidores estejam em locais protegidos com acesso restrito. -Elaborar planos de evacuação claros e conhecidos por todos os envolvidos, caso a infraestrutura física da instituição seja comprometida.	Alta Administração
Identificação de processos críticos e ativos de informação essenciais para o IFTO.	-Identificar quais são os processos acadêmicos e administrativos essenciais para o funcionamento da instituição e como garantir sua continuidade em caso de incidentes. -Mapear os ativos de informação do IFTO.	Equipe de TI
Analise de ameaças e vulnerabilidades.	-Identificar e avaliar os riscos, ameaças e vulnerabilidades à segurança da informação e definir ações de mitigação.	Equipe de TI
Política de Segurança da Informação.	-Estabelecer regras para o uso seguro dos ativos de informação do IFTO.	Gestor de Segurança da Informação
Política de Controle de Acesso.	-Estabelecer regras para acesso aos recursos computacionais do IFTO. -Estabelecer controles de acesso para sistemas, aplicativos e serviços de TIC. -Implementar MFA para sistemas críticos (como os de gestão acadêmica e administrativa) para aumentar a segurança no acesso aos dados. -Controlar e monitorar o acesso a sistemas e informações sensíveis com base no princípio do menor privilégio, garantindo que apenas usuários autorizados tenham acesso a dados confidenciais. -Restringir acessos a informações sensíveis apenas a usuários autorizados.	Equipe de TI
Política de Proteção de Dados.	-Estabelecer regras para a proteção de dados.	Equipe de TI
Política de *Backup* de dados.	-Estabelecer política de *backup* de dados. -Definir estratégias de *backups* frequentes para garantir a integridade dos dados e evitar perda de informações críticas. -Realizar *backups* automáticos diários em locais seguros localmente e em nuvem e testar a restauração regularmente.	Equipe de TI

Programa de Treinamento e Conscientização em Segurança da Informação.	-Estabelecer um plano de ação para oferta de cursos de capacitação em Segurança da Informação. -Oferecer treinamentos contínuos para professores, estudantes e técnicos administrativos sobre boas práticas seguras de uso de e-mails, navegação na internet e identificação de *links* ou anexos maliciosos.	Departamento de Recursos Humanos e Gestor de Segurança da Informação
Proteção perimetral de redes.	-Configurar *firewalls* robustos e sistemas de prevenção e detecção de de intrusão (IDS/IPS). -Implementar segmentação da rede para isolar sistemas críticos e minimizar o impacto de eventuais falhas ou ataques cibernéticos. -Implementar soluções de segurança em tempo real para proteção contra vírus e outras ameaças de *malware*, com atualizações automáticas. -Implementar filtros de e-mail e campanhas de conscientização contra *phishing.* -Realizar monitoramento contínuo de rede para detectar atividades suspeitas. -Utilizar SIEM (*Security Information and Event Management*) para monitoramento em tempo real. -Monitoramento 24/7 de *logs* e eventos de segurança.	Equipe de TI
Plano de Resposta a Incidentes.	-Definir procedimentos de resposta a incidentes assegurando que a equipe de TI saiba como agir em caso de ataques cibernéticos, falhas técnicas ou desastres naturais. -Redundância de servidores em nuvem e *on-premises*. -Realizar simulações de incidentes de segurança para preparar os envolvidos e testar a eficácia do plano de resposta e recuperação.	Responsável pela setor de TI da unidade do IFTO
Plano de Continuidade Operacional.	-Implementar estratégias de redundâncias em link de internet, servidores, banco de dados, serviços e redes para evitar indisponibilidades. -Utilizar geradores e UPS para manter operações durante quedas de energia.	Responsável pela setor de TI da unidade do IFTO
Plano de Recuperação de Desastres (PRD).	-Desenvolver e documentar um PRD abrangente. -Realizar testes periódicos do plano. -Atualizar o plano conforme necessário. -Aplicar atualizações de *patches* de segurança periodicamente em todos os sistemas operacionais, aplicativos e dispositivos. -Verificar regularmente a eficácia dos processos de recuperação de dados para garantir que, em caso de falha, os sistemas possam ser restaurados com sucesso.	Responsável pela setor de TI da unidade do IFTO
Plano de Auditoria Contínua.	-Implementar sistemas de monitoramento de *logs* para detectar atividades anormais e garantir que todas as ações em sistemas críticos sejam auditáveis. -Realizar auditorias periódicas de segurança e revisar as políticas e controles estabelecidos no plano de continuidade.	Equipe de TI
Plano de Comunicação.	-Estabelecer canais e processos claros para comunicar incidentes de segurança a partes interessadas, como	Alta Administração

	alunos, pais, funcionários e órgãos reguladores.	

7.2 Estratégias de Detecção

As estratégias de detecção apresentadas na tabela 4 compreendem mecanismos de monitoramento contínuo, projetados para identificar de forma ágil potenciais ameaças antes de sua materialização, tais como sistemas de detecção de intrusão (IDS) e soluções correlatas. A detecção tempestiva de riscos e ameaças à segurança da informação, incluindo violações de dados, incidentes cibernéticos e falhas sistêmicas, constitui um elemento fundamental para assegurar a resiliência operacional e a proteção dos ativos institucionais.

Tabela 4 - Estratégias de detecção

Estratégia	Medida de segurança	Responsável pela Execução
Monitoramento contínuo de sistemas e serviços de TIC.	-Implementar ferramentas de monitoramento em tempo real. -Configurar alertas para atividades suspeitas. -Analisar logs de eventos regularmente.	Equipe de TI
Análise de Tráfego de Rede.	-Utilizar sistemas de detecção de intrusão (IDS). -Monitorar padrões de tráfego anômalos. -Realizar varreduras periódicas na rede.	Equipe de TI
Auditorias de Segurança Regulares.	-Conduzir auditorias internas e externas. -Avaliar conformidade com políticas de segurança. -Identificar vulnerabilidades e pontos fracos.	Equipe de TI
Análise de *logs.*	-Monitorar *logs* de sistemas e redes para identificar anomalias.	Equipe de TI
Gestão de Vulnerabilidades.	-Executar avaliações de vulnerabilidades regularmente. -Aplicar *patches* e atualizações de segurança. -Manter um inventário atualizado de ativos.	Equipe de TI

7.3 Estratégias de Recuperação

As estratégias de recuperação constituem um conjunto de medidas técnicas e organizacionais essenciais para a rápida restauração de serviços críticos e a mitigação eficaz de impactos operacionais. Essas ações abrangem desde a implementação de backups sistemáticos até a elaboração detalhada de Plano de Recuperação de Desastre e Plano de Resposta a Incidentes, garantindo ao IFTO capacidade de resiliência institucional diante de diversos cenários adversos. Tais estratégias possibilitam:

a) a restauração ágil das operações essenciais;

b) a redução significativa do tempo de inatividade; e

c) a proteção contínua dos ativos institucionais.

Conforme demonstrado na tabela 5, o IFTO adota um conjunto robusto de medidas de recuperação, especificamente desenvolvidas para enfrentar desde intercorrências cotidianas até eventos críticos como:

a) desastres naturais;

b) Falhas de infraestrutura tecnológica; e

c) incidentes cibernéticos de maior complexidade.

Tabela 5 - Estratégias de Recuperação

Estratégia	Medida de segurança	Responsável pela Execução
Backup Regular de Dados.	-Realizar *backups* periódicos dos dados críticos. -Armazenar *backups* em locais seguros e distintos.	Administrador de Redes.

	-Verificar regularmente a integridade dos *backups.*	
Infraestrutura Redundante.	-Implementar sistemas redundantes para componentes críticos. -Configurar balanceamento de carga. -Monitorar o desempenho dos sistemas redundantes.	Administrador de Redes.
Recuperação em Nuvem.	-Configurar *backups* automáticos para a nuvem. -Estabelecer procedimentos para recuperação a partir da nuvem. -Garantir a segurança dos dados armazenados na nuvem.	Administrador de Redes.
Treinamento e Simulações de Recuperação.	-Conduzir treinamentos regulares para a equipe sobre procedimentos de recuperação. -Realizar simulações de desastres para testar a eficácia dos planos. -Avaliar e melhorar continuamente os processos de recuperação.	Setor de Gestão de Pessoas. Gestor de Segurança da Informação.

8. **PLANOS DE CONTINUIDADE**

O Plano de Continuidade de Negócios em Segurança da Informação do IFTO estrutura-se em três componentes estratégicos integrados, concebidos para garantir a plena resiliência operacional da instituição. Esses planos proporcionam um *framework* abrangente que assegura:

a) capacidade de resposta eficaz a incidentes de qualquer natureza;

b) manutenção ininterrupta das operações essenciais;

c) recuperação integral dos ativos informacionais; e

d) preservação da excelência acadêmica e da confiança institucional.

Essa arquitetura estratégica visa proteger os interesses de toda a comunidade acadêmica, incluindo:

a) corpo discente e docente;

b) técnicos administrativos;

c) parceiros e fornecedores; e

d) prestadores de serviços e voluntários.

Os três pilares que constituem o PCNSI são:

a) Plano de Administração de Crises (PAC): define as funções e responsabilidades das equipes antes, durante e após a ocorrência de uma crise. No IFTO, esse plano implica o estabelecimento de protocolos claros para lidar com situações adversas, como ataques cibernéticos, falhas sistêmicas ou desastres naturais que possam comprometer a infraestrutura de TI. Uma gestão de crises eficiente assegura uma resposta coordenada, mitiga impactos negativos e facilita a comunicação entre todas as partes envolvidas;

b) Plano de Continuidade Operacional (PCO): tem como objetivo restabelecer as operações críticas do IFTO no menor tempo possível, minimizando os efeitos de incidentes. No contexto do instituto, esse plano visa garantir o funcionamento ininterrupto de sistemas essenciais, tais como plataformas de ensino a distância, registros acadêmicos e canais de comunicação interna. A rápida recuperação desses serviços é primordial para assegurar a continuidade das atividades educacionais e administrativas; e

c) Plano de Recuperação de Desastres (PRD): tem por finalidade restaurar integralmente os sistemas e dados após um evento crítico. Sua implementação abrange a recuperação de servidores, bancos de dados e demais componentes vitais da infraestrutura de TI do IFTO. No âmbito educacional, onde a perda de informações acadêmicas ou administrativas pode acarretar consequências severas, um PRD robusto garante o retorno seguro às operações cotidianas, preservando a integridade, a confidencialidade e a disponibilidade dos dados institucionais.

8.1 PLANO DE ADMINISTRAÇÃO DE CRISE

8.1.1 Apresentação

O Plano de Administração de Crise (PAC) tem como objetivo assegurar que o IFTO esteja preparado para responder a crises de segurança da informação de maneira eficaz, protegendo seus ativos digitais e preservando a confiança institucional. O documento estabelece protocolos de ação para diversos cenários de crise, definindo processos para gerenciar, mitigar ou eliminar impactos, considerando todos os agentes envolvidos. A implementação ocorre por meio de ações coordenadas e comunicação estratégica até a completa resolução da situação.

8.1.2 Escopo

O Plano de Administração de Crise abrange a gestão de incidentes de segurança da informação no IFTO, incluindo, mas não se limitando a:

a) vazamentos de dados;

b) ataques cibernéticos;

c) violações de privacidade;

d) perda de informações; e

e) Demais ameaças à integridade, confidencialidade e disponibilidade dos sistemas institucionais.

O Plano de Administração de Crise aplica-se a:

a) todos os setores administrativos e acadêmicos;

b) servidores docentes e técnico-administrativos;

c) prestadores de serviços;

d) estudantes;

e) empresas terceirizadas; e

f) toda a infraestrutura de TI da instituição.

8.1.3 Objetivo

O Plano de Administração de Crise tem como finalidade principal:

a) estabelecer diretrizes claras e protocolos padronizados para:

- identificação oportuna de incidentes;

- contenção imediata de ameaças;

- resposta eficaz às ocorrências; e

- recuperação completa dos sistemas.

b) minimizar impactos adversos em três dimensões críticas:

- financeiros: redução de perdas materiais;

- reputacionais: preservação da imagem institucional; e

- operacionais: manutenção da capacidade funcional.

c) assegurar a continuidade ininterrupta de:

- atividades acadêmicas essenciais; e

- processos administrativos estratégicos.

8.1.4 Plano de Administração de Crise

O PAC será ativado quando um incidente de segurança da informação for detectado ou quando houver suspeita de uma violação de privacidade. A tabela 6 apresenta os procedimentos, ações e responsáveis pela execução do PAC.

Tabela 6 - Plano de Administração de Crise

Fase	Procedimento	Ações	Responsável
Antes da Crise	Planejamento de ações.	Definir a Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR).	Comitê de Segurança da Informação
		Definir papéis e responsabilidades da ETIR.	Comitê de Segurança da Informação
		Elaborar os procedimentos para a Administração de Crise.	Comitê de Segurança da Informação
Durante a Crise	Identificação do incidente.	-Acompanhar o registro de incidentes através dos canais de comunicação da área de TI. -Monitorar continuamente sistemas e redes. -Registrar relatos de servidores, estudantes ou sistemas de detecção automática. -Análise inicial para confirmar a ocorrência do incidente.	Equipe de TI
	Classificação do incidente.	-Avaliação da gravidade (baixa, média, alta, crítica). -Determinação do tipo de incidente (vazamento de dados, *ransomware*, *phishing*, etc).	Equipe de TI
	Comunicação.	Notificar as partes interessadas (direção, funcionários, alunos, autoridades) de forma clara e transparente.	Equipe de TI
	Contenção.	-Isolamento de sistemas afetados. -Bloqueio de acessos não autorizados. -Bloqueio de acessos não autorizados. -Suspensão temporária de serviços, se necessário.	Equipe de TI
	Análise e Investigação.	-Coleta de evidências. -Identificação da causa raiz. -Avaliação do impacto.	Equipe de TI
	Mitigação.	-Implementar medidas para reduzir o impacto imediato.	Equipe de TI
	Resposta.	-Eliminação da ameaça. -Recuperação de sistemas e dados. -Comunicação interna e externa.	Equipe de TI
	Recuperação.	-Restauração de operações normais de sistemas e dados afetados. -Verificação da integridade dos sistemas. -Implementação de medidas preventivas.	Equipe de TI
Pós-Crise	Prevenção.	-Reforçar controles de segurança para evitar recorrências.	Equipe de TI
	Documentação.	-Registrar o processo de resolução do incidente de segurança da informação (atividades, ações e procedimentos executados).	Equipe de TI
		-Elaborar relatório de incidentes com registro de ações tomadas e lições aprendidas.	Equipe de TI
	Melhoria Contínua.	-Revisar e aprimorar o plano para fortalecer a resiliência contra futuras ameaças.	Equipe de TI
	Encerramento da Crise.	-Comunicar as áreas de negócios afetadas. Se envolver todos os usuários divulgar amplamente o incidente de segurança ocorrido e as medidas adotadas para a solução.	Responsável pelo Setor de TI

Fonte: Diretoria de Tecnologia da Informação

O PAC deve ser revisado periodicamente e testado por meio de simulações para garantir sua eficácia em situações reais. Todo o aprendizado referente a crise enfrentada deve ser registrado para agilizar a resposta a novas crises.

8.1.5 Papéis e Responsabilidades

Para que o PAC seja executado de forma eficiente foram definidos os seguintes papéis e responsabilidades:

a) Alta Administração: alocação de recursos humanos, financeiros e tecnológicos;

b) Comitê de Segurança da Informação: decisões estratégicas sobre segurança da informação;

c) Equipe de TI: contenção técnica, recuperação de sistemas e dados críticos e investigação forense, se necessário;

d) Responsável pelo Setor de TI: administração do PAC da sua unidade;

e) Usuários: seguir protocolos de segurança e reportar incidentes de forma imediata;

f) Equipe jurídica: conformidade com leis de proteção de dados e regulamentações;

g) Equipe de comunicação: gestão de comunicação interna e externa; e

h) Equipe de gestão de pessoas: realização de treinamentos para servidores.

8.1.6 Ativação do PAC

O PAC será ativado quando:

a) um incidente de segurança for confirmado;

b) houver suspeita de uma violação significativa; e

c) o impacto potencial for classificado como médio, alto ou crítico.

8.1.7 Encerramento do PAC

O PAC será encerrado quando:

a) a ameaça for completamente eliminada;

b) os sistemas e dados forem recuperados;

c) as operações normais forem restauradas; e

d) as lições aprendidas forem documentadas e incorporadas ao PAC.

Os passos para o encerramento do PAC são:

1. Confirmação da resolução do incidente.
2. Reunião final com a Equipe de Tratamento e Resposta a Incidentes Cibernéticos.
3. Comunicação do encerramento às partes interessadas.
4. Revisão e atualização do plano.

8.1.8 Treinamentos e simulações

O IFTO deverá realizar os seguintes tipos de treinamentos e simulações para o PAC:

a) realização de treinamentos regulares para servidores e estudantes sobre boas práticas de segurança da informação e proteção de dados; e

b) simulações de crises para testar a eficácia do plano e identificar áreas de melhoria.

8.1.9 Revisão e atualização

O PAC será revisado anualmente ou após cada incidente significativo para garantir sua eficácia e conformidade com as melhores práticas e regulamentações vigentes.

8.1.10 Conclusão

A elaboração e execução de PAC no IFTO traz uma série de benefícios estratégicos, operacionais e reputacionais. Esses ganhos são essenciais para garantir a resiliência do instituto diante de incidentes de segurança da informação ou outras crises. Dentre os benefícios podem ser observados:

a) proteção da integridade e continuidade das operações (minimização de interrupções e recuperação rápida);

b) proteção de dados sensíveis (prevenção de vazamentos, conformidade legal);

c) preservação da reputação institucional (confiança da comunidade, transparência);

d) redução de impactos financeiros (minimização de perdas e economia de recursos);

e) melhoria da cultura de segurança (conscientização, prevenção de futuros incidentes);

f) preparação para cenários de crise (resposta estruturada, redução de estresse);

g) conformidade com normas e boas práticas (alinhamento a padrões internacionais e auditorias e certificações);

h) proteção da comunidade acadêmica (segurança de servidores e estudantes); e

i) resiliência institucional (capacidade de adaptação e fortalecimento da governança).

O PAC proporciona ao IFTO uma estrutura robusta para lidar com incidentes de segurança da informação e outras crises. Os benefícios incluem a proteção de dados, a preservação da reputação, a redução de custos e a garantia da continuidade das operações. Além disso, o PAC fortalece a confiança da comunidade acadêmica e posiciona o instituto como uma organização preparada e resiliente, pronta para enfrentar desafios em um mundo cada vez mais digital e complexo.

8.2 PLANO DE CONTINUIDADE OPERACIONAL

8.2.1 Apresentação

O Plano de Continuidade Operacional (PCO) visa garantir que o IFTO esteja preparado para manter suas operações críticas em funcionamento, mesmo diante de incidentes de segurança da informação, assegurando a continuidade dos serviços administrativos, acadêmicos e a proteção de dados da comunidade. O PCO descreve os cenários de inoperância e suas respectivas medidas alternativas planejadas, definindo as ações prioritárias para garantir a continuidade dos serviços essenciais.

8.2.2 Escopo

O PCO abrange a garantia da continuidade das operações críticas do IFTO em cenários de interrupção causados por incidentes de segurança da informação, como ataques cibernéticos, vazamento de dados, falhas de sistemas, desastres naturais ou outros eventos que comprometam a disponibilidade, integridade ou confidencialidade dos sistemas e dados. Aplica-se a todos os setores, sistemas de TI, servidores, estudantes e terceirizados.

8.2.3 Objetivo

O objetivo do PCO é assegurar a recuperação rápida e eficiente das operações críticas do IFTO após um incidente de segurança da informação, minimizando impactos acadêmicos, financeiros e reputacionais, e garantindo a continuidade dos serviços essenciais

e preservando a funcionalidade de plataformas de ensino, registros acadêmicos e comunicações internas, mesmo em cenários adversos.

8.2.4 Plano de Continuidade Operacional

O PCO será ativado após a ocorrência de um incidente de segurança da informação. A tabela 7 apresenta os procedimentos, ações e responsáveis pela execução do Plano de Continuidade Operacional.

Tabela 7 - Plano de Continuidade Operacional

Fase	Procedimento	Ações	Responsável
Análise de Impacto nos Negócios (BIA).	Identificação de operações críticas.	-Mapeamento dos processos e sistemas essenciais (ex.: matrículas, notas, aulas online, comunicação interna). -Avaliar os processos de TI para identificar quais são críticos para as operações da instituição e determinar os impactos potenciais de interrupções nesses processos. -Classificar cada processo de acordo com sua criticidade. -Estabelecer o Tempo Objetivo de Recuperação (RTO) para cada processo. -Definir prioridades para recuperação.	Equipe de TI
Gestão de Riscos e Ameaças.	Avaliação de riscos e ameaças.	-Identificar riscos e ameaças potenciais que podem afetar a continuidade dos serviços de TI e implementar medidas para mitigar esses riscos e ameaças. -Realizar uma análise de riscos para identificar vulnerabilidades. -Análise de impacto de cada cenário de interrupção.	Equipe de TI
Plano de resposta	Ativação de procedimentos de Contingência.	-Criar um plano de resposta detalhado que descreva as ações a serem tomadas para manter ou restaurar as operações de TI durante e após uma interrupção. -Definir procedimentos de resposta a incidentes (contingência). -Estabelecer planos de comunicação durante crises. -Designar responsabilidades específicas para a equipe de TI durante incidentes. -Redirecionamento de operações para sistemas alternativos (uso de backups, migração para infraestrutura em nuvem).	Responsável pelo setor de TI da unidade
Comunicação	Notificação.	-Notificação transparente à comunidade acadêmica (alunos, professores, funcionários) e partes interessadas. -Divulgação de informações claras sobre o status das operações e prazos de recuperação.	Equipe de Comunicação
Resposta	Resposta rápida.	-Isolamento de sistemas afetados para evitar propagação de ameaças. -Ativação de planos de contingência e equipes de resposta. -Implementação de medidas temporárias para manter as operações críticas.	Equipe de TI
Recuperação de Sistemas e Dados	Restauração de operações de TI.	-Restauração de sistemas e dados afetados a partir de *backups* seguros e atualizados.	Administrador de Redes

		-Verificar integridade e segurança dos sistemas e dados recuperados.	
Normalidade	Retorno à normalidade.	-Transição gradual para operações padrão. -Monitoramento contínuo para garantir estabilidade dos sistemas.	Administrador de Redes
Prevenção	Redundância de Infraestrutura.	-Implementar sistemas redundantes para eliminar pontos únicos de falha e garantir a disponibilidade contínua dos serviços de TI. -Utilizar servidores e equipamentos de rede redundantes. -Estabelecer conexões de internet redundantes com diferentes provedores. -Implementar fontes de energia ininterrupta (UPS) e geradores de backup. -Implementar controles de segurança para mitigar riscos identificados. -Estabelecer políticas de segurança da informação.	Administrador de Redes
	Segurança da Informação.	Implementação de controles de segurança (ex.: *backups* regulares, redundância de sistemas, *firewalls*).	Administrador de Redes
	Testes e Exercícios Regulares.	-Realizar testes periódicos do PCO para identificar falhas e áreas de melhoria, garantindo que a equipe esteja preparada para responder a incidentes reais. -Conduzir simulações de desastres e exercícios de mesa. -Avaliar o desempenho da equipe durante os testes e fornecer feedback. -Atualizar o PCO com base nos resultados dos testes.	Administrador de Redes
	Treinamento.	-Capacitação de servidores, estudantes, prestadores de serviços para situações de crise. -Realização de simulados para testar a eficácia do PCO.	Equipe de Gestão de Pessoas

Fonte: Diretoria de Tecnologia da Informação

Implementar esses procedimentos e ações ajudará o IFTO a manter a resiliência de seus serviços de TI, minimizando interrupções e garantindo a continuidade das operações essenciais.

8.2.5 Papéis e Responsabilidades

Os papéis e responsabilidades deste plano são:

a) Alta Administração: alocação de recursos humanos, financeiros e tecnológicos;

b) Comitê de Segurança da Informação: decisões estratégicas sobre segurança da informação;

c) Equipe de TI: contenção técnica, execução de backups, recuperação de sistemas e dados críticos e investigação forense, se necessário;

d) Responsável pelo Setor de TI: administração do PCO;

e) Equipe jurídica: conformidade com leis de proteção de dados e regulamentações;

f) Equipe de comunicação: gestão de comunicação interna e externa; e

g) Equipe de gestão de pessoas: realização de treinamentos para servidores.

8.2.6 Ativação do PCO

O PCO será ativado quando:

a) um incidente de segurança comprometer a disponibilidade de sistemas críticos;

b) houver interrupção prolongada das operações acadêmicas ou administrativas; e

c) o impacto for classificado como médio, alto ou crítico.

Os passos para o ativação do PCO são:

1. Detecção da interrupção ou incidente.
2. Notificação imediata ao Comitê de Segurança da Informação.
3. Avaliação do impacto e decisão de ativar o PCO.
4. Mobilização das equipes e ativação dos procedimentos de contingência.

8.2.7 Encerramento do PCO

O PCO será encerrado quando:

a) as operações críticas forem restauradas;

b) a estabilidade dos sistemas for confirmada; e

c) o impacto do incidente for completamente mitigado.

Os passos para encerramento do PCO são:

1. Confirmação da recuperação total das operações.
2. Reunião final da ETIR.
3. Comunicação do encerramento às partes interessadas.
4. Documentação do incidente e lições aprendidas.

8.2.8 Treinamentos e simulações

a) realização de treinamentos regulares para funcionários e alunos sobre procedimentos de continuidade; e

b) simulações de cenários de interrupção para testar a eficácia do PCO.

8.2.9 Revisão e atualização

O PCO será revisado anualmente ou após cada incidente significativo para garantir sua eficácia e conformidade com as melhores práticas e regulamentações vigentes, como a Lei Geral de Proteção de Dados (LGPD) e normas ISO/IEC 27001.

8.2.10 Conclusão

Ao seguir este PCO, o IFTO assegura a continuidade dos serviços administrativos, acadêmicos, a proteção dos dados da comunidade e a minimização de impactos financeiros e reputacionais. A execução do PCO no IFTO traz benefícios estratégicos, operacionais e reputacionais que são essenciais para garantir a resiliência e a sustentabilidade da instituição.

O PCO é especialmente relevante em cenários de interrupções causadas por incidentes de segurança da informação, desastres naturais, falhas de sistemas ou outras crises. Abaixo estão os principais ganhos que o instituto obtém com a implementação do PCO:

a) garantia da continuidade das operações críticas (minimização de interrupções e recuperação rápida);

b) proteção de dados e informações sensíveis (prevenção de perda de dados, conformidade com leis de proteção de dados); e

c) preservação da reputação institucional.

8.3 PLANO DE RECUPERAÇÃO DE DESASTRES

8.3.1 Apresentação

O Plano de Recuperação de Desastres (PRD) descreve os cenários de inoperância e seus respectivos procedimentos planejados, definindo as atividades prioritárias para restabelecer o nível de operação dos serviços no ambiente afetado dentro de um prazo tolerável.

8.3.2 Escopo

O PRD abrange a recuperação de sistemas, dados e operações críticas do IFTO após um desastre relacionado à segurança da informação, como ataques cibernéticos (ex.: ransomware, DDoS), vazamentos de dados, falhas de hardware, desastres naturais ou outros eventos que comprometam a disponibilidade, integridade ou confidencialidade dos sistemas e informações. Aplica-se a todos os setores, sistemas de TI, servidores, estudantes e terceirizados.

8.3.3 Objetivo

O objetivo do PRD é estabelecer as diretrizes e procedimentos necessários para garantir a continuidade dos processos críticos da organização em caso de desastres, minimizando os impactos sobre as operações e assegurando a retomada das atividades no menor tempo possível.

8.3.4 Plano de Recuperação de Desastres

A tabela 8 apresenta os procedimentos, as atividades e os responsáveis pela execução do Plano de Recuperação de desastres.

Tabela 8 - Plano de Recuperação de desastres

Fase	Procedimento	Ações	Responsável
Prevenção	Avaliação de riscos.	-Identificar e avaliar potenciais riscos de segurança da informação.	Equipe de TI
	Implementação de controles de segurança da informação.	-Implementação de políticas de segurança e proteção de dados.	Equipe de TI
	Realização de Treinamento.	-Realizar treinamento e conscientização dos servidores, estudantes, prestadores de serviços, voluntários.	Equipe de TI
	Realização de testes de segurança e simulações.	-Realizar periodicamente testes de invasão, simulações de ataques internos e externos.	Equipe de TI
Preparação	Definição de Equipe de resposta a incidentes de segurança.	-Criar de equipe de resposta a incidentes de segurança da informação.	Alta Administração
	Definição de data center alternativo.	-Definir locais alternativos para continuidade operacional.	Alta Administração
	Configuração de infraestrutura redundante.	-Implementar estratégias automatizadas de backups regulares de dados críticos. - Implementar infraestrutura redundante de sistemas em nuvem computacional. -Implementar rotinas automatizadas para atualizações de *softwares* e sistemas	Alta Administração

	Comunicação.	-Elaborar planos de comunicação interna e externa.	Equipe de Comunicação
Identificação do desastre	Detecção do incidente por meio de monitoramento contínuo, relatos de funcionários ou sistemas de alerta.	-Monitorar continuamente o funcionamento de ativos de informação.	Equipe de TI
	Identificação de ativos danificados.	-Identificar e listar todos os ativos danificados da ocorrência do desastre.	Equipe de TI
	Identificação de acessos interrompidos.	-Identificar as interrupções de conexões e acessos gerados após o desastre, informando se a abrangência está na rede local, rede WAN ou com o provedor de serviços.	Equipe de TI
	Lista de serviços descontinuados.	-Mapear quais serviços foram descontinuados contendo as informações de perda de ativo e de conexão, abrangendo todos os componentes necessários à plena operação da aplicação como servidores, máquinas virtuais, banco de dados, *firewall, storage, routers e switches*, bem como respectivas configurações de proxy, dns, rotas, vlans etc.	Equipe de TI
	Classificação do desastre.	-Classificação do desastre com base na gravidade (baixa, média, alta, crítica) e no tipo (ataque cibernético, falha de hardware, desastre natural).	Equipe de TI
Ativação do PRD	Notificação.	-Informar o Comitê de Segurança da Informação. -Informar a ETIR.	Equipe de TI
	Reunião.	-Avaliação do impacto e decisão de ativar o PRD.	Equipe de TI
	Elaborar o cronograma de recuperação.	-Elaborar um cronograma de recuperação das aplicações levando em consideração: a priorização dos serviços essenciais, ou determinação de nível institucional, o RTO definido para cada serviço essencial e a força de trabalho disponível.	Responsável pelo Setor de TI da unidade
Resposta	Contenção.	-Isolar os sistemas afetados.	Equipe de TI
	Comunicação.	-Comunicar às partes interessadas.	Equipe de TI
Recuperação de Sistemas de Dados	Avaliação.	-Avaliar os danos causados.	Equipe de TI
	Substituição de ativos e equipamentos.	-Em caso de perda de ativos, deverá ser imediatamente informado ao Responsável pelo Setor de TI na unidade a necessidade de aquisição de ativos perdidos que não puderem ser recuperados. -A equipe irá mensurar quanto tempo a aquisição irá impactar o RTO de cada serviço comunicando ao Responsável pelo Setor de	Equipe de TI

		TI da unidade se há alguma solução alternativa a ser tomada enquanto é realizada a aquisição. Então, a equipe de TI deve verificar quais ativos foram danificados estão cobertos por garantia e se poderá ser acionada neste caso através dos fornecedores. -As informações pertinentes à alteração do tempo de recuperação dos serviços serão passadas às equipes do PCO e PAC.	
	Reconfiguração de ativos e equipamento.	-Deverá verificar se as configurações dos ativos reparados ou substituídos estão em funcionamento pleno. Caso não estejam, prover cronograma estimado para configurar estes ativos.	Equipe de TI
	Restauração de *backups*.	-Restauração de sistemas a partir de backups seguros e atualizados.	Equipe de TI
	Verificação de integridade.	-Verificação da integridade e segurança dos dados e sistemas recuperados.	Equipe de TI
Aperfeiçoamento contínuo	Avaliação	-Avaliar medidas de segurança para evitar reincidência.	Equipe de TI
	Teste de ambiente.	-Garantir os mesmos níveis de capacidade e disponibilidade dos serviços essenciais antes do desastre.	Equipe de TI
	Transição.	-Realizar a transição gradual para operações padrão.	Equipe de TI
	Validação.	-Monitoramento contínuo para garantir a estabilidade dos sistemas. -Realizar testes automatizados de monitoramento dos serviços. -Validar as configurações e funcionalidades dos sistemas.	Equipe de TI
	Implementação de melhorias.	-Implementar melhorias para evitar recorrências. -Atualizar políticas de segurança e controles preventivos.	Equipe de TI
	Treinamento.	-Realizar treinamento da equipe com base nas lições aprendidas.	Responsável pelo Setor de TI
Encerramento do PRD	Documentação das lições aprendidas.	-Documentar o incidente e análise das causas. -Identificar as falhas e melhorias no plano de recuperação. -	Equipe de TI

Fonte: Diretoria de Tecnologia da Informação

Implementar esses procedimentos e ações ajudará o IFTO a prevenir e responder desastres relacionados à segurança da informação, minimizando interrupções e garantindo a continuidade das operações essenciais.

8.2.5 Papéis e Responsabilidades

Os papéis e responsabilidades para este plano são:

a) Alta Administração: alocação de recursos humanos, financeiros e tecnológicos;

b) Comitê de Segurança da Informação: decisões estratégicas sobre segurança da informação;

c) Equipe de TI: contenção técnica, execução de backups, recuperação de sistemas e dados críticos e investigação forense, se necessário;

d) Responsável pelo Setor de TI: administração do PRD;

e) Equipe jurídica: conformidade com leis de proteção de dados e regulamentações;

f) Equipe de comunicação: divulgação adequada das informações aos stakeholders; e

g) Equipe de gestão de pessoas: realização de treinamentos para servidores.

8.3.5 Encerramento do PRD

Ao término do procedimento de recuperação, as informações serão consolidadas em parecer específico informando o restabelecimento de cada serviço, equipamentos adquiridos, procedimentos de recuperação realizados e fornecedores acionados.

Este plano de recuperação de desastres garante que o IFTO esteja preparado para enfrentar situações críticas, minimizando impactos e mantendo a confiança de seus stakeholders. Esses planos devem ser ajustados de acordo com as necessidades específicas do IFTO, considerando seu porte, a complexidade de seus sistemas de TI e o nível de exposição a riscos. Além disso, é fundamental que o PCNSI seja revisado regularmente e testado para garantir que a instituição esteja preparada para reagir a qualquer evento que possa comprometer a continuidade de suas operações.

9. TESTES E SIMULAÇÕES

Os testes e simulações são essenciais para validar a eficácia do PCNSI. Ao realizar exercícios práticos e avaliar os resultados, o IFTO garante estar preparado para enfrentar interrupções e proteger seus ativos de informação, mantendo a confiança da comunidade e cumprindo sua missão educacional.

Conforme recomenda a Instrução Normativa PR/GSI nº 3, de 28 de maio de 2021, o PCNSI deverá ser testado e revisado regularmente, com intuito de que seus resultados sejam documentados e possam garantir a sua efetividade em caso de necessidade de ativação. O Responsável pelo Setor de TI das unidades do IFTO deverá coordenar a realização de testes de segurança semestralmente ou com a insurgência de novos fatores de risco, mudança na análise de impacto, ou com a inclusão de um novo serviço no PCNSI para garantir que os procedimentos previstos neste plano são viáveis e eficazes.

9.1 Tipos de Testes e Simulações

a) **Testes de Recuperação de Desastres (*Disaster Recovery Tests*)**

Objetivo: verificar a capacidade de restaurar sistemas críticos e dados após uma interrupção.

Exemplos de Cenários:

-Restauração de servidores após uma falha de hardware.

-Recuperação de dados a partir de backups após um ataque de *ransomware*.

-Reativação de sistemas de ensino online após uma queda de energia.

b) **Simulações de Incidentes de Segurança**

Objetivo: avaliar a resposta da equipe a incidentes de segurança, como ataques cibernéticos ou vazamentos de dados.

Exemplos de Cenários:

-Simulação de um ataque de *phishing* que compromete credenciais de acesso.

-Detecção e contenção de um malware em sistemas críticos.

-Resposta a um vazamento de dados pessoais de alunos ou colaboradores.

c) **Testes de Continuidade de Processos Críticos**

Objetivo: garantir que os processos essenciais da instituição possam ser mantidos ou retomados rapidamente.

Exemplos de Cenários:

-Continuidade das matrículas e registros acadêmicos em caso de falha no sistema principal.

-Manutenção das aulas online durante uma interrupção prolongada da infraestrutura de TI.

d) **Simulações de Desastres Naturais ou Emergências Físicas**

Objetivo: preparar a instituição para responder a eventos como incêndios, enchentes ou tempestades.

Exemplos de Cenários:

-Evacuação segura de instalações e proteção de equipamentos críticos.

-Migração de operações para um local alternativo em caso de indisponibilidade da sede principal.

e) **Testes de Comunicação e Coordenação**

Objetivo: avaliar a eficácia dos planos de comunicação interna e externa durante uma crise.

Exemplos de Cenários:

-Notificação de alunos, professores e colaboradores sobre uma interrupção prolongada.

-Coordenação entre equipes de TI, gestores e fornecedores durante um incidente.

9.2 Exemplos Práticos de Testes aplicados ao PCNSI

a) **Simulação de Ataque de *Ransomware***

Cenário: um ataque de *ransomware* criptografa os dados dos servidores acadêmicos.

Ações Testadas:

-Detecção e isolamento do ataque.

-Restauração dos dados a partir de *backups*.

-Comunicação com a comunidade acadêmica sobre a interrupção.

b) **Teste de Recuperação de Sistemas de Ensino Online**

Cenário: a plataforma de ensino online fica indisponível devido a uma falha no servidor.

Ações Testadas:

-Ativação de servidores redundantes.

-Migração temporária para uma plataforma alternativa.

-Comunicação com professores e estudantes sobre a mudança.

c) **Simulação de Incêndio no Data Center**

Cenário: um incêndio danifica parte da infraestrutura de TI do IFTO.

Ações Testadas:

-Evacuação segura do local.

-Ativação de um data center alternativo.

-Recuperação de sistemas críticos a partir de *backups* remotos.

9.3 Periodicidade e frequência de execução de testes e simulações

Os testes e simulações deverão ser executados minimamente:

a) testes periódicos de recuperação de backups (dados e aplicação): semanalmente;

b) testes periódicos de recuperação de backups (aplicações e serviços hospedados em plataforma em nuvem): semestralmente;

c) simulação de ataques cibernéticos: trimestralmente;

d) testes de *failover* de servidores (nuvem computacional): semestralmente; e

e) treinamento de conscientização para servidores e estudantes: anualmente.

10. COMUNICAÇÃO

O processo de comunicação garante que todas as partes interessadas (estudantes, professores, técnicos administrativos, prestadores de serviços, voluntários, fornecedores e sociedade) estejam informadas e alinhadas durante situações de crise, minimizando impactos negativos e preservando a confiança na instituição. Ao investir em canais eficientes, mensagens claras e treinamento da equipe, o IFTO demonstra seu compromisso com a transparência e a segurança da informação. O instituto adota como canais de comunicação para o PCNSI:

a) Canais Internos

-E-mails institucionais: para comunicados formais e detalhados.

-Sistemas de mensagens internas: ferramentas como Google Chat ou WhatsApp para comunicação rápida.

-Quadros de avisos e murais: para comunicados em locais físicos da instituição.

b) Canais Externos

-Site institucional: para comunicados oficiais à comunidade externa.

-Redes Sociais: Twitter, Instagram e Facebook para atualizações rápidas e engajamento.

-SMS e Notificações por Aplicativo: para alertas urgentes, como cancelamento de aulas ou interrupções críticas.

-Contato com a Imprensa: comunicados à mídia em casos de grande visibilidade.

A tabela 9 apresenta o Plano de Comunicação para o PCNSI seja executado de forma eficiente pelo IFTO.

Tabela 9 - Plano de Comunicação do PCNSI

Estratégia	Ferramenta
Comunicação Equipe de TI	WhatsApp
Comunicação com as autoridades	Sistema Eletrônico de Informações (SEI)
Comunicação com Público Interno	E-mail institucional
Comunicação com Público Externo	Portal institucional

11. TREINAMENTO E CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

O treinamento e a conscientização sobre o PCNSI garante que a comunidade (estudantes, professores, técnicos administrativos, prestadores de serviços, voluntários, fornecedores, parceiros educacionais) estejam cientes de seus papéis e responsabilidades na proteção dos ativos de informação e na resposta a incidentes. O programa de treinamento e conscientização deve ser adaptado para diferentes grupos dentro da instituição:

a) equipe de TI e segurança da informação: foco em técnicas avançadas de proteção, resposta a incidentes e gestão de riscos;

b) gestores e coordenadores: treinamento sobre suas responsabilidades no PCNSI, como tomada de decisão durante crises e comunicação com a comunidade acadêmica;

c) professores e pesquisadores: conscientização sobre a proteção de dados acadêmicos, propriedade intelectual e uso seguro de ferramentas digitais;

d) estudantes: educação sobre práticas básicas de segurança, como criação de senhas fortes, identificação de *phishing* e proteção de dispositivos pessoais;

e) colaboradores administrativos: treinamento em procedimentos de segurança para manuseio de dados sensíveis e uso de sistemas institucionais; e

f) terceiros e fornecedores: orientação sobre políticas de segurança da instituição e requisitos para acesso a sistemas e dados.

Sugere-se o treinamento e a conscientização sobre o PCNSI sejam realizados conforme as seguintes frequências e periodicidade:

a) treinamentos iniciais: para novos colaboradores, professores e estudantes no início de cada semestre ou ano letivo;

b) atualizações periódicas: treinamentos anuais ou semestrais para revisar conceitos e apresentar novas ameaças; e

c) campanhas contínuas: comunicação regular (mensal ou trimestral) para manter a segurança da informação em evidência.

Ao capacitar e engajar toda a comunidade, o IFTO fortalece sua capacidade de prevenir incidentes, responder a crises e proteger seus ativos de informação, garantindo a continuidade de suas operações e a confiança de todos os envolvidos.

12. ATIVAÇÃO DO PCNSI

A ativação do PCNSI deve ocorrer quando um incidente compromete a disponibilidade, integridade, confidencialidade das informações institucionais, impactando as atividades acadêmicas e administrativas.

12.1 Critérios para ativação do PCNSI

O IFTO definiu os seguintes critérios para a ativação do PCNSI:

1.1 Impacto na Continuidade das Atividades Críticas

Se a falha comprometer um ou mais dos seguintes serviços essenciais:

a) Ambiente virtual de aprendizagem (EAD, plataformas educacionais);

b) Sistemas acadêmicos (matrículas, notas, histórico escolar, etc.);

c) Sistemas administrativos e financeiros (pagamentos, folha de pagamento, etc.);

d) Infraestrutura de TI (redes, servidores, conectividade, bancos de dados); e

e) Acesso e autenticação a sistemas (falhas no login, controle de acessos indevidos).

1.2 Gravidade do Incidente

O PCNSI será acionado em casos de:

a) Ataques cibernéticos graves (*ransomware*, DDoS, vazamento de dados sensíveis);

b) Roubo ou exposição de dados acadêmicos e administrativos;

c) Falhas na infraestrutura de TI (colapso de servidores, falha de banco de dados);

d) Interrupção de energia prolongada sem redundância operacional;

e) Desastres naturais (enchentes, incêndios, terremotos) afetando centros de dados; e

f) Falhas humanas que resultem em indisponibilidade significativa dos serviços.

1.3. Tempo Máximo Aceitável de Permanência da Falha (RTO e RPO)

Dois fatores essenciais determinam a ativação do PCNSI:

1.3.1 RTO (Recovery Time Objective - Tempo Objetivo de Recuperação)

A tabela 10 apresenta o tempo máximo aceitável de indisponibilidade de um sistema antes que o IFTO sofra impactos críticos.

Tabela 10 - Tempo Objetivo de Recuperação

Sistema/Ambiente	RTO (Tempo Máximo de Inatividade)
Ambiente Virtual de Aprendizagem (EAD).	8 horas
Sistema acadêmico (matrículas, notas, etc.)	8 horas
Sistemas administrativos e financeiros.	8 horas
Infraestrutura de TI (redes, servidores, etc.)	8 horas
Controle de acesso e autenticação.	8 horas

Se a falha ultrapassar o RTO definido, o PCNSI deve ser ativado para garantir a continuidade operacional.

1.3.2 RPO (Recovery Point Objective - Tempo Objetivo de Perda de Dados)

A tabela 11 determina o tempo máximo aceitável de perda de dados sem causar impactos severos.

Tabela 11 - Tempo Objetivo de Perda de Dados

Sistema/Ambiente	RPO (Máxima perda de dados aceitável)
Ambiente Virtual de Aprendizagem (EAD)	8 horas
Sistemas acadêmicos (matrículas, notas, etc.)	8 horas
Sistemas administrativos e financeiros	8 horas
Infraestrutura de TI (bancos de dados, servidores)	8 horas

Se a perda de dados for superior ao RPO estabelecido, é necessário ativar o plano para recuperar as informações o mais rápido possível.

12.2 Processo de ativação do PCNSI

Para a ativação do PCNSI deve-se seguir os seguintes passos:

1. Identificação do incidente: equipe de TI detecta falha e avalia impacto.

2. Avaliação dos critérios de ativação: comparação com os tempos de RTO e RPO.

3. Aprovação da ativação do PCNSI: Comitê de Gestão de Crises autoriza a execução das medidas de contingência.

4. Implementação do plano de resposta: ações imediatas para contenção e recuperação.

5. Monitoramento e comunicação: informar partes interessadas e avaliar progressos.

6. Restauração completa: retorno ao estado normal e análise pós-incidente.

12.2.1 Responsáveis pela ativação do PCNSI

O responsável pelo setor de Tecnologia da Informação da unidade será o responsável por acionar todos os contatos e partes interessadas na execução do PCNSI. A comunicação deve ser por telefone, ou pessoalmente, caso não seja possível o contato. A tabela 12 apresenta os dados de contato da autoridade responsável pelo PCNSI na unidade do IFTO.

Tabela 12 - Contatos dos Responsáveis pelos Setores de TI das unidades do IFTO

Setor	Responsável pelo Setor de TI	E-mail	Telefone
Araguaína	Diogo Mourão de Almeida Pereira	ti.araguaina@ifto.edu.br	63 3414-0446
Araguatins	Rayllon Rodrigues Sousa Reis	ti.araguatins@ifto.edu.br	63 3474-4800/4806
Colinas do Tocantins	Luciano Ribeiro da Silva	ti.colinas@ifto.edu.br	63 99972-2908
Dianópolis	Kleyton Matos Moreira	ti.dianopolis@ifto.edu.br	63 99992-5276

Formoso do Araguaia	Caio Augusto Gobbo	ti.formoso@ifto.edu.br	63 3357-1982
Gurupi	Eder Carvalho Gomes	ti.gurupi@ifto.edu.br	63 3311-5400/5410
Lagoa da Confusão	Victor Hugo Santos Costa	ti.lagoa@ifto.edu.br	63 3364-1571
Palmas	Isaú Soares de Medeiros	gti.palmas@ifto.edu.br	63 3236-4002/4000
Paraíso	Ricardo Sousa Pimentel	ti.paraiso@ifto.edu.br	63 3361-0310/0300
Pedro Afonso	Pedro Gabriel Cruz Lima	ti.pedroafonso@ifto.edu.br	63 3466-1633
Porto Nacional	Renan Sousa Albuquerque	ti.porto@ifto.edu.br	63 3363-9700/9704
Reitoria	Kleyton Matos Moreira	dti@ifto.edu.br	63 3229-2212
Tocantinópolis	Kleyton Matos Moreira	dti@ifto.edu.br	63 3229-2212

Fonte: Diretoria de Tecnologia da Informação

13. ENCERRAMENTO DO PCNSI

O encerramento do PCNSI e o retorno à normalidade no IFTO segue critérios para garantir que a recuperação seja completa e sustentável. Esse processo envolve a validação da restauração dos serviços, auditoria das ações tomadas, revisão de segurança e comunicação às partes interessadas.

13.1 Critérios para encerramento do PCNSI

O PCNSI será encerrando quando os seguintes parâmetros forem atingidos:

13.1.1 Restauração Completa dos Serviços Críticos

Todos os sistemas críticos apresentados na tabela 13 devem estar operacionais e testados para garantir a continuidade das atividades acadêmicas e administrativas.

Tabela 13 - Sistemas Críticos IFTO

Sistema/Ambiente	Status para Encerramento
Ambiente Virtual de Aprendizagem (EAD)	Disponível, com acessos validados
Sistemas acadêmicos (matrículas, notas, etc.)	Restaurado sem perda de dados
Sistemas administrativos e financeiros	Funcionalidade completa validada
Infraestrutura de TI (redes, servidores, etc.)	Operacional com redundância testada
Controle de acesso e autenticação	Funcionamento normalizado

13.1.2 Conformidade com RTO e RPO

a) o RTO (Tempo Objetivo de Recuperação) foi atendido e não houve impacto prolongado nas operações; e

b) o RPO (Tempo Objetivo de Perda de Dados) foi respeitado, e dados restaurados dentro do limite aceitável.

13.1.3 Validação da Integridade e Segurança dos Dados

Antes do encerramento do PCNSI, é essencial garantir que:
a) não houve perda ou corrupção de dados críticos;
b) os backups utilizados foram testados e verificados; e
c) a integridade dos dados acadêmicos e administrativos foi preservada.

13.1.4 Monitoramento de Segurança e Certificação da Remediação

Para que o PCNSI seja encerrado deve-se verificar:

a) testes de vulnerabilidades foram conduzidos para garantir que o incidente não deixou brechas;

b) medidas corretivas foram aplicadas para evitar recorrências; e

c) sistemas foram atualizados e reforçados com patches de segurança.

13.1.5 Auditoria e Relatório Pós-Incidente

Após a normalização, um relatório completo do incidente deve ser elaborado, incluindo:
a) causa raiz do incidente e medidas para evitar recorrência;
b) ações tomadas durante a resposta ao incidente;
c) impacto operacional e tempo de recuperação; e
d) lições aprendidas e melhorias sugeridas no PCNSI.

13.2. Processo para Retorno à Normalidade

Uma vez cumpridos os critérios de encerramento, o IFTO pode retomar as operações normais seguindo estes passos:

1. **Comunicação Oficial de Normalização**

a) informar estudantes, professores, técnicos administrativos, prestadores de serviços, voluntários, fornecedores, parceiros educacionais sobre o restabelecimento dos serviços; e

b) publicar um comunicado oficial interno e, se necessário, externo.

2. **Reativação Completa dos Processos Acadêmicos e Administrativos**

a) retomar matrículas, aulas, avaliações e operações financeiras sem restrições; e

b) reabrir prazos e restabelecer calendários acadêmicos impactados.

3. **Monitoramento Pós-Incidente**

a) período de observação (24h a 72h) para garantir a estabilidade dos sistemas; e

b) análise contínua de logs e acessos para detectar anomalias.

4. **Revisão e Atualização do PCNSI**

a) incorporar as lições aprendidas para aprimorar o plano; e

b) ajustar políticas de segurança e contingência conforme necessário.

O encerramento do PCNSI deve ocorrer apenas quando todos os critérios forem cumpridos e a normalidade for garantida. Além disso, a avaliação pós-incidente é essencial para fortalecer a resiliência da Instituição de Ensino e prevenir futuros incidentes.

14. REVISÃO E MELHORIA CONTÍNUA

A revisão e melhoria contínua do PCNSI são essenciais para manter a eficácia do plano em uma instituição de ensino. Ao adotar um ciclo constante de avaliação, ajustes e atualizações, o IFTO garante que estará sempre preparado para proteger seus ativos de informação, manter a continuidade de suas operações e cumprir sua missão educacional, mesmo diante de desafios imprevistos. A revisão e melhoria do PCNSI devem ser realizadas de forma contínua, mas com marcos específicos:

a) revisões anuais: avaliação completa do PCNSI, incluindo políticas, procedimentos e infraestrutura;

b) revisões semestrais: análise de resultados de testes e simulações, com ajustes pontuais; e

c) revisões após incidentes: atualização imediata do plano após incidentes reais ou mudanças significativas na infraestrutura de TI.

REFERÊNCIAS

ABNT. NBR ISO 22301:2020. **Segurança e resiliência: sistema de continuidade de negócios (requisitos).**

ABNT. NBR ISO 22313:2020. **Segurança e resiliência: sistemas de gestão de continuidade de negócios (orientações para o uso da ABNT NBR ISO 22301)**.

ABNT. NBR ISO 22316:2020. **Segurança e resiliência: resiliência organizacional (princípios e atributos).**

ABNT. ISO/TS 22317:2020. **Segurança da sociedade: sistemas de gestão de continuidade de negócios (Diretrizes para análise de impacto nos negócios (BIA)).**

ABNT NBR ISO 22320:2020. **Segurança e resiliência: gestão de emergências (Diretrizes para gestão de incidentes).**

ABNT NBR ISO 22322:2020. **Segurança da sociedade: gestão de emergências (Diretrizes para aviso público).**

BRASIL. Gabinete de Segurança Institucional. **Instrução Normativa Nº 1, de 13 de junho de 2008. Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta.** Brasília-DF, 2008. Disponível em: https://www.gov.br/governodigital/pt-br/legislacao/14_IN_01_gsidsic.pdf Acesso em: 4 de fev. 2025.

BRASIL. Departamento de Segurança da Informação e Comunicações / Gabinete de Segurança Institucional da Presidência da República. **Norma Complementar Nº 06, de 11 de novembro de 2009. Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações.** Brasília-DF, 2009. Disponível em: http://dsic.planalto.gov.br/legislacao/nc_6_gcn.pdf Acesso em: 4 de Nov. 2020.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Instrução Normativa Nº 3, de 28 de maio de 2021.** Disponível em: https://www.gov.br/gsi/pt-br/ssic/legislacao/copy_of_IN03_consolidada.pdf Acesso em: 31 de jan. 2024.

IFTO. Diretoria de Tecnologia da Informação. **Política de Segurança da Informação do IFTO.** Palmas-TO, 2020.

IFTO. Diretoria de Tecnologia da Informação. **Plano de Gestão de Riscos para área de TI do IFTO.** Palmas-TO, 2020.

ANEXO I

FLUXO DE GESTÃO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

Fase	Atividade	Responsável
Detecção	Registro de incidente de segurança da informação através dos canais de contato com a equipe de Administração de Crises. -Central de Serviços SUAP. -Plataforma Integrada de Ouvidoria e Acesso à Informação.	Equipe de TI
Diagnóstico	-Investigação sobre a origem do incidente, coletar evidências e avaliar sua gravidade.	Equipe de TI
Tratamento	-Planejamento e execução das ações de contenção, recuperação com retorno dos serviços afetados e mitigação dos impactos. -Definir as ações corretivas e mitigação a serem realizadas. -Implementação de medidas para restaurar a normalidade.	Equipe de TI
Comunicação	-Comunicar as áreas envolvidas na solução do incidente de segurança da informação.	Responsável pelo Setor de TI
Melhoria	-Análise e definição dos procedimentos para evitar reincidência do incidente (melhoria contínua).	Equipe de TI
Finalização	-Revisão do incidente de segurança da informação ocorrido.	Equipe de TI
Treinamento	-Conscientização e treinamento de usuários.	Equipe de TI

ANEXO II

ROTEIRO PARA SIMULAÇÃO DE TESTES DO PCNSI
(ESTRATÉGIAS DE PREVENÇÃO)

1. Identificação

Ano/Semestre	Unidade	Responsável

2. Infraestrutura predial

Estratégia	Procedimentos	Frequência	Responsável	Está adequado (S/V/NA)	Providências necessárias
Combate a incêndio	Verificar funcionamento adequado dos extintores de incêndio.	semestral	Administração	S	
	Verificar a temperatura de equipamentos na sala do datacenter e sala de equipamentos.	diária	Administração	S	
	Verificar o funcionamento adequado do sistema de detecção de incêndio/alarme/detecção de fumaça.	semestral	Administração	S	
Alagamentos	Verificar limpeza de ar-condicionados, calhas, telhas, ralos e canos.	mensal	Administração	S	
Segurança física	Verificar as permissões de acessos para o datacenter e a sala de equipamentos.	semanal	Equipe de TI	S	
	Verificar funcionamento adequado do sistema de vigilância eletrônica.	semanal	Administração	S	
	Verificar acesso de visitantes à salas de equipamentos de TIC.	diário	Administração	S	
Instalações elétricas internas	Verificar estado das instalações elétricas na sala do datacenter e sala de equipamentos.	mensal	Administração	S	
Climatização	Verificar o período de manutenção preventiva do ar-condicionado.	mensal	Administração	S	
Proteção contra raios	Verificar o estado do sistema contra-raios.	semestral	Administração	S	

3. Sistema de energia elétrica

Estratégia	Procedimentos	Frequência	Responsável	Está adequado (S/V/NA)	Providências necessárias
Instalações elétricas externas	Verificar o estado das instalações elétricas externas.	anual	Administração	S	
	Verificar o estado do quadro de energia que alimenta o	anual	Administração	S	

	datacenter e a sala de equipamentos.				
Manutenção do grupo gerador	Verificar as manutenções preventivas realizadas no grupo gerador.	semestral	Administração	S	
	Verificar as manutenções corretivas realizadas no grupo gerador.	semestral	Administração	S	
	Verificar o nível de combustível do grupo gerador.	semanal	Administração	S	
	Verificar o de funcionamento do grupo gerador.	semanal	Administração	S	
Nobreak	Verificar a manutenção preventiva dos nobreaks do data center e sala de equipamentos.	anual	Administração	S	
	Verificar a manutenção corretiva dos nobreaks do data center e sala de equipamentos.	anual	Administração	S	

4. Ativos de rede

Estratégia	Procedimentos	Frequência	Responsável	Está adequado (S/V/NA)	Providências necessárias
Manter ativos de rede em condições adequadas	Realizar acompanhamento sobre período de garantia de equipamento.	semestral	Equipe de TI	S	
	Realizar testes de funcionamento do equipamento.	semestral	Equipe de TI	S	
	Realizar revisão de documentação de configuração de equipamento.	semestral	Equipe de TI	S	
	Verificar se equipamento consta no inventário de equipamentos IFTO.	anual	Equipe de TI	S	
Atualização do *firmware*	Verificar atualizações de *firmware* para equipamento.	semestral	Equipe de TI	S	
Configuração de *hardware* e *software*	Verificar atualizações de *hardware* e *software*.	semestral	Equipe de TI	S	
Backup	Verificar a existência de cópias de segurança de dados e sistemas.	trimestral	Equipe de TI	S	
	Simular recuperação de *backup* de dados e sistemas.	trimestral	Equipe de TI	S	

Redundância	Testar a redundância em dos dispositivos principais de rede (*switches*, servidores etc).	mensal	Equipe de TI	S	

5. Conectividade

Estratégia	Procedimentos	Frequência	Responsável	Está adequado (S/V/NA)	Providências necessárias
Gestão dos serviços de conectividade Internet	Verificar situação de contratos com operadoras de Internet.	anual	Responsável pela TI na Unidade	S	
	Testar o funcionamento dos *Links* de Internet.	mensal	Equipe de TI	S	
Monitoramento e correções automáticas	Verificar atualizações de *hardware* e *software*.	mensal	Equipe de TI	S	
Acesso à Internet em contingência	Testar redundância de *Link* de Internet.	mensal	Equipe de TI	S	
	Testar *failover* de Link de Internet.	mensal	Equipe de TI	S	
Fibra óptica	Verificar estado das conexões de fibras ópticas.	semestral	Equipe de TI	S	
	Testar comunicação através das fibras ópticas.	anual	Administração	S	

6. Sistemas básicos

Estratégia	Procedimentos	Frequência	Responsável	Está adequado (S/V/NA)	Providências necessárias
Instalação	Verificar inconsistências em serviços e *softwares* instalados.	mensal	Equipe de TI	S	
Atualização	Verificar atualizações automáticas de sistemas.	mensal	Equipe de TI	S	
	Verificar relatórios de sistemas operacionais no *software* GLPI.	mensal	Equipe de TI	S	
Licenciamento	Verificar licenças de sistemas operacionais.	anual	Equipe de TI	S	
Cópia de segurança (backup)	Verificar o funcionamento adequado dos *scripts* de *backup.*	semanal	Equipe de TI	S	
	Testar a restauração do *backup*.	semanal	Equipe de TI	S	
	Verificar a qualidade e o	semanal	Equipe de TI	S	

	tempo de vida dos dispositivos e mídias utilizados para *backup.*				
Certificado SSL	Verificar validade dos certificados digitais em serviços e sistemas de informação.	trimestral	Equipe de TI	S	

7. Sistemas Desenvolvidos pelo IFTO

Estratégia	Procedimentos	Frequência	Responsável	Está adequado (S/V/NA)	Providências necessárias
Gestão de mudanças	Verificar registro de mudanças em serviços e sistemas de informação.	mensal	Responsável pela Equipe de TI	S	
Controle de versões	Testar integridade das versões de sistemas desenvolvidos pelo IFTO.	mensal	Responsável pela Equipe de TI	S	
Desenvolvimento seguro	Testar do código fonte visando segurança cibernética.	semestral	Equipe de TI	S	
	Testar as mudanças em ambiente de homologação.	semestral	Equipe de TI	S	
	Testar homologação de mudanças.	semestral	Responsável pela Equipe de TI	S	
Servidor de aplicação e banco de dados	Testar conexões entre banco de dados e aplicações.	semestral	Equipe de TI	S	
	Testar autenticação de usuários.	semestral	Equipe de TI	S	
	Testar *scripts* de integração com outros sistemas.	semestral	Equipe de TI	S	
	Testar procedimentos de criação e restauração de dados.	semestral	Equipe de TI	S	
	Verificar atualizações de segurança.	mensal	Equipe de TI	S	
Sistema de Controle de acesso	Testar autenticação de usuários e sistemas.	semanal	Equipe de TI	S	
	Testar comunicação dos sistemas de informação e serviços de TI.	semanal	Equipe de TI	S	
	Testar a comunicação de rede.	semanal	Equipe de TI	S	
	Verificar atualizações	semanal	Equipe de TI	S	

	automáticas de segurança.				

8. Sistemas de Terceiros

Estratégia	Procedimentos	Frequência	Responsável	Está adequado (S/V/NA)	Providências necessárias
Contratos	Verificar funcionamento adequado da aplicação	mensal	Fiscal do Contrato	S	
	Testar segurança da aplicação	semestral	Responsável pela Equipe de TI	S	

9. Providências necessárias

Providência	Encaminhamento

10. Observações gerais

ANEXO III

RELATÓRIO DE REGISTRO E TRATAMENTO DE INCIDENTE

1. Identificação

Data	Hora	Responsável pelo registro	Origem
Fonte da detecção do incidente		( ) Identificado pela Equipe de TI. ( ) Notificação do Administrador de Redes. ( ) Denúncia de titulares/terceiros. ( ) Notícias ou redes sociais. ( ) Notificação da ANPD. ( ) Outros: _____ _____	
Descrição da forma como o incidente foi conhecido			

2. Definição

Descrição	
Escopo	( ) Dados ( ) Dados Pessoais ( ) Infraestrutura de rede ( ) Segurança ( ) Serviços de TI ( ) Outro: _____
Tipo	( ) Acesso não autorizado a sistemas de informação. ( ) Alteração/exclusão não autorizada de dados. ( ) Descarte incorreto de documentos ou dispositivos eletrônicos. ( ) Divulgação indevida de dados pessoais. ( ) Exploração de vulnerabilidade em sistemas de informação. ( ) Falha em equipamento (hardware). ( ) Falha no sistema de contingência de energia elétrica. ( ) Falha em sistema de informação (software). ( ) Negação de Serviço (DDos). ( ) Perda/roubo de documentos ou dispositivos eletrônicos. ( ) Publicação não intencional de dados pessoais. ( ) Roubo de credenciais / engenharia social. ( ) Sequestro de dados. ( ) Violação de credencial. ( ) Vírus de computador/malware. ( ) Outro tipo de incidente cibernético:_____

Princípios de SI afetados	( ) Autenticidade ( ) Confidencialidade ( ) Disponibilidade ( ) Integridade
Reincidência	( ) Sim ( ) Não

3. Diagnóstico

Data/Hora		**Responsável**	
Análise			
Priorização	Gravidade (G)		**Pontuação GUT** G X U X T
	Urgência (U)		
	Tendência (T)		
Impacto			
Necessário informar DPO:	( ) Sim ( ) Não	**Doc. SEI:**	
Ações necessárias			
Natureza dos dados pessoais afetados			
Informações sobre os titulares de dados pessoais envolvidos			

4. Tratamento

Data/hora conclusão			**Responsável**	
Ações realizadas				
Informações complementares				
Notificação DPO	**Data**		**Protocolo**	

5. Melhoria

Data/Hora		**Responsável**	
Medidas de segurança necessárias	( ) Atualização de Sistemas. ( ) Controle de acesso físico. ( ) Controle de acesso lógico. ( ) Cópias de segurança (*backups*). ( ) Criptografia/Pseudonimização. ( ) Firewall. ( ) Gestão de ativos. ( ) Monitoramento de uso de rede e sistemas. ( ) Múltiplos fatores de autenticação. ( ) Plano de resposta a incidentes. ( ) Política de Segurança da Informação. ( ) Política de Privacidade. ( ) Processo de Gestão de Riscos. ( ) Proteção *endpoint* (antivírus). ( ) Registro de incidentes. ( ) Registro de acesso (logs). ( ) Segregação de rede. ( ) Testes de invasão. ( ) Outras: _____		
Ações necessárias específicas			

Informações complementares	

ANEXO IV

CHECKLIST PARA ACOMPANHAMENTO DE RECUPERAÇÃO DE DESASTRES

Etapa	Procedimento	Responsável	Status (✓/✗)	Observações
1. Identificação do Incidente				
1.1	Detectar e registrar o incidente (ex.: ataque cibernético, vazamento de dados).	Equipe de TI		
1.2	Classificar o incidente conforme a gravidade e o impacto.	Administrador de Redes		
2. Contenção do Incidente				
2.1	Isolar sistemas ou redes afetados para evitar propagação.	Administrador de Redes		
2.2	Desativar contas comprometidas ou acessos suspeitos.	Administrador de Redes		
2.3	Coletar evidências para análise forense (logs, arquivos, etc.).	Administrador de Redes		
3. Análise e Diagnóstico				
3.1	Identificar a causa raiz do incidente (ex.: malware, falha humana).	Administrador de Redes		
3.2	Avaliar o impacto nos sistemas, dados e operações do IFTO.	Administrador de Redes		
4. Comunicação				
4.1	Notificar a equipe de gestão e o comitê de continuidade de negócios.	Responsável pelo setor de TI na unidade		
4.2	Informar a comunidade acadêmica sobre o incidente e as medidas em andamento.	Responsável pelo setor de comunicação institucional		
4.3	Comunicar-se com órgãos reguladores, se necessário (ex.: ANPD, MEC).	Responsável pelo setor jurídico		
5. Recuperação de Sistemas				
5.1	Restaurar sistemas críticos a partir de *backups* seguros.	Administrador de Redes		
5.2	Verificar a integridade dos dados restaurados.	Administrador de Sistemas		
5.3	Reconfigurar sistemas e redes para garantir segurança reforçada.	Administrador de Redes		
5.4	Realizar testes de funcionalidade dos sistemas recuperados.	Equipe de TI		
6. Mitigação de Riscos				
6.1	Aplicar *patches* de segurança e atualizações em sistemas vulneráveis.	Administrador de Redes		
6.2	Reforçar políticas de acesso (ex: autenticação de dois fatores).	Administrador de Redes		
6.3	Revisar e atualizar políticas de backup e recuperação de desastres.	Administrador de Sistemas		
7. Treinamento e Conscientização				
7.1	Realizar treinamentos para a equipe sobre lições aprendidas.	Responsável pelo Setor de TI da unidade		
7.2	Promover campanhas de conscientização sobre segurança da informação para a comunidade acadêmica.	Setor de Comunicação		
8. Documentação e Relatório				
8.1	Documentar detalhes do incidente, ações tomadas e resultados.	Equipe de TI		
8.2	Elaborar relatório final para a gestão e órgãos reguladores, se necessário.	Equipe de TI		

Etapa	Procedimento	Responsável	Status (✓/✗)	Observações
9. Revisão e Melhoria				
9.1	Revisar o plano de recuperação de desastres com base nas lições aprendidas.	Equipe de TI		
9.2	Implementar melhorias nos processos e tecnologias de segurança.	Equipe de TI		

ANEXO V
PLANO DE PREVENÇÃO, DETECÇÃO E RESPOSTA PARA ATAQUES DE MALWARE

Etapa	Procedimento	Atividade	Responsável
Prevenção e Preparação	Avaliação de riscos	Identificar sistemas críticos, vulnerabilidades e possíveis vetores de ataque.	Equipe de TI.
	Backup regular	Implementar backup automático e armazenar cópias em locais offline e seguros.	Equipe de TI.
	Políticas de Segurança	Atualizar e treinar equipes sobre boas práticas e protocolos de segurança.	Equipe de TI.
	Monitoramento e Detecção	Implementar ferramentas de detecção de malware e monitoramento de rede.	Equipe de TI.
	Plano de Resposta a Incidentes	Elaborar um plano de resposta documentado, com atribuição de responsabilidades.	Responsável pelo Setor de TI.
Detecção e Contenção	Identificação do Incidente	Confirmar o ataque por meio de alertas, logs ou comportamento anormal do sistema.	Equipe de TI
	Isolamento	Desconectar dispositivos e sistemas afetados da rede para evitar propagação	Desconectar dispositivos e sistemas afetados da rede para evitar propagação.
	Bloqueio de Ameaça	Utilizar ferramentas de segurança para bloquear arquivos maliciosos e suspender credenciais comprometidas.	Equipe de TI.
	Comunicação Interna	Notificar equipes de segurança, TI e liderança, evitando divulgação não autorizada.	Equipe de TI.

Erradicação e Recuperação	Análise Forense	Identificar a origem e a extensão do ataque, preservando evidências.	Equipe de TI.
	Remoção do Malware	Executar ferramentas de remoção de malware e varreduras completas.	Equipe de TI.
	Restauração de Dados	Recuperar sistemas e dados a partir de backups seguros, evitando reintroduzir *malware.*	Equipe de TI
	Testes e Validação	Garantir que todos os sistemas estejam limpos e operacionais antes de restabelecer as operações.	Equipe de TI
Comunicação e Notificação	Comunicação com Stakeholders	Informar clientes, fornecedores e autoridades conforme exigido por regulamentações.	Responsável pelo setor de TI
	Registro do Incidente	Documentar todas as etapas e decisões tomadas durante a resposta.	Responsável pelo setor de TI
	Assessoria Legal	Consultar especialistas para avaliação das implicações legais e cumprimento de legislações.	Responsável pelo setor de TI
Avaliação Pós-Incidente e Melhoria Contínua	Análise de Causa Raiz	Revisar o incidente para compreender as falhas que permitiram o ataque.	Equipe de TI
	Aprimoramento do Plano	Atualizar protocolos, políticas e ferramentas com base nas lições aprendidas.	Equipe de TI
	Treinamentos e Simulações	Reforçar capacitação dos colaboradores e realizar testes periódicos do plano de resposta.	Equipe de TI
	Revisão de Controles	Avaliar e fortalecer os mecanismos de proteção, como firewalls, autenticação multifator e gestão de acessos.	Equipe de TI
Melhoria Contínua	Investir em Segurança	Manter uma cultura de segurança cibernética e investir em tecnologias adequadas.	Alta Gestão
	Engajamento Contínuo	Promover conscientização entre todos os níveis da	Setor de Gestão de Pessoas

		organização sobre ameaças cibernéticas.	

ANEXO VI
PLANO DE RESPOSTAS A RISCOS, AMEAÇAS E VULNERABILIDADES

Risco/Ameaça	Impacto	Procedimento a ser realizado	Atividade a ser executada	Responsável
Vazamento de Dados Pessoais.	Perda de confiança dos estudantes, servidores e comunidade, multas por descumprimento da LGPD, danos à reputação da instituição e processos judiciais.	Investigar e conter o vazamento.	Bloquear acessos comprometidos.	Equipe de TI
Ataques Cibernéticos.	Paralisação das operações, perda de dados, perda de confiança dos estudantes, servidores e comunidade e custos de recuperação e danos à imagem da instituição.	Isolar e mitigar o ataque.	Aplicar correções e reforçar *firewall.*	Administrador de Redes
Acesso Não Autorizado.	roubo de informações, alteração ou exclusão de dados críticos e fraudes.	Revogar acessos indevidos.	Revisar *logs* e senhas.	Administração de Redes
Falhas em Sistemas ou *Hardware.*	Paralisação das atividades acadêmicas e administrativas, atrasos acadêmicos, prejuízos financeiros, perda de informações.	Substituir hardware. Atualizar/corrigir sistema	Implementar medidas corretivas.	Equipe de TI
Uso Inadequado de Dispositivos Pessoais.	Exposição de dados acadêmicos, financeiros ou pessoais (LGPD), acesso indevido a pesquisas confidenciais, infecção por malware (ransomware, spyware), comprometimento de credenciais institucionais (phishing), acesso não autorizado a e-mails, sistemas acadêmicos e banco de dados, fraude em matrículas ou emissão de documentos, sanções legais por descumprimento da LGPD, suspensão de acessos ou responsabilização	Impor políticas de uso seguro de recursos computacionais.	Educar usuários sobre segurança da informação.	Equipe de TI

	disciplinar, disseminação de vírus na rede institucional e ataques a servidores internos via conexão insegura.			
Engenharia Social e *Phishing.*	Roubo de credenciais, acesso não autorizado a sistemas e vazamento de dados.	Realizar campanhas de conscientização sobre segurança da informação.	Testar usuários com simulações.	Gestor de Segurança da Informação
Falta de *Backup* ou *Backup* Inadequado.	Perda permanente de dados e interrupção prolongada das operações e impacto negativo em rankings educacionais.	Revisar e corrigir políticas de *backup.* Realizar monitoramento contínuo das estratégias de *backups.*	Criar políticas de *backup* eficientes.	Administrador de Redes
Vulnerabilidades em Sistemas de Terceiros.	Comprometimento da rede institucional, vazamento de dados, ataques à rede interna, interrupção de serviços e danos reputacionais; comprometimento de sistemas dependentes (ex.: paralisação do SUAP devido a falha no provedor de nuvem); perda de confiança de alunos e parceiros devido a incidentes recorrentes.	Corrigir vulnerabilidades e aplicar *patches.*	Fazer auditorias de segurança da informação.	Prestador de Serviços
Uso Indevido de Redes Wi-Fi.	vazamento de dados, ataques internos, uso indevido de recursos de rede e ataques internos, fraudes e golpes.	Monitorar e restringir acessos.	Aplicar criptografia em redes.	Administração de Redes
Desastres Naturais ou Acidentes.	Perda de hardware, interrupção de serviços, corrupção de dados, prejuízos financeiros e acadêmico.	Ativar planos de recuperação de desastres.	Implementar soluções de contingência.	Alta Gestão
Falta de Conscientização e Treinamento.	Vazamento de dados, invasão de sistemas, infecção por malware, fraudes e danos à reputação.	Realizar treinamentos periódicos de segurança da informação.	Promover cursos de cibersegurança.	Setor de Gestão de Pessoas
Não Conformidade com a LGPD.	Sanções administrativas, indenizações por danos morais, suspensão de sistemas, interrupção de matrículas e avaliações e perda de credibilidade em rankings educacionais.	Ajustar processos para conformidade com a LGPD.	Criar planos de adequação com a LGPD.	Alta Gestão
Exposição de Dados em	Vazamento de dados acadêmicos,	Restringir permissões de	Monitorar o uso de plataformas	Administrador de Redes

Plataformas de Ensino.	manipulação de notas, interrupção do sistema de informação e pesquisas comprometidas.	acesso.	de Ensino.	
Fraudes e Manipulação de Dados.	Jurídico, acadêmico, reputacional e financeiro.	Investigar fraudes e reforçar segurança.	Implementar sistemas antifraude.	Administrador de Redes
Riscos em Dispositivos Móveis.	Vazamento de dados, acesso não autorizado a sistemas, fraudes, sanções e danos reputacionais.	Monitorar dispositivos móveis.	Configurar controles de acesso.	Equipe de TI
Falha Humana.	Perda de dados acadêmicos, interrupção operacional, retrabalho, riscos legais e danos à confiança.	Automatizar processos. Realizar capacitações periódicas.	Criar campanhas de conscientização e treinamento sobre segurança da informação.	Setor de Gestão de Pessoas
Falha de Energia.	Perda de dados, interrupção de aulas, prejuízos financeiros, riscos à segurança e impacto acadêmico.	Ativar geradores e fontes alternativas.	Redirecionar operações para fontes alternativas.	Alta Gestão
Falha de Conectividade.	Interrupção de aula EAD, inacessibilidade de sistemas, perda de produtividade, comprometimento de dados e danos reputacionais.	Estabelecer redundâncias de conectividade.	Garantir conexões seguras alternativas.	Administrador de Redes
Violação de Privacidade.	jurídico/regulatório, reputacional, operacional e psicológico	Estabelecer um Programa de Conscientização, Educação e Treinamento em Segurança da Informação.	Realizar capacitações semestrais sobre LGPD e simulações de vazamentos para testar respostas.	Responsável pelo Setor de TI Setor de Gestão de Pessoas

Documento assinado eletronicamente por **Fabiana Ferreira Cardoso**, **Gestor (a) de Segurança da Informação**, em 10/04/2025, às 10:26, 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 10/04/2025, às 10:40, 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 **2733886** e o código CRC **61DB53C1**.