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

PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

HISTÓRICO DE REVISÕES

Data	Item	Descrição
20/12/2023	1	Elaboração do programa de governança em privacidade.

1. INTRODUÇÃO

Um programa de governança em privacidade (PGP) deve ser projetado para proteger os direitos do cidadão em relação à privacidade da informação e deve ser desenvolvido e implementado seguindo as leis jurisdicionais relevantes. O PGP no IFTO consolida as atividades que visam garantir a proteção à privacidade e o cuidado adequado com os dados coletados e tratados.

Existe o entendimento de que o PGP deverá ser atualizado e ampliado permanentemente, de forma a retratar o amadurecimento e desafios institucionais, observando sempre o alinhamento com as diretrizes determinadas pela ANPD. Por isso, o IFTO tem executado ações visando a conformidade relacionada à Privacidade de Dados.

O PGP definido pelo IFTO é baseado nas recomendações publicadas pela Secretaria de Governo Digital. A estrutura é concebida a partir do ciclo PDCA (Plan, Do, Check e Act) bem como as ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27701:2019. Tecnologia da Informação - Técnicas de Segurança – Código de Prática para controles de segurança da informação e ABNT NBR ISO/IEC 27005:2011. Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.

1.1. Escopo

O escopo do PGP abrange inicialmente os serviços de tecnologia da informação, tais como: SUAP - Sistema Unificado de Administração Pública, SEI - Sistema Eletrônico de Informação, Correio Eletrônico (E-mail) dentre outros.

1.2. Objetivos

O objetivo do PGP é implementar medidas que visem garantir a proteção de dados e a privacidade dos usuários dos serviços do IFTO sempre em consonância com melhores práticas e legislação vigente. Para que este objetivo seja alcançado são definidas os seguintes objetivos específicos:

a) demonstrar o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) ser aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) ser adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

d) estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) estar integrado a sua estrutura geral de governança e estabelecer e aplicar mecanismos de supervisão internos e externos;

g) contar com planos de resposta a incidentes e remediação; e

h) estar atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

1.3. **Abrangência**

O PGP abrange usuários da rede IFTO: servidores, estudantes, prestadores de serviços, parceiros de negócios, fornecedores de tecnologias e *softwares*, órgãos reguladores e auditorias e outras partes interessadas.

1.4. **Benefícios esperados**

A partir da execução do PGP espera-se ter os seguintes benefícios:

a) redução de riscos e vulnerabilidades a partir da educação de usuários sobre violações de segurança, ataques cibernéticos e vazamentos de dados;

b) ter conformidade com os padrões de segurança da informação recomendados na legislação vigente;

c) proteger a imagem institucional ao demonstrar compromisso com a segurança de dados dos servidores, estudantes, prestadores de serviços e partes interessadas;

d) reduzir erros humanos tais como abertura de e-mails de phishing ou divulgação de senhas;

e) economizar dinheiro em termos de custos de recuperação, multas e ações legais;

f) implantar a cultura de segurança da informação onde todos os usuários compreendam a importância da proteção de informação e fazer da segurança uma prioridade;

g) proteger informações sensíveis e ativos do IFTO por meio de melhores práticas de segurança da informação;

h) aumenta a confiança de todas as partes interessadas.

2. GOVERNANÇA DE PRIVACIDADE DE DADOS

A governança de privacidade de dados tem o objetivo de garantir a proteção de dados e a privacidade dos cidadãos em todas as etapas de desenvolvimento dos processos organizacionais do IFTO. Neste sentido o IFTO pretende atender a Lei n° 13.709, de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) deforma a assegurar a proteção à privacidade, a transparência, o desenvolvimento econômico e tecnológico, a padronização de normas, a segurança jurídica e o favorecimento à concorrência e a livre atividade econômica.

3. ESTRUTURA DO PROGRAMA DE GOVERNANÇA DE PRIVACIDADE

O PGP estabelece uma metodologia que influenciará permanentemente os processos de tomada de decisão com base em riscos e melhorias contínuas na maturidade da organização. Ele é estruturado em 3 (três) etapas, conforme apresentada a figura 1.

Figura 1 - Etapas do PGPD

O PGP apresentado na figura 1 estabelece uma metodologia abrangente que influenciará permanentemente os processos de tomada de decisão com base em riscos e melhorias contínuas na maturidade. Pode-se, entretanto, criar projetos para alcançar os objetivos do programa.

Na criação de projetos para se alcançar os objetivos do PGP, deve-se selecionar a metodologia mais adequada a realidade institucional (SGD, 2023).

3.1. Iniciação e Planejamento

Esta etapa busca compreender quais as informações e dados importantes deve ser conhecidos. Segundo o guia de elaboração de programa de governança em privacidade da SGD/ME, esta etapa consiste nos seguintes marcos: nomeação do Encarregado de Tratamento de Dados; alinhamento de expectativas com a alta administração; análise da maturidade - diagnóstico do atual estágio de adequação à LGPD; análise e adoção de medidas de segurança, inclusive diretrizes e cultura interna; instituição de estrutura organizacional para

governança e gestão de proteção de dados pessoais; inventário de dados pessoais; e levantamento dos contratos relacionados a dados pessoais. Esta etapa envolve as atividades:

a) alinhamento de expectativas entre o encarregado e a alta direção do IFTO, priorizando as ações mais urgentes, se, esquecer de mencionar os projetos e as estruturas da organização envolvidas;

b) apresentação, para pró-reitores, diretores, gerentes e dirigentes o papel exercido pelo encarregado de tratamento de dados como relevante e influenciador: como o encarregado pode servir e agregar valor ao IFTO, dado o disposto na LGPD e confirmar e garantir aos servidores do IFTO que, enquanto representante interno da ANPD, seu papel deve ser uma assistência de grande valor e não um obstáculo;

c) priorização e foco em melhorias, tendo consciência da estrutura, dos requisitos de dados pessoais, bem como da maturidade de *compliance* do IFTO: Lançamento e implementação de mecanismos para geração de relatórios internos de atividades de processamento de dados pessoais, sejam tais atividades novas, majoritárias ou com alterações; Conclusão de um inventário de dados pessoais, destacado no início desta seção, com a lista dos principais serviços que utilizam dados pessoais do órgão; e

d) alcance de credibilidade e valor entre os dirigentes do IFTO;

e) apresentação de minuta de política de privacidade aos dirigentes do IFTO, com o comprometimento de revisar, conforme os apontamentos de melhorias sugeridos;

f) instituição, em conjunto com o Comitê de Governança de TI do IFTO ou, e coordenação de uma estrutura organizacional para governança e gestão da proteção de dados pessoais;

g) projeção ou refinamento de uma nova estratégia de privacidade: um mapeamento do atual cenário e fornecimento de uma visão geral do orçamento necessário, bem como a associação e o relacionamento aos pontos de atenção listados;

h) avaliação de maturidade da organização, observando fatores como a rastreabilidade de dados, estruturando-os e descrevendo as informações tratadas em cada sistema, a comunicação com o cidadão e a transparência. Além de retratar o nível de adequação à LGPD, o índice de maturidade é também utilizado como um índice de performance;

g) medidas de segurança devem ser analisadas e adotadas, revisando e propondo aprimoramento das diretrizes e cultura internas;

h) estrutura organizacional para a governança e gestão de proteção de dados;

i) mapeamento de dados pessoais utilizados pelo IFTO, realizado através de um inventário de dados, especialmente dos dados pessoais; e

j) levantamento dos serviços que tratam dados pessoais no Inventário de dados viabiliza a relação de um cruzamento com os contratos que os suportam. O mapeamento de contratos relativos ao tratamento de dados pessoais contribui para possíveis e necessárias adequações contratuais, tanto nos contratos existentes, quanto nos futuros.

Nesta fase deve ser incluída uma estrutura organizacional para compor o conhecimento de dados pessoais em todo o IFTO, além de supervisionar as três etapas de ações executadas na criação e manutenção do Programa de Privacidade de Dados.

3.2. Construção e Execução

Esta etapa trata da implementação propriamente dita do Programa de Governança de Privacidade e deve considerar: gerenciamento de direitos individuais, consentimento e rastreamento de preferência e redução de responsabilidade por violação. Esta etapa consiste nos seguintes marcos: políticas e práticas para proteção da privacidade do cidadão; cultura de segurança e proteção de dados e *privacy by design*; relatório de impacto à proteção de dados pessoais (RIPD); política de privacidade e política de segurança da informação; adequação de cláusulas contratuais; e termo de uso. Esta etapa envolve as atividades:

a) implementação do plano de ação elaborado e detalhado na fase de Planejamento;
b) demonstração, para os dirigentes do IFTO, do progresso e dos resultados obtidos com as atividades envolvendo o inventário dos dados e a divulgação e conscientização da LGPD junto aos servidores;
c) se necessário, redefinição de prioridades, baseando-se nos resultados alcançados e no retorno dos dirigentes do IFTO.
d) estabelecimento e manutenção de documentação relacionada à LGPD e aos dados pessoais tratados no órgão, com informações sobre: atividades em andamento e planejadas; responsáveis pelos serviços e sistemas que utilizam dados pessoais; e incidentes e vazamento de dados pessoais.
e) definição de mecanismos de reportes internos, assegurando transparência e rapidez na troca de informação, além de reafirmar o papel como facilitador, suporte e nunca um obstáculo.

Os marcos da etapa de Construção e Execução são:

a) políticas e práticas para a proteção da privacidade do cidadão: papéis específicos dos servidores envolvidos na coleta, retenção, processamento, compartilhamento e eliminação de dados pessoais; educação dos usuários em relação a políticas e práticas de proteção de privacidade e dos cidadões em relação aos seus direitos quanto à privacidade da informação;

b) cultura de segurança e proteção de dados e *privacy by design*: intuito de comunicar os objetivos, metas e indicadores utilizados, além de divulgar o papel da administração pública como custodiante dos dados e sua responsabilidade ao tratar os dados pessoais dos cidadões;

c) relatório de impacto à proteção de dados pessoais (RIPD): instrumento de verificação e demonstração da conformidade do tratamento de dados pessoais realizado pela instituição e serve tanto para a análise quanto para a documentação do tratamento dos dados pessoais. Descreve os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

d) política de privacidade e política de segurança da informação: desenvolvimento ou atualização das diretrizes internas de proteção de dados pessoais. Deve ser verificado se não há tratamento excessivo de dados, se os controles de segurança são suficientes para os dados tratados, se é necessário a retenção de determinados dados tratados e se é necessário revisar contratos;

e) adequação de cláusulas contratuais: os contratos devem apresentar informações sobre delimitações claras e objetivas das responsabilidades do controlador e operador; a forma que é realizada a coleta e o tratamento de dados; a existência da possibilidade de o titular acessar os seus dados coletados, a forma que é realizada a correção, bloqueio ou eliminação de dados mediante solicitação do titular; a existência da possibilidade de revogação do consentimento dado do titular; o detalhamento de quem tem acesso aos dados, o responsável por seu uso e tratamento, a forma de armazenamento e as particularidades de possíveis auditorias; e as medidas de proteção e segurança dos dados coletados e armazenados pela contratada;

f) termo de uso: documento que fornece uma descrição detalhada do serviço, das condições e das regras aplicáveis a ele..

3.3. Monitoramento

Esta etapa é responsável por garantir o aprimoramento contínuo do Programa de Governança em Privacidade. A etapa aborda aspectos que incluem, em grande parte, coleta e análise de informações, bem como elaboração de relatórios e apresentação de resultados. Ela consiste nos seguintes marcos: indicadores de performance, gestão de incidentes e análise e reporte de resultados. Esta etapa envolve as atividades:

a) gerenciamento do estabelecimento de métricas para auxiliar no acompanhamento das ações do programa de gerenciamento de privacidade;

b) divulgação dos resultados entre as diversas áreas do órgão - estabelecimento de uma estrutura de divulgação de resultados para a alta administração do IFTO.

Os marcos da etapa monitoramento são:

a) indicadores de performance: incluem a análise regular dos principais indicadores de desempenho para verificar lacunas no PGP assim como o status de outras iniciativas de privacidade;

b) gestão de incidentes: registra os incidentes de segurança da informação e de privacidade ocorridos e que armazene informações como: a descrição dos incidentes ou eventos, as informações e sistemas envolvidos, as medidas técnicas e de segurança utilizadas para a proteção das informações, os riscos relacionados ao incidente e as medidas tomadas para mitigá-los a fim de evitar reincidências;

c) análise de resultados: demonstra o valor do PGP à alta administração;

d) reporte de resultados: mostra a evolução das ações e resultados obtidos, bem como o papel da privacidade para o cidadão reforçam e fortalecem a cultura de privacidade de dados.

4. PAPÉIS E RESPONSABILIDADES

Conforme determina a Lei Geral de Proteção de Dados são definidos os seguintes papéis e responsabilidades para o programa de privacidade de dados:

4.1. Titular

Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento, podendo ser servidores, discentes ou pessoas físicas externas ao IFTO.

4.2. Controlador

Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, neste caso, o IFTO. O controlador pode exercer diretamente o tratamento dos dados, mas pode, também, designar um operador.

4.3. Operador

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, podendo ser: servidor responsável por atividades administrativas ou sistêmicas; membro de colegiado que trata de dados pessoais; e ainda qualquer agente público cuja atividade exija o tratamento de dados pessoais no âmbito do IFTO, incluindo, neste caso, os setores de controle da instituição, tais como: Auditoria Interna, Corregedoria, Comissão de Ética e Procuradoria.

4.4. Encarregado de Tratamento de Dados Pessoais

Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Compete à esta pessoa:

a) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

b) receber comunicações da autoridade nacional e adotar providências;

c) orientar os servidores, estudantes e prestadores de serviço a respeito das práticas a serem tomadas em relação de dados pessoais;

d) apoiar a definição das diretrizes de construção do inventário de dados pessoais relativas ao registro das operações de tratamento de dados pessoais determinado pelo art. 37 da LGPD;

e) conduzir ou aconselhar a elaboração de relatório de impacto à proteção de dados pessoais, de acordo com casos previstos pela LGPD em que tal documento é necessário;

f) conduzir ou aconselhar a implementação de regras de boas práticas e de governança específicas pelo art. 50 da LGPD;

g) Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

4.5. Autoridade Nacional de Proteção de Dados

Órgão vinculado à Presidência da República responsável por fiscalizar a aplicação da LGPD nas entidades da Administração Pública e aplicar sanções em caso de descumprimento de suas determinações, entre outras atribuições. Tem a missão de regular o setor de tratamento de dados pessoais. Está autorizada, portanto, a agir em proteção aos princípios e fundamentos da Lei Geral de Proteção de Dados; e

4.6. Comissão Permanente de Gerenciamento de Dados Institucionais do IFTO

Comissão responsável por apoiar o encarregado nas ações de avaliação de abertura de dados públicos e nas ações de tratamento de dados quanto à adequação à Lei Geral de Proteção de Dados Pessoais.

5. MATRIZ RACI

A matriz RACI apresentada na tabela 3 é utilizada para definir com clareza as atribuições, papéis e responsabilidades de cada colaborador nas atividades do processo. A sigla RACI significa, em inglês: *Responsible, Accountable, Consulted e Informed*.

a) responsible (responsável): pessoa, função ou unidade organizacional responsável pela execução de uma atividade no âmbito de um processo; representa quem irá, de fato executar a tarefa. Deve haver ao menos um por tarefa;

b) accountable (responsabilizado): dono da atividade, deverá fornecer os meios para que a atividade possa ser executada, e será responsabilizado caso a atividade não alcance os seus objetivos; cada atividade só pode possuir um *Accountable*; Define quem será responsável pelo sucesso da atividade. Fica encarregado de verificar se a atividade foi realizada com sucesso e dentro do prazo. Deve haver um, e apenas um, por atividade;

c) consulted (consultado): pessoa que deve ser consultada durante a execução da atividade; As informações levantadas junto a essas pessoas tornam-se entradas para a execução da atividade; Geralmente exercem papel de conselho na tomada de decisões;

d) ***informed (informado):*** pessoa que será informada acerca do progresso da execução da atividade.

Tabela 1 - Matriz de responsabilidades

Etapa	AA	CSI	ETDP	CPGDI	DTI	T
Iniciação e Planejamento.	A	C	R	C	I	I
Construção e Execução.	A	C	R	C	I	I
Monitoramento.	A	C	R	C	I	I

Legenda:

AA: Alta Administração

CSI: Comitê de Segurança da Informação.

ETDP: Encarregado de Tratamento de Dados Pessoais.

CPGDI: Comissão Permanente de Gerenciamento de Dados Institucionais.

DTI: Diretoria de Tecnologia da Informação.

T: Titular

6. INDICADOR DE DESEMPENHO

O programa de gerenciamento de privacidade deve ser monitorado e avaliado periodicamente através de indicador de desempenho de forma a realizar eventuais ajustes necessários. Esse monitoramento tem como objetivo acompanhar a eficácia do processo, identificando tendências, falhas e oportunidades de correções, promovendo sempre a melhoria contínua. A tabela 4 apresenta o indicador de desempenho do processo.

Tabela 4 - Indicador de Desempenho

Indicador	Índice de serviços com dados pessoais inventariados.
Descrição	Índice de serviços com dados pessoais inventariados
Objetivo	Medir o percentual de serviços com dados pessoais inventariados.
Periodicidade	Anual
Fonte	Encarregado de Tratamento de Dados Pessoais
Fórmula	Número de serviços com dados pessoais inventariados / Número de serviços com dados pessoais do IFTO * 100;
Meta	Monitorar a quantidade de serviços com dados pessoais inventariados.

7. REFERÊNCIAS

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

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

BRASIL. **Lei n° 13.709, de 14 de agosto de 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em 24 nov. 2023.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Estratégia Nacional de Segurança Cibernética.** Decreto 10.222, de 5 de Fevereiro de 2020. (BRASIL, 2020).

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Guia de elaboração de programa de governança de privacidade**. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_programa_governanca_privacidade.pdf Acesso em: 21 nov. 2023.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de Segurança para Internet.** Disponível em: https://cartilha.cert.br/fasciculos/ Acesso em: 03 mar. 2022.

NIST SPECIAL PUBLICATION 800-16. **Computer Security-Information Technology Security Training Requirements: A Role-and Performance-Based Model, version 1.0**, 1998. (NIST, 1998).

ANEXO I

PLANO DE AÇÃO

Controle	Id	Função NIST PF	Ação	Previsão
Controle 19 - Inventário e Mapeamento				
19	19.1	Identificar	Documentar os sistemas, serviços e processos que tratam dados pessoais.	Dezembro de 2023
	19.2	Identificar	Mapear os agentes de tratamento (controlador, co-controladores e operadores) responsáveis pelo processamento de dados pessoais.	Dezembro de 2023
	19.3	Identificar	Documentar as fases do tratamento em que o operador atua.	Dezembro de 2023
	19.4	Identificar	Mapear os fluxos ou ações do tratamento de dados pessoais.	Junho de 2024
	19.5	Identificar	Mapear o escopo (abrangência ou área geográfica) dos tratamentos de dados pessoais.	Dezembro de 2023
	19.6	Identificar	Documentar a natureza (fonte) dos dados pessoais tratados.	Agosto de 2024
	19.7	Identificar	Registrar as bases legais que fundamentam as atividades de tratamento de dados pessoais e dados pessoais sensíveis.	Dezembro de 2023
	19.8	Identificar	Inventaria as categorias dos dados pessoais e dados pessoais sensíveis objetos dos tratamentos realizados.	Junho de 2024
	19.9	Identificar	Registrar o tempo de retenção de dados pessoais tratados conforme a finalidade de cada processamento.	Dezembro de 2023
	19.10	Identificar	Inventariar as categorias dos titulares de dados pessoais utilizados no tratamento.	Dezembro de 2024
	19.11	Identificar	Registrar os compartilhamentos de dados pessoais realizados com operadores terceiros e outras instituições conforme Art. 26 e 27 da LGPD, incluindo quais dados pessoais foram divulgados, a quem e com que finalidade.	Dezembro de 2023
	19.12	Identificar	Mapear os ambientes (ex: interno, nuvem, terceiros, etc) em que os dados pessoais objetos dos tratamentos são processados.	Dezembro de 2023

	19.13	Identificar	Registrar as transferências internacionais de dados pessoais realizadas conforme o Capítulo V da LGPD, incluindo quais dados pessoais foram divulgados e a quem.	Dezembro de 2023
	19.14	Identificar	Mapear os contratos estabelecidos/firmados com terceiros operadores responsáveis pelos tratamentos de dados pessoais.	Dezembro de 2023
Controle 20 - Finalidade e hipóteses legais				
20	20.1	Identificar	Identificar as finalidades específicas antes da realização dos tratamentos de dados pessoais.	Junho de 2024
	20.2	Identificar	Identificar as hipóteses de tratamento antes da realização dos processamentos de dados pessoais.	Junho de 2024
	20.3	Identificar	Identificar as bases legais que fundamentam as atividades de tratamento de dados pessoais e dados pessoais sensíveis antes da realização do tratamento.	Junho de 2024
	20.4	Controlar	Realizar o tratamento de dados pessoais apenas para o atendimento de finalidade específica, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.	Junho de 2024
	20.5	Controlar	Tratar dados pessoais sensíveis para executar políticas públicas previstas apenas em leis e regulamentos.	Dezembro de 2024
	20.6	Controlar	Realizar tratamento de dados pessoais sensíveis baseado na hipótese de tutela da saúde, restringe o tratamento exclusivamente a profissionais de saúde, serviços de saúde ou autoridade sanitária.	Dezembro de 2024
	20.7	Controlar	Adotar mecanismos para assegurar que a divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa, em nenhuma hipótese, revele dados pessoais.	Dezembro de 2024
	20.8	Controlar	Realizar estudos em saúde pública, trata os dados pessoais exclusivamente dentro da instituição, mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico, e estritamente para a finalidade de realização de estudos e pesquisas.	Dezembro de 2024
	20.9	Controlar	Manter processo contínuo de gerenciamento das hipóteses legais de tratamento, incluindo o desenvolvimento de capacidades para cumprimento de obrigações decorrentes da definição da hipótese legal de tratamento, tais como: gerenciamento do consentimento, elaboração de Avaliação de Legitimo Interesse, etc.	Dezembro de 2024

	20.10	Controlar	Realizar compartilhamento de dados pessoais, adota medidas que assegurem a compatibilidade do propósito geral da finalidade original informada ao titular.	Junho de 2024
	20.11	Controlar	Coletar cookies identifica, no banner de segundo nível, as hipóteses legais utilizadas, de acordo com cada finalidade/categoria de cookie, utilizando o consentimento como principal hipótese legal, exceção feita aos cookies estritamente necessários, que podem se basear no legítimo interesse ou, se for caso cumprimento de obrigações ou atribuições legais.	Dezembro de 2024
	20.12	Controlar	Coletar cookies permite, no banner de segundo nível, a obtenção do consentimento específico de acordo com as categorias identificadas, observados o disposto na LGPD.	Dezembro de 2024
	20.13	Controlar	Manter o fornecimento do serviço quando os titulares de dados pessoais se recusam a fornecer o consentimento para cookies não necessários.	Dezembro de 2024
	20.14	Controlar	Realizar o tratamento de dados de crianças e adolescentes do no seu melhor interesse com base em hipótese legal prevista pela LGPD e, no que couber, conforme preconizado pelo art. 14 da LGPD.	Junho de 2024
Controle 21: Governança				
21	21.1	Governar	Adotar medidas para adequar seus processos e atividades relacionadas ao tratamento de dados pessoais às legislações/normativos de privacidade e proteção de dados vigentes.	Dezembro de 2024
	21.2	Governar	Elaborar e divulgar o seu Programa Institucional de Privacidade de Dados, conforme estabelecido no art.50 da LGPD.	Dezembro de 2023
	21.3	Governar	Estabelecer e comunicar a claramente as funções e responsabilidades dos colaboradores envolvidos nos tratamentos de dados pessoais.	Dezembro de 2023
	21.4	Governar	Disponibilizar para o encarregado os recursos necessários para implementação da LGPD e acesso direto à alta administração.	Junho de 2024
	21.5	Governar	Determinar as responsabilidades e respectivos papéis para o tratamento de dados pessoais com o(s) controlador(es) conjunto(s) envolvido(s).	Dezembro de 2024
	21.6	Governar	Divulgar a seus colaboradores internos e externos as políticas e procedimentos operacionais relacionados à proteção de dados pessoais.	Junho de 2024
	21.7	Governar	Compreender os requisitos legais, regulatórios e contratuais relativos à privacidade e direciona-los por meio regras de boas práticas e de governança publicadas pela instituição.	Dezembro de 2024

	21.8	Governar	Definir tolerância ao risco organizacional no âmbito das operações de tratamento de dados pessoais e informar as partes interessadas.	Dezembro de 2024
	21.9	Governar	Definir indicadores que serão utilizados para medir os resultados e desempenho do órgão na implementação do Programa Institucional de Privacidade de Dados.	Dezembro de 2024
	21.10	Governar	Instituir uma equipe que realiza o monitoramento das vulnerabilidades técnicas dos serviços que tratam dados pessoais	Dezembro de 2024
Controle 22: Políticas, processos e procedimentos				
22	22.1	Governar	Revisou e adequou a Política de Segurança da Informação ou instrumento similar à LGPD.	Junho de 2023
	22.2	Governar	Elaborar política diretrizes de proteção de dados pessoais.	Dezembro de 2024
	22.3	Governar	Identificar, estabelecer, avaliar e gerenciar políticas, processos e procedimentos de gerenciamento de risco de privacidade do tratamento de dados pessoais e acordar com as partes interessadas e comunicar o seu progresso.	Dezembro de 2023
	22.4	Governar	Adequar os instrumentos convocatórios (editais licitatórios) à LGPD.	Junho de 2024
	22.5	Governar	Definri e estabelecer um processo para monitorar as leis e políticas de privacidade com o objetivo de identificar alterações que afetem o programa de proteção de dados pessoais.	Dezembro de 2024
	22.6	Controlar	Estabelecer um processo formal para a concessão de direitos de acesso privilegiado para o processamento de dados pessoais.	Dezembro de 2024
	22.7	Controlar	Estabelecer procedimento ou metodologia para assegurar que os princípios da LGPD estão sendo respeitados desde a fase de concepção do produto ou do serviço até a sua execução (Privacy by Design).	Dezembro de 2024
	22.8	Controlar	Implementar processos para que o tratamento dos dados pessoais seja preciso, completo, atualizado, adequado e relevante para a finalidade de uso.	Dezembro de 2024
	22.9	Controlar	Estabelecer políticas, procedimentos e adota mecanismos documentados para o descarte de dados pessoais.	Dezembro de 2024
	22.10	Controlar	Adequar o Plano de Resposta a Incidentes (ou documento similar) à LGPD de forma a tratar violações relativas à privacidade dos titulares de dados pessoais.	Junho de 2024
	22.11	Controlar	Estabelecer procedimentos para comunicar à Autoridade Nacional de	Junho de 2024

			Proteção de Dados e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares	
	22.12	Controlar	Revisar periodicamente as políticas, processos, planos e procedimentos de proteção de dados pessoais	Dezembro de 2024
Controle 23: Conscientização e treinamento				
23	23.1	Governar	Implementa e mantêm uma estratégia abrangente de treinamento e conscientização a fim de garantir que a força de trabalho compreenda sobre suas responsabilidades e procedimentos de proteção de dados pessoais.	Dezembro de 2024
	23.2	Governar	Contemplar o treinamento adequado sobre a temática de privacidade e de proteção de dados pessoais no plano de desenvolvimento de pessoas.	Junho de 2024
	23.3	Governar	Definir ações de treinamento e conscientização realizadas pela instituição que visem a manter os colaboradores atualizados sobre os desenvolvimentos no ambiente regulatório, contratual e tecnológico que possam afetar a conformidade de privacidade da organização.	Dezembro de 2024
	23.4	Governar	Executar regularmente (por exemplo, anual) ou conforme necessário (por exemplo, após um incidente) treinamento básico e direcionado de proteção de dados pessoais conforme as funções das pessoas envolvidas com o tratamento.	Dezembro de 2024
Controle 24: Minimização de dados				
24	24.1	Controlar	Avaliar e classificar os dados pessoais a serem coletados em obrigatórios e opcionais a fim de priorizar somente a coleta dos dados obrigatórios para a prestação do serviço.	Junho de 2024
	24.2	Controlar	Restringir ao máximo a coleta de dados de forma que seja suficiente para atender a finalidade específica do tratamento.	Dezembro de 2024
	24.3	Controlar	Realizar o tratamento de dados pessoais, aplica o princípio da minimização de dados para restringir a quantidades de dados pessoais ao estritamente necessário para atendimento da finalidade específica.	Dezembro de 2024
	24.4	Controlar	Adotar medidas para assegurar que as configurações de privacidade sejam aplicadas por padrão (Privacy by Default) nos serviços fornecidos.	Dezembro de 2024
	24.5	Controlar	Adotar o princípio 'need-to-how', em que deve ser dado acesso apenas aos dados pessoais necessários para o desempenho das funções dos colaboradores.	Dezembro de 2024
	24.6	Controlar	Adotar como padrão, sempre que possível, interações e transações que	Dezembro de 2024

			não envolvam a identificação dos titulares.	
	24.7	Controlar	Adotar mecanismos para limitar a vinculação dos dados pessoais coletados.	Dezembro de 2024
	24.8	Controlar	Configurar em sistemas de informação para que as referências de atributos são substituídas por valores de atributos. Por exemplo, para o atributo "aniversário", um valor de atributo poderia ser "1/12/1980" e uma referência de atributo seria "nascido em dezembro".	Dezembro de 2024
	24.9	Controlar	Configurar sistemas de informação para que os dados pessoais utilizados em ambiente de TDH (teste, desenvolvimento e homologação) passam por um processo de anonimização.	Dezembro de 2024
	24.10	Controlar	Realizar a revisão periódica dos dados pessoais tratados para que continuem a ser o mínimo necessários para cumprir com a finalidade.	Dezembro de 2024
	24.11	Controlar	Determinar e desidentificar os dados pessoais que necessitam ser anonimizados de acordo com o tratamento e exigências estabelecidas por leis aplicáveis.	Dezembro de 2024
	24.12	Controlar	Configurar sistemas de informação para que ao fornecer a base de informações para órgãos de pesquisa ou para realização de estudos em saúde pública, os dados pessoais são, sempre que possível, anonimizados ou pseudoanonimizados.	Dezembro de 2024
	24.13	Controlar	Configurar sistemas de informação para que ao coletar cookies disponibiliza botão de fácil visualização, no banner de primeiro e de segundo nível, que permita rejeitar todos os cookies não necessários.	Dezembro de 2024
	24.14	Controlar	Configurar sistemas de informação para que ao coletar cookies desativa, no banner de primeiro nível, cookies baseados no consentimento por padrão (opt-in).	Dezembro de 2024
	24.15	Controlar	Configurar sistemas de informação para que ao coletar cookies classifica os cookies em categorias no banner de segundo nível	Dezembro de 2024
Controle 25: Gestão do Tratamento				
25	25.1	Controlar	Configurar os sistemas para registrar a data em que os dados pessoais são coletados, criados, atualizados, excluídos ou arquivados.	Dezembro de 2024
	25.2	Controlar	Limitar a quantidade de processamento sobre os dados pessoais sob sua custódia.	Dezembro de 2024
	25.3	Controlar	Definir e documenta os objetivos da minimização do tratamento sobre os dados pessoais sob sua custódia.	Dezembro de 2024

	25.4	Controlar	Configurar sistemas de informação para que os dados são mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral?	Dezembro de 2024
	25.6	Controlar	Utiliza técnicas ou métodos apropriados para garantir exclusão ou destruição segura de dados pessoais (incluindo originais, cópias e registros arquivados), de modo a impedir sua recuperação.	Dezembro de 2024
	25.7	Controlar	Avaliar se os dados pessoais são retidos (armazenados) durante o tempo estritamente necessário para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas.	Dezembro de 2024
	25.8	Controlar	Implementar no serviço a detecção da expiração do período de retenção e aviso automático de que deve ser avaliada a possibilidade de exclusão dos dados pessoais após o cumprimento das finalidades.	Dezembro de 2024
	25.9	Controlar	Bloquear e adotar medidas de proteção para isentar de processamento adicional os dados pessoais quando os propósitos informados ao titular são atingidos, mas a retenção for exigida pelas leis aplicáveis.	Dezembro de 2024
Controle 26: acesso e qualidade				
26	26.1	Controlar	Estabelecer um canal de comunicação ativo, seguro e autenticado com um ponto de contato para receber e responder a reclamações e requisições do titular sobre o tratamento de dados pessoais?	Junho de 2024
	26.2	Controlar	Adotar meios para verificar a validade e exatidão das solicitações de correção realizadas por parte do titular de dados pessoais.	Dezembro de 2024
	26.3	Controlar	Fornece meios para que o titulares de dados pessoais possam solicitar as correções dos dados pessoais ou contestar a exatidão e integridade dos dados pessoais com direito a confirmação de recebimento da solicitação.	Dezembro de 2024
	26.4	Controlar	Fornecer, na medida do possível, as respostas ao titular de dados pessoais de forma equivalente àquela em que a solicitação foi realizada.	Dezembro de 2024
	26.5	Controlar	Adotar mecanismos de rastreamento para garantir que todas as petições e reclamações recebidas dos titulares de dados pessoais sejam analisadas e tratadas adequadamente em tempo hábil.	Junho de 2024

	26.6	Controlar	Utilizar padrões técnicos, principalmente os definidos pela ANPD, que facilitem o controle pelos titulares dos seus dados pessoais.	Dezembro de 2024
	26.7	Controlar	Implementar meios práticos para permitir que os titulares gerenciem os seus dados pessoais, de forma simples, rápida e eficiente, e que não acarrete atrasos indevidos ou custo ao titular.	Dezembro de 2024
	26.8	Controlar	Confirmar na medida do possível, a exatidão, relevância e integridade dos dados pessoais na coleta.	Dezembro de 2024
	26.9	Controlar	Implementar medidas que visam a garantir e maximizar a exatidão, qualidade e completude dos dados pessoais coletados.	Dezembro de 2024
	26.10	Controlar	Revisar periodicamente e corrigir conforme necessário os dados pessoais imprecisos ou desatualizados.	Dezembro de 2024
	26.11	Comunicar	Fornecer informações ao titular de dados pessoais sobre o andamento de suas solicitações.	Dezembro de 2024
	26.12	Comunicar	Comunicar qualquer alteração, correção ou remoção dos dados pessoais para operadores e terceiros com quem os dados pessoais foram compartilhados	Dezembro de 2024
Controle 27: Compartilhamento, transferência e divulgação.				
27	27.1	Identificar	Identificar os compartilhamentos de dados pessoais realizados com operadores terceiros e outras instituições conforme Art. 26 e 27 da LGPD, incluindo quais dados pessoais foram divulgados, a quem, a que horas e com que finalidade.	Dezembro de 2024
	27.2	Identificar	Identificar as transferências internacionais de dados pessoais realizadas conforme o Capítulo V da LGPD, incluindo quais dados pessoais foram divulgados, a quem, a que horas e com que finalidade	Dezembro de 2024
	27.3	Controlar	Ao compartilhar dados pessoais, adotar um processo de formalização e registro, identificando objeto e finalidade, base legal e duração do tratamento.	Junho de 2024
	27.4	Controlar	Solicitar descrição formal das medidas de proteção de dados pessoais adotadas pelas entidades com quem compartilha dados pessoais.	Junho de 2024
	27.5	Controlar	Observar o disposto pelo art. 33-36 da LGPD para a realização de transferência internacional de dados pessoais	Dezembro de 2024
Controle 28: Supervisão em Terceiros				
28	28.1	Controlar	Estabelecer as funções e responsabilidades do operador envolvido no tratamento de dados pessoais, principalmente a notificação em caso de violação de dados pessoais.	Dezembro de 2023

	28.2	Controlar	Estabelecer acordos de confidencialidade, termos de responsabilidade ou termos de sigilo com operadores de dados pessoais controlados pelos órgãos.	Dezembro de 2023
	28.3	Controlar	Estabelecer no contrato que o operador não processe os dados pessoais para finalidades que divergem da finalidade principal informada pelo controlador.	Dezembro de 2023
	28.4	Controlar	Determinar por contrato o assunto e o prazo do serviço a ser prestado, a extensão, a forma e a finalidade do tratamento de dados pessoais pelo operador, bem como os tipos de dados pessoais processados.	Dezembro de 2024
	28.5	Controlar	Documentar no contrato de nível de serviço os requisitos de proteção de dados pessoais que os operadores de dados pessoais devem atender.	Dezembro de 2024
	28.6	Controlar	Adotar meios para garantir que os sistemas do operador de dados pessoais tenham mecanismos de proteção de dados implementados.	Dezembro de 2024
	28.7	Controlar	Instruir ao operador que implemente meios práticos para permitir que os titulares exerçam seu direito de gerenciamento dos dados pessoais.	Dezembro de 2024
	28.8	Controlar	Exigir do operador o cumprimento de todas as cláusulas estipuladas em contrato sobre divulgação de dados pessoais, a menos que proibido por lei.	Dezembro de 2024
	28.9	Controlar	Exigir que o operador o informe sobre assuntos envolvendo o tratamento de dados pessoais para que o controlador esteja em conformidade com suas obrigações, principalmente em casos de solicitações juridicamente vinculativas para divulgação de dados pessoais, violação de dados pessoais, sobre alterações relevantes ao serviço.	Dezembro de 2024
	28.10	Controlar	Especificar as condições sob as quais o operador deve devolver ou descartar com segurança os dados pessoais após a conclusão do serviço, rescisão de qualquer contrato ou de outra forma mediante solicitação do controlador.	Dezembro de 2024
	28.11	Controlar	Especificar no contrato entre controlador e operador sobre o uso de subcontratados para processar dados pessoais.	Dezembro de 2024
	28.12	Controlar	Monitorar e inspecionar a implementação dos requisitos estabelecidos nas cláusulas contratuais pelos operadores.	Dezembro de 2024
	28.13	Controlar	Realizar a revisão das cláusulas contratuais em vigência com os operadores terceiros para adequá-los à LGPD	Dezembro de 2024
Controle 29: abertura, transparência e notificação				
29	29.1	Controlar	Adotar meios para apresentar as informações de tratamento de dados	Dezembro de 2024

			pessoais de forma clara para que possam ser compreendidas por uma pessoa que não esteja familiarizada com as tecnologias da informação, internet ou jargões jurídicos.	
	29.2	Controlar	Adotar meios para disponibilizar a política de privacidade em local de fácil acesso, antes ou no momento do tratamento de dados pessoais, sem a necessidade de o titular ter que solicitá-lo especificamente.	Dezembro de 2023
	29.3	Controlar	Adotar algum mecanismo, sempre que possível, para comprovar que o titular de dados pessoais obteve acesso à política de privacidade fornecidas.	Dezembro de 2024
	29.4	Controlar	Revisar a política de privacidade, cookies e outras aplicáveis ao tratamento de dados pessoais, antes ou assim que possível, para refletir mudanças realizadas no tratamento.	Dezembro de 2024
	29.5	Comunicar	Destacar na Política de Privacidade informações sobre os dados pessoais que a organização coleta e a(s) finalidade(s) do tratamento para a qual a coleta é realizada, hipóteses e bases legais.	Dezembro de 2024
	29.6	Comunicar	Publicar a identidade e as informações de contato do encarregado, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.	Dezembro de 2023
	29.7	Comunicar	Fornecer informações aos titulares sobre como é realizado o tratamento de dados pessoais, tais como o período de retenção dos dados pessoais coletados, entre outras ações de tratamento	Dezembro de 2024
	29.8	Comunicar	Os titulares de dados são informados quando há alterações na forma de tratamento dos dados pessoais.	Dezembro de 2024
	29.9	Comunicar	Fornecer orientações ao titular sobre a forma e meios utilizados de gerenciamento aos dados pessoais.	Dezembro de 2024
	29.10	Comunicar	Informar se a organização compartilha dados pessoais com entidades externas, os dados pessoais compartilhados e a finalidade para tal compartilhamento.	Dezembro de 2024
	29.11	Comunicar	Fornecer informações sobre a proteção e descarte seguro dos dados pessoais coletados.	Dezembro de 2024
	29.12	Comunicar	Fornecer quando solicitado por instituição competente, informações relativas a violações de privacidade dos titulares, juntamente com quaisquer ações associadas que o solicitante possa tomar para mitigar os riscos adicionais decorrentes da violação	Dezembro de 2024
Controle 30: Avaliação de impacto, monitoramento e auditoria				
30	30.1	Governar	Observar o conteúdo mínimo a ser inserido no Relatório de Impacto à Proteção de Dados Pessoais - RIPD conforme o disposto no Art. 38, parágrafo único da LGPD.	Dezembro de 2023

	30.2	Governar	Estabelecer processo para avaliar o impacto na privacidade ao fornecer serviços que tratam dados pessoais.	Dezembro de 2024
	30.3	Governar	Avaliar os riscos dos processos de tratamento de dados pessoais que foram identificados.	Dezembro de 2024
	30.4	Governar	Documentar os riscos de privacidade oriundos da avaliação de impacto à Proteção de Dados Pessoais.	Dezembro de 2024
	30.5	Governar	Documentar as medidas de proteção de dados pessoais adotadas para mitigação do impacto à Proteção de Dados Pessoais.	Dezembro de 2023
	30.6	Governar	Realizar e documentar os resultados de uma avaliação de impacto à Proteção de Dados Pessoais.	Dezembro de 2024
	30.7	Governar	Desenvolver, divulgar (no que couber) e atualizar relatórios (por exemplo, relatórios sobre violações, investigações, auditorias), a fim de demonstrar responsabilidade e conformidade com leis e regulamentos de proteção de dados pessoais.	Dezembro de 2024
	30.8	Controlar	Monitorar e auditar regularmente as operações de tratamento de dados pessoais, especialmente aquelas envolvendo dados pessoais sensíveis, para garantir que estejam em conformidade com as leis, regulamentos e termos contratuais aplicáveis.	Dezembro de 2024
	30.9	Controlar	Monitorar e auditar os controles de proteção de dados pessoais periodicamente para garantir que as operações que envolvam dados pessoais estejam em conformidade com normas e regulamentos internos e externos, quando aplicável, a organização.	Dezembro de 2024
	30.10	Controlar	Implementa medidas apropriadas para monitorar e auditar periodicamente os controles de privacidade e a eficácia da política de privacidade interna (política de proteção de dados pessoais) da instituição.	Dezembro de 2024
	30.11	Controlar	Assegurar que as auditorias sejam conduzidas por partes qualificadas e independentes (internas ou externas à organização).	Dezembro de 2024
	30.12	Controlar	Produzir um relatório anual detalhando as ações tomadas para conformidade e um resumo das ações pendentes.	Dezembro de 2024
Controle 31: Segurança aplicada a privacidade				
31	31.1	Proteger	Adotar medidas de segurança, técnicas e administrativas, testadas e avaliadas, aptas a proteger dados pessoais de acordo com os resultados de uma avaliação de riscos ou impacto de proteção de dados pessoais.	Dezembro de 2023

31.2	Proteger	Submeter os controles de segurança e proteção de dados a revisão e reavaliação periódicas em um processo contínuo de gerenciamento de riscos de segurança.	Dezembro de 2024
31.3	Proteger	Implementar o processo para registro, cancelamento e provisionamento de usuários em sistemas que realizam tratamento de dados pessoais.	Junho de 2024
31.4	Proteger	Considerar o princípio do privilégio mínimo na concessão de direitos de acesso para o processamento de dados pessoais.	Junho de 2024
31.5	Proteger	Estabelecer meios fortes de autenticação são providos para o processamento dos dados pessoais, em especial os dados sensíveis (dados de saúde e demais dados previstos pelo art.5º, II da LGPD).	Dezembro de 2024
31.6	Proteger	Gerenciar o acesso físico aos dados e dispositivos.	Dezembro de 2024
31.7	Proteger	Realizar o compartilhamento ou transferência de dados pessoais por meio de um canal criptografado e de cifra recomendada pelos sítios especializados de segurança.	Dezembro de 2023
31.8	Proteger	Implementar rotinas em sistemas de informação para que os dados pessoais armazenados/retidos possuem controles de integridade permitindo identificar se os dados foram alterados sem permissão.	Dezembro de 2024
31.9	Proteger	Implantar soluções para que o IFTO adote mecanismos para restauração de dados pessoais.	Dezembro de 2024
31.10	Proteger	Restringir e controlar a impressão de documentos que contenha dados pessoais encaminhados para as impressoras corporativas.	Dezembro de 2023
31.11	Proteger	Implantar soluções que possibilitem descartar materiais impressos de forma segura.	Dezembro de 2024
31.12	Proteger	Considerar as medidas de mitigação de riscos resultantes do RIPD no processo de desenvolvimento de sistemas.	Dezembro de 2024
31.13	Proteger	Realizar e registrar através de ferramentas aprovadas e controladas a manutenção e reparação dos ativos organizacionais.	Dezembro de 2024
31.14	Proteger	Aprovar, registrar e executar a manutenção remota dos ativos organizacionais de forma a impedir o acesso não autorizado.	Dezembro de 2024
31.15	Proteger	Realizar registros de eventos (logs), considerando o princípio de minimização de dados, grava o acesso ao dado pessoal, incluindo por quem, quando, qual titular de dados pessoais foi acessado e quais mudanças (se houver alguma) foram feitas (adições,	Dezembro de 2024

			modificações ou exclusões), como um resultado do evento.	
	31.16	Proteger	Monitorar proativamente a ocorrência de eventos que podem ser associados à violação de dados pessoais.	Dezembro de 2024
	31.17	Proteger	Registrar incidentes de segurança da informação que envolvem violação de dados pessoais.	Junho de 2024
	31.18	Proteger	Comunica à Autoridade Nacional de Proteção de Dados sobre a ocorrência de incidente de segurança e proteção de dados pessoais.	Junho de 2024

ANEXO II

SISTEMAS, SERVIÇOS E PROCESSOS QUE TRATAM DADOS PESSOAIS

Sistema/Serviço	Área	Processo Organizacional	Criticidade
E-mail	- DTI	- Todos	Alta
Impressão e digitalização de documentos	- PROAD	- Todos	Alta
Internet	- DTI	- Todos	Alta
Moodle	- PROEN - PROEX	- Ensino - Extensão	Alta
Portal Institucional	Diretoria de Comunicação	- Comunicação	Alta
Rede Wi-Fi	Todas	- Todos	Alta
Sistema de submissão de artigos científicos	- PROPI	- Pesquisa	Alta
Sistema do processo seletivo	- PROAE	- Seletivo	Alta
Sistema Unificado de Administração Pública (SUAP)	Administração	- Almoxarifado. - Boletins de Serviços. - Compras. - Contratos. - Frota. - Materiais. - Patrimônio. - Reservas de Salas. - Telefones.	Alta
	Central de Serviços	- Abrir chamado. - Base de Conhecimentos. - Cadastros. - Chamados. - Dashboard. - Meus Chamados. - Relatórios.	Alta
	Comunicação Social	- Enquetes. - Eventos. - Relatórios.	Alta
	Des. Institucional	- Gestão. - Planejamento. - Planejamento Estratégico. - Planejamento Institucional.	Alta

	Documentos e Processos	- Documentos Eletrônicos. - Processos Eletrônicos. - Processos Físicos.	Alta
	Ensino	- Alunos e Professores. - Cadastros Gerais. - Cursos, Matrizes e Componentes. - Estatísticas. - ETEP. - Processos Seletivos. - Relatórios. - Atas Eletrônicas.	Alta
	Extensão	- Estágios e Afins. - Projetos. - Demandas Externas.	Alta
	Gestão de Pessoas	- Servidores. - Setores. - Campi. - Administração de Pessoal. - Desenvolvimento de Pessoal. - Atenção a Saúde do Servidor. - Licença Capacitação. - Programa de Gestão. - SIAPE. - Relatórios. - Cadastros.	Alta
	Pesquisa	- Editais. - Projetos. - Declarações. - Editora. - Laboratórios.	Alta
	Segurança Institucional	- Solicitações de Entrada.	Alta
	Tecnologia da Informação	- Acessibilidade. - Desenvolvimento. - Segurança. - Serviços. - Usuários.	Alta
SEI	Gestão	- Gestão de Processos. - Gestão de Documentos.	Alta
SOPHIA	Gestão	- Gestão de Bibliotecas.	Alta
Sistemas Internos	Gestão	- Gestão de Concursos. - Gestão de Eventos. - Gestão de Creche. - Gestão de Restaurante.	Alta

Fonte: Diretoria de Tecnologia da Informação

Documento assinado eletronicamente por **Fabiana Ferreira Cardoso**, **Gestora de Segurança da Informação**, em 21/12/2023, às 17:24, 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 **Ustana Ferraz Soares**, **Encarregada pelo Tratamento de Dados Pessoais**, em 21/12/2023, às 17:29, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Kleyton Matos Moreira**, **Diretor**, em 22/12/2023, às 14:35, 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 **2224683** e o código CRC **15E225B8**.

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

Referência: Processo nº 23235.021734/2023-79 SEI nº 2224683