INSTITUTO FEDERAL
Pernambuco

PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

Versão 1.1
Recife, novembro de 2024

Comissão Permanente de Gestão de Dados Pessoais do IFPE

A Portaria IFPE nº 804, de 4 de junho de 2024 (que atualizou a Portaria IFPE nº 1.327, de 11 de novembro de 2022), designou os responsáveis pelas unidades a seguir para constituírem a Comissão Permanente de Gestão de Dados Pessoais do IFPE:

UNIDADE	RESPONSÁVEL	ATUAÇÃO
1. Coordenação de Controladoria (Encarregado/a de Dados Pessoais do IFPE)	Titular da Controladoria ou seu/sua substituto/a oficial	Presidente
2. Ouvidoria Geral do IFPE	Titular da Unidade Setorial de Ouvidoria ou Ouvidor/a Adjunto/a	Membro
3. Serviço de Informação ao Cidadão	Gestor/a do Serviço de Informação ao Cidadão ou seu/sua substituto/a oficial	Membro
4. Diretoria de Tecnologia da Informação (DTI)	Titular da DTI ou seu/sua substituto/a oficial	Membro
5. Diretoria de Gestão de Pessoas (DGPE)	Titular da DGPE ou seu/sua substituto/a oficial	Membro
6. Pró-Reitoria de Integração e Desenvolvimento Institucional (Prodin)	Titular da Prodin ou seu/sua substituto/a oficial	Membro
7. Pró-Reitoria de Ensino (Proden)	Titular da Proden ou seu/sua substituto/a oficial	Membro
8. Pró-Reitoria de Pesquisa, Pós-Graduação e Inovação (Propesq)	Titular da Propesq ou seu/sua substituto/a oficial	Membro
9. Pró-Reitoria de Extensão (Proext)	Titular da Proext ou seu/sua substituto/a oficial	Membro
10. Pró-Reitoria de Administração (Proad)	Titular da Proad ou seu/sua substituto/a oficial	Membro
11. Diretoria de Assistência ao Estudante (DAE)	Titular da DAE ou seu/sua substituto/a oficial	Membro
12. Diretoria-Geral – *Campus* Cabo de Santo Agostinho	Diretor/a-Geral do *Campus* Cabo de Santo Agostinho ou seu/sua substituto/a oficial	Membro
13. Diretoria-Geral – *Campus* Palmares	Diretor/a-Geral do *Campus* Palmares ou seu/sua substituto/a oficial	Membro

Histórico de Alterações

Versão	Data	Autor/a
1.0	**02/8/2024**	Encarregada de Dados Pessoais do IFPE - Maria Dayana Lopes de Oliveira
1.1	**21/11/2024**	Encarregada de Dados Pessoais do IFPE - Maria Dayana Lopes de Oliveira

SUMÁRIO

INTRODUÇÃO

A Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), em sua Seção II, "Das Boas Práticas e da Governança", dispõe:

> Art. 50 Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Ainda no art. 50 § 2º, a lei apresenta as características mínimas de um Programa de Governança em Privacidade (PGP), conforme apresentado a seguir:

- 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;
- ser aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
- ser adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
- estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
- ter o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
- estar integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
- contar com planos de resposta a incidentes e remediação; e
- ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

Em conformidade com a LGPD, a Política Geral de Proteção de Dados Pessoais do IFPE, aprovada por meio da Resolução Consup/IFPE nº 124, de 30 de março de 2022, dispõe, em seu art. 15:

> Art. 15. As medidas a serem adotadas para a elaboração do Programa de Governança em Privacidade de Dados Pessoais no IFPE correspondem a liderança, estratégias, habilidades, pessoas, processos, ferramentas e ações, por meio, no mínimo, do mapeamento, do tratamento, da categorização, da definição dos impactos, da formalização de medidas e da conscientização.
>
> Parágrafo único. As medidas de proteção devem ser incrementadas, preferencialmente, com o auxílio de ferramentas e instrumentos de

> tecnologia da informação, a serem especificados em regulamento, especialmente no que concerne à anonimização de dados pessoais. (IFPE, 2022)

O presente documento apresenta o Programa de Governança em Privacidade (PGP) a ser implementado pelo IFPE, em consonância com o *Guia de Elaboração do Programa de Governança em Privacidade* **(versão 2.2**, **de 19/3/2024),** elaborado pela Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos (MGI), especialmente recomendado e dirigido aos órgãos e às entidades da administração pública federal, tendo como referência fundamental o *Guia do Framework de Privacidade e Segurança da Informação*, elaborado e publicado pela SGD.

Conforme o *Guia de Elaboração do Programa de Governança em Privacidade*, diferentemente de um projeto, que tem início, meio e fim, um programa define uma metodologia abrangente que influenciará permanentemente os processos de tomada de decisão baseado em riscos e melhorias contínuas na maturidade. Apesar disso, pode-se criar projetos para se alcançarem os objetivos do programa.

A estrutura do PGP, em conformidade com o *Guia*, é inspirada no ciclo PDCA (Plan, Do, Check e Act), bem como nas normas ABNT NBR ISO/IEC 27001:2013, ABNT NBR ISO/IEC 27701:2019 e ABNT NBR ISO/IEC 27005:2011.

Desse modo, o programa está estruturado nas seguintes etapas:

ETAPA 1 - Iniciação e Planejamento;
ETAPA 2 - Construção e Execução;
ETAPA 3 – Monitoramento.

O PGP do IFPE tem como finalidade direcionar a implementação da proteção de dados pessoais na instituição, em consonância com os aspectos elencados no art. 50 da LGPD, listados anteriormente. Ressalta-se que este documento será atualizado sempre que necessário para manter alinhamento com as diretrizes determinadas pelas autoridades em privacidade e segurança da informação.

1. ETAPA 1 - Iniciação e Planejamento

De acordo com o *Guia de Elaboração de Programa de Governança em Privacidade,* da SGD/MGI, a etapa de Iniciação e Planejamento busca compreender quais são as primeiras informações e os dados importantes que devem ser conhecidos. Essa etapa compreende os seguintes marcos:

1. Nomeação do/a Encarregado/a;
2. Alinhamento de Expectativas com a Alta Administração;
3. Análise da Maturidade - Diagnóstico do atual estágio de adequação à LGPD;
4. Análise e Adoção de Medidas de Segurança, Diretrizes e Cultura Interna;
5. Instituição de Estrutura Organizacional para a Governança e Gestão da Proteção de Dados Pessoais;
6. Inventário de Dados Pessoais; e
7. Levantamento dos Contratos Relacionados a Dados Pessoais.

1.1. Nomeação do/a Encarregado/a

De acordo com o inciso VIII do art. 5° da LGPD, o/a encarregado/a é a pessoa indicada pelo/a controlador/a e pelo/a operador/a para atuar como canal de comunicação entre o/a controlador/a, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Conforme o § 2º do art. 9º da Política Geral de Proteção de Dados Pessoais do IFPE, "O/A encarregado/a de dados pessoais do IFPE é o/a diretor/a da Controladoria, que atua como canal de comunicação entre o controlador de dados pessoais, os titulares dos dados e a ANPD".

Assim sendo, a Portaria REI/IFPE nº 233, de 21 de fevereiro de 2024, designou servidores para responderem como titular e substituto no tratamento de Dados Pessoais, no âmbito do IFPE: a servidora Maria Dayana Lopes de Oliveira, ocupante do cargo efetivo de Auditora, coordenadora da Controladoria do IFPE, para exercício do encargo de Encarregada pelo Tratamento de Dados Pessoais, e o servidor Marlon Oliveira Martins Leandro, ocupante do cargo efetivo de Professor de Ensino Básico, Técnico e Tecnológico, para responder como substituto da encarregada pelo tratamento de dados pessoais.

Conforme o art. 11 da Política Geral de Proteção de Dados Pessoais do IFPE, o/a encarregado/a tem como atribuições:

> I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
> II - acompanhar sistematicamente as ações de tratamento de dados pessoais, identificando o fim da ação e o possível fim da custódia ou ação de renovação dos prazos;
> III - aprovar, com a Comissão Permanente de Gestão de Dados Pessoais (CPGDP), o Inventário de Dados Pessoais, o Relatório de Impacto à Proteção de Dados Pessoais, o Mapeamento do Processo de Tratamento de Dados Pessoais e o Relatório de Gestão do Risco de Vazamento de Dados;
> IV - emitir normas complementares, regulamentos, políticas internas, resoluções e portarias sobre a LGPD, que não podem transpor, inovar ou modificar o texto da norma que complementam;
> V - executar as demais atribuições determinadas pelo controlador de dados pessoais ou estabelecidas em normas complementares;
> VI - manter o controle das ações de tratamento de dados, dos seus operadores e dos titulares de dados;
> VII - notificar o(s)/a(s) operador(es)/a(as) do dado pessoal quando alcançado o período de custódia, acompanhando a eliminação dos dados, conforme regulamento próprio;
> VIII - notificar o(s)/a(s) operador(es)/ a(as) do dado pessoal quando do pedido voluntário de revogação do consentimento, acompanhando a eliminação do dado e a notificação ao solicitante, conforme regulamento próprio;
> IX - orientar os servidores da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

> X - receber as solicitações de informações acerca dos dados pessoais armazenados, devendo responder sobre as ações de tratamento de dados somente ao solicitante titular dos dados;
> XI - receber as comunicações da ANPD e adotar providências; e
> XII - supervisionar as atividades necessárias à implementação, à execução, à manutenção, ao desenvolvimento e ao aperfeiçoamento da LGPD no âmbito do IFPE.

Ademais, considerando as boas práticas, é importante que o IFPE assegure ao/à encarregado/a recursos adequados para realização de suas atividades, que podem incluir:

- uma estrutura organizacional suficiente (instalações, equipamentos e pessoal) para governança e gestão da proteção de dados pessoais;
- autonomia, independência e tempo suficiente para determinar a aplicação de recursos e ações necessárias para o cumprimento das funções relativas ao tratamento de dados pessoais realizados pelo órgão;
- acesso necessário, bem como o pronto apoio das unidades administrativas (recursos humanos, jurídico, TI, segurança etc.) no atendimento das solicitações de informações em relação às operações de tratamento de dados pessoais;
- amplo acesso à estrutura organizacional para investigar proativamente os níveis de conformidade e instruir os responsáveis pelos riscos a corrigir as lacunas encontradas;
- contínuo aperfeiçoamento por meio de treinamentos e capacitações realizadas nas áreas de segurança da informação e proteção de dados pessoais.

Os dados da atual encarregada são públicos e estão acessíveis no site institucional do IFPE.

1.2 Alinhamento de Expectativas com a Alta Administração

A participação da alta administração, representando o papel do/a controlador/a, é de suma importância para a efetividade das ações relativas ao cumprimento das obrigações estipuladas pela LGPD. É válido ressaltar que o apoio da alta administração é essencial para o sucesso do trabalho executado pelo/a encarregado/a, incluindo seu envolvimento nas decisões relacionadas a tratamento de dados pessoais na instituição e fornecendo uma estrutura organizacional suficiente (instalações, equipamentos e pessoal) para governança e gestão da proteção de dados pessoais.

Conforme o art. 14 da Resolução nº 57 de 30 de novembro de 2018, do Conselho Superior, o Comitê de Governança, Riscos e Controles (CGRC) do IFPE é responsável por assessorar permanentemente os dirigentes em questões relativas à Gestão de Governança, Riscos e Controles.

Compete ao CGRC do IFPE, entre outras atribuições, incentivar a adoção de boas práticas de governança, bem como garantir a aderência às regulamentações, leis, códigos, normas e padrões, com vistas à condução das políticas e à prestação de serviços de interesse público.

Assim sendo, em reunião do CGRC ocorrida em 02/08/2024, foram apresentadas pela encarregada pelo tratamento de dados pessoais as ações previstas para adequação do IFPE aos ditames da LGPD, bem como a estrutura deste Programa de Governança em Privacidade e o status de realização de cada uma das etapas e marcos do programa, conforme o modelo recomendado pela SGD/MGI.

Com a aprovação do PGP na reunião do CGRC, conforme ata da reunião, considera-se cumprida a etapa de alinhamento de expectativas com a alta administração. Ademais, levando-se em conta que o PGP do IFPE é um documento que deve sempre ser revisado e atualizado, serão realizados novos alinhamentos, sempre que necessário.

1.3 Análise da Maturidade - Diagnóstico do atual estágio de adequação à LGPD

A Portaria SGD/MGI nº 852, de 28 de março de 2023, dispõe sobre o Programa de Privacidade e Segurança da Informação (PPSI) e a instituição do Framework de Privacidade e Segurança da Informação. Conforme o art. 9º dessa portaria, consideram-se como etapas para a implementação do framework:

> I - autoavaliação: execução de avaliação pelo próprio órgão, considerando o modelo de avaliação de maturidade e capacidade disponibilizado por meio do framework;
>
> II - análise de lacunas: a partir da autoavaliação, esta etapa consiste na identificação de oportunidades quanto à necessidade de implementação de medidas ou de melhoria contínua das medidas já implementadas para aumento da capacidade e maturidade do órgão ou entidade;
>
> III - planejamento: após identificadas as oportunidades de melhorias identificadas na etapa anterior, o órgão deve realizar planejamento que especifique o prazo e as necessidades de recursos para implementação, considerando aspectos orçamentários e de recursos humanos do próprio órgão ou entidade; e

Ante o exposto e em atenção aos Ofícios SGD/MGI nº 1365/2023 e 1468/2023, constantes no Processo SEI nº 19974.101789/2023-31, a Coordenação da Controladoria, em parceria com a Diretoria de Tecnologia da Informação (DTI), respondeu e enviou por e-mail, no dia 27/12/2023, para MGI/MGI-SGD-DPSI <cgpd@economia.gov.br>, o formulário referente ao Framework de Privacidade e Segurança da Informação, contendo os Planos de Ação atualizados do Ciclo 1, bem como os Planos de Ação do Ciclo 2.

De acordo com o referido formulário, a maturidade do IFPE em relação à **Estruturação Básica de Gestão em Segurança da Informação e Privacidade está em estágio "Em Aprimoramento** (0,77 - Indicador de Maturidade do Controle de Estruturação Básica)", com a pendência de "Instituir uma Equipe de Tratamento de Resposta a Incidentes Cibernéticos", que, apesar de constar no art. 37 da Política de Segurança da Informação e Comunicação do IFPE, ainda não foi instituída formalmente. Apresentamos abaixo os parâmetros para identificar o nível de maturidade das instituições, conforme apresentado no *Guia do Framework de Privacidade e Segurança da Informação* (Brasil, 2023a):

Quadro 1 - Relação entre o Indicador e o Nível de Maturidade

iMC[1]	Nível de Maturidade
0,00 a 0,29	Inicial
0,30 a 0,49	Básico
0,50 a 0,69	Intermediário
0,70 a 0,89	Em Aprimoramento
0,90 a 1,00	Aprimorado

Fonte: *Guia do Framework de Privacidade e Segurança da Informação* (Brasil, 2023a)

No quadro a seguir são apresentados os indicadores da Estrutura Básica, do iSeg (Segurança da informação) e do iPriv (Privacidade) do IFPE em comparação com a média da região Nordeste:

Quadro 2 - Comparação da Média dos Indicadores do IFPE com os da Região Nordeste

Descrição	Estrutura Básica	iSeg	iPriv
Média dos órgãos do SISP[2] da Região Nordeste	0,57	0,30	0,26
Valor individual do IFPE	0,77	0,54	0,57

Fonte: Ofício SEI nº 56508/2024/MGI (Brasil, 2024c).

A seguir apresentamos um quadro-resumo com os níveis de maturidade do IFPE relativos ao Indicador de Segurança e ao Indicador de Privacidade:

Quadro 3 - Detalhes dos Indicadores de Segurança e de Privacidade

ISEG	Indicador de Segurança = 0,54		Intermediário
ID CONTROLE	NOME CONTROLE	Indicador de Maturidade do Controle de Segurança da Informação	Nível de Maturidade
1	CIS CONTROLE 1: INVENTÁRIO E CONTROLE DE ATIVOS INSTITUCIONAIS	0,77	Em Aprimoramento
2	CIS CONTROLE 2: INVENTÁRIO E CONTROLE DE ATIVOS DE SOFTWARE	0,66	Intermediário

[1] Indicador de Maturidade por Controle (iMC)
[2] Sistema de Administração dos Recursos de Tecnologia da Informação (SISP)

3	CIS CONTROLE 3: PROTEÇÃO DE DADOS	0,51	Intermediário
4	CIS CONTROLE 4: CONFIGURAÇÃO SEGURA DE ATIVOS INSTITUCIONAIS E SOFTWARE	0,55	Intermediário
5	CIS CONTROLE 5: GESTÃO DE CONTAS	0,70	Em Aprimoramento
6	CIS CONTROLE 6: GESTÃO DO CONTROLE DE ACESSO	0,63	Intermediário
7	CIS CONTROLE 7: GESTÃO CONTÍNUA DE VULNERABILIDADES	0,38	Básico
8	CIS CONTROLE 8: GESTÃO DE REGISTROS DE AUDITORIA	0,55	Intermediário
9	CIS CONTROLE 9: PROTEÇÕES DE E-MAIL E NAVEGADOR WEB	0,63	Intermediário
10	CIS CONTROLE 10: DEFESAS CONTRA MALWARE	0,30	Básico
11	CIS CONTROLE 11: RECUPERAÇÃO DE DADOS	0,68	Intermediário
12	CIS CONTROLE 12: GESTÃO DA INFRAESTRUTURA DE REDE	0,33	Básico
13	CIS CONTROLE 13: MONITORAMENTO E DEFESA DA REDE	0,64	Intermediário
14	CIS CONTROLE 14: CONSCIENTIZAÇÃO E TREINAMENTO DE COMPETÊNCIAS SOBRE SEGURANÇA	0,15	Inicial
15	CIS CONTROLE 15: GESTÃO DE PROVEDOR DE SERVIÇOS	0,17	Inicial
16	CIS CONTROLE 16: SEGURANÇA DE APLICAÇÕES	0,30	Básico
17	CIS CONTROLE 17: GESTÃO DE RESPOSTA A INCIDENTES	0,44	Básico
18	CIS CONTROLE 18: TESTES DE INVASÃO	0,32	Básico

IPRIV	Indicador de Privacidade = 0,57		Intermediário
19	PRIVACIDADE CONTROLE 19: INVENTÁRIO E MAPEAMENTO	0,45	Básico
20	PRIVACIDADE CONTROLE 20: FINALIDADE E LEGITIMIDADE	0,60	Intermediário
21	PRIVACIDADE CONTROLE 21: GOVERNANÇA	0,62	Intermediário
22	PRIVACIDADE CONTROLE 22: POLÍTICAS, PROCESSOS E PROCEDIMENTOS	0,70	Em Aprimoramento
23	PRIVACIDADE CONTROLE 23: CONSCIENTIZAÇÃO E TREINAMENTO	0,39	Básico
24	PRIVACIDADE CONTROLE 24: MINIMIZAÇÃO DE DADOS	0,32	Básico
25	PRIVACIDADE CONTROLE 25: GESTÃO DO TRATAMENTO	0,31	Básico
26	PRIVACIDADE CONTROLE 26: ACESSO E QUALIDADE	0,68	Intermediário
27	PRIVACIDADE CONTROLE 27: COMPARTILHAMENTO, TRANSFERÊNCIA E DIVULGAÇÃO	0,64	Intermediário
28	PRIVACIDADE CONTROLE 28: SUPERVISÃO EM TERCEIROS	0,77	Em Aprimoramento
29	PRIVACIDADE CONTROLE 29: ABERTURA, TRANSPARÊNCIA E NOTIFICAÇÃO	0,53	Intermediário
30	PRIVACIDADE CONTROLE 30: AVALIAÇÃO DE IMPACTO, MONITORAMENTO E AUDITORIA	0,33	Básico
31	PRIVACIDADE CONTROLE 31: SEGURANÇA APLICADA A PRIVACIDADE	0,34	Básico

Fonte: Elaboração própria a partir das respostas apresentadas ao Programa de Privacidade e Segurança da Informação, encaminhadas via e-mail no dia 27/12/2023.

As respostas e o nível de maturidade subsidiam análises que possibilitam o direcionamento de esforços e a priorização das ações necessárias para a construção da conformidade à Lei Geral de Proteção de Dados Pessoais (LGPD). No quadro a seguir é apresentada a atualização do Plano de Ação do IFPE para o “Ciclo 1” e “Ciclo 2” e o Plano

de Ação do “Ciclo 3”, tendo como responsáveis a encarregada de dados pessoais e o diretor de Tecnologia da Informação:

Quadro 4 - Planos de Ação do IFPE relativos ao Programa de Privacidade e Segurança da Informação

Ciclo	ID	Medida	Responsáveis	Previsão de Fim
1	0.2	O órgão nomeou um Gestor de Segurança da Informação?	Jobson Tenório do Nascimento	31/12/2024
1	0.4	O órgão instituiu um Comitê de Segurança da Informação?	Jobson Tenório do Nascimento	31/12/2024
1	0.5	O órgão instituiu uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR?	Jobson Tenório do Nascimento	31/12/2024
1	1.1	O órgão estabelece e mantém um inventário detalhado de ativos institucionais?	Jobson Tenório do Nascimento	31/12/2024
1	1.5	O órgão endereça ativos não autorizados?	Jobson Tenório do Nascimento	31/12/2024
1	2.1	O órgão estabelece e mantém um inventário de software?	Jobson Tenório do Nascimento	31/12/2024
1	2.2	O órgão assegura que o software autorizado seja atualmente suportado?	Jobson Tenório do Nascimento	31/12/2024
3	2.6	O órgão utiliza ferramentas automatizadas de inventário de software?	Jobson Tenório do Nascimento	31/12/2024
1	2.7	O órgão endereça o software não autorizado?	Jobson Tenório do Nascimento	31/12/2024
2	3.1	O órgão estabelece e mantém um processo de gestão de dados?	Jobson Tenório do Nascimento	31/12/2024
2	3.2	O órgão estabelece e mantém um inventário de dados?	Jobson Tenório do Nascimento	31/12/2024
3	3.14	O órgão registra o acesso a dados sensíveis?	Jobson Tenório do Nascimento	31/12/2024
1	6.1	O órgão estabelece e mantém um inventário de sistemas de autenticação e autorização?	Jobson Tenório do Nascimento	31/12/2024
1	6.3	O órgão estabelece um Processo de Revogação de Acesso?	Jobson Tenório do Nascimento	31/12/2024
3	6.5	O órgão exige MFA para acesso remoto à rede?	Jobson Tenório do Nascimento	31/12/2024
1	6.6	O órgão exige MFA para acesso administrativo?	Jobson Tenório do Nascimento	31/12/2024
3	7.4	O órgão executa a gestão automatizada de patches do sistema operacional?	Jobson Tenório do Nascimento	31/12/2024
1	7.7	O órgão corrige vulnerabilidades detectadas?	Jobson Tenório do Nascimento	31/12/2024
1	8.1	O órgão estabelece e mantém um processo de gestão de log de auditoria?	Jobson Tenório do Nascimento	31/12/2024

1	8.2	O órgão garante o armazenamento adequado do registro de auditoria?	Jobson Tenório do Nascimento	31/12/2024
2	8.4	O órgão retém os logs de auditoria?	Jobson Tenório do Nascimento	31/12/2024
3	8.7	O órgão coleta logs de auditoria de consulta DNS?	Jobson Tenório do Nascimento	31/12/2024
2	10.1	O órgão instala e mantém um software antimalware?	Jobson Tenório do Nascimento	31/12/2024
2	10.2	O órgão configura atualizações automáticas de assinatura antimalware?	Jobson Tenório do Nascimento	31/12/2024
1	11.2	O órgão estabelece e mantém um processo de recuperação de dados?	Jobson Tenório do Nascimento	31/12/2024
1	11.4	O órgão estabelece e mantém uma instância isolada de dados de recuperação?	Jobson Tenório do Nascimento	31/12/2024
1	11.5	O órgão testa os dados de recuperação?	Jobson Tenório do Nascimento	31/12/2024
2	14.1	O órgão implanta e mantém um programa de conscientização de segurança?	Jobson Tenório do Nascimento	31/12/2024
3	14.8	O órgão treina os colaboradores sobre os perigos de se conectar e transmitir dados institucionais em redes inseguras?	Jobson Tenório do Nascimento	31/12/2024
2	15.1	O órgão cria e gerencia o inventário de provedores de serviços?	Jobson Tenório do Nascimento	31/12/2024
3	16.8	O órgão separa sistemas de produção e não produção?	Jobson Tenório do Nascimento	31/12/2024
1	19.1	A organização documenta os sistemas, serviços e processos que tratam dados pessoais?	Maria Dayana Lopes de Oliveira	31/12/2024
1	19.2	O órgão mapeia os agentes de tratamento (controlador, co-controladores e operadores) responsáveis pelo processamento de dados pessoais?	Maria Dayana Lopes de Oliveira	31/12/2024
1	19.5	O órgão mapeia o escopo (abrangência ou área geográfica) dos tratamentos de dados pessoais?	Maria Dayana Lopes de Oliveira	31/12/2024
3	19.6	O órgão documenta a natureza (fonte) dos dados pessoais tratados?	Maria Dayana Lopes de Oliveira	31/12/2024
1	19.7	A organização registra as bases legais que fundamentam as atividades de tratamento de dados pessoais e dados pessoais sensíveis?	Maria Dayana Lopes de Oliveira	31/12/2024
3	19.8	O órgão inventaria as categorias dos dados pessoais e dados pessoais sensíveis objetos dos tratamentos realizados?	Maria Dayana Lopes de Oliveira	31/12/2024

1	19.11	O órgão registra 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?	Maria Dayana Lopes de Oliveira	31/12/2024
1	19.12	O órgão mapeia os ambientes (ex: interno, nuvem, terceiros, etc) em que os dados pessoais objetos dos tratamentos são processados?	Maria Dayana Lopes de Oliveira	31/12/2024
1	19.13	O órgão registra as transferências internacionais de dados pessoais realizadas conforme o Capítulo V da LGPD, incluindo quais dados pessoais foram divulgados e a quem?	Maria Dayana Lopes de Oliveira	31/12/2024
1	19.14	O órgão mapeia os contratos estabelecidos/firmados com terceiros operadores responsáveis pelos tratamentos de dados pessoais?	Maria Dayana Lopes de Oliveira	31/12/2024
2	20.1	O órgão identifica as finalidades específicas antes da realização dos tratamentos de dados pessoais?	Maria Dayana Lopes de Oliveira	31/12/2024
2	20.2	O órgão identifica as hipóteses de tratamento antes da realização dos processamentos de dados pessoais?	Maria Dayana Lopes de Oliveira	31/12/2024
2	20.3	A organização identifica as bases legais que fundamentam as atividades de tratamento de dados pessoais e dados pessoais sensíveis antes da realização do tratamento?	Maria Dayana Lopes de Oliveira	31/12/2024
2	20.4	O órgão prioritariamente realiza 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?	Maria Dayana Lopes de Oliveira	31/12/2024
2	20.10	O órgão, ao realizar compartilhamento de dados pessoais, adota medidas que assegurem a compatibilidade do propósito geral da finalidade original informada ao titular?	Maria Dayana Lopes de Oliveira	31/12/2024
2	20.14	O tratamento de dados pessoais de crianças e adolescentes é realizado no seu melhor interesse com base em hipótese legal prevista pela LGPD e, no que couber, conforme preconizado pelo art. 14 da LGPD?	Maria Dayana Lopes de Oliveira	31/12/2024
1	21.2	O órgão já elaborou e divulgou o seu Programa Institucional de Privacidade de Dados, conforme estabelecido no art.50 da LGPD?	Maria Dayana Lopes de Oliveira	31/08/2024
2	21.4	O órgão disponibiliza para o encarregado os recursos necessários para implementação da LGPD e acesso direto à alta administração?	Maria Dayana Lopes de Oliveira	31/12/2024
2	21.6	O órgão divulga a seus colaboradores internos e externos as políticas e procedimentos operacionais relacionados à proteção de dados pessoais?	Maria Dayana Lopes de Oliveira	31/10/2024

2	22.1	A organização revisou e adequou a Política de Segurança da Informação ou instrumento similar à LGPD?	Jobson Tenório do Nascimento	31/12/2024
2	22.4	Os instrumentos convocatórios (editais licitatórios) estão adequados à LGPD?	Maria Dayana Lopes de Oliveira	31/12/2024
2	22.10	A organização adequou seu Plano de Resposta a Incidentes (ou documento similar) à LGPD de forma a tratar violações relativas à privacidade dos titulares de dados pessoais?	Jobson Tenório do Nascimento	31/12/2024
3	23.1	O órgão 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?	Jobson Tenório do Nascimento	31/12/2024
2	23.2	O plano de desenvolvimento de pessoas do órgão contempla treinamento adequado sobre a temática de privacidade e de proteção de dados pessoais?	Maria Dayana Lopes de Oliveira	31/08/2024
2	24.1	O órgão avalia e classifica 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?	Maria Dayana Lopes de Oliveira	31/12/2024
3	24.13	O órgão ao coletar cookies disponibiliza botão de fácil visualização, no banner de primeiro e de segundo nível, que permita rejeitar todos os cookies não-necessários?	Jobson Tenório do Nascimento	31/12/2024
3	26.3	O órgão 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?	Maria Dayana Lopes de Oliveira	31/12/2024
2	26.5	O órgão adota 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?	Maria Dayana Lopes de Oliveira	31/12/2024
2	27.3	O órgão, ao compartilhar dados pessoais, adota um processo de formalização e registro, identificando objeto e finalidade, base legal e duração do tratamento?	Maria Dayana Lopes de Oliveira	31/12/2024
2	27.4	O órgão solicita descrição formal das medidas de proteção de dados pessoais adotadas pelas entidades com quem compartilha dados pessoais?	Maria Dayana Lopes de Oliveira	31/12/2024
1	28.2	São estabelecidos acordos de confidencialidade, termos de responsabilidade ou termos de sigilo com operadores de dados pessoais controlados pelos órgãos?	Maria Dayana Lopes de Oliveira	31/12/2024
1	28.3	O órgão estabelece no contrato que o operador não processe os dados pessoais para finalidades que divergem da finalidade principal informada pelo controlador?	Maria Dayana Lopes de Oliveira	31/12/2024

3	28.11	O órgão especifica no contrato entre controlador e operador sobre o uso de subcontratados para processar dados pessoais?	Maria Dayana Lopes de Oliveira	31/12/2024
3	29.1	O órgão adota meios para apresentar as informações de tratamento de dados 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?	Maria Dayana Lopes de Oliveira	31/12/2024
1	29.2	O órgão adota 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?	Maria Dayana Lopes de Oliveira	31/08/2024
1	30.1	O órgão observa 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?	Maria Dayana Lopes de Oliveira	31/12/2024
1	30.5	O órgão documenta as medidas de proteção de dados pessoais adotadas para mitigação do impacto à Proteção de Dados Pessoais?	Maria Dayana Lopes de Oliveira	31/12/2024
2	31.3	A organização implementa processo para registro, cancelamento e provisionamento de usuários em sistemas que realizam tratamento de dados pessoais?	Jobson Tenório do Nascimento	31/12/2024
2	31.4	A instituição considera o princípio do privilégio mínimo na concessão de direitos de acesso para o processamento de dados pessoais?	Jobson Tenório do Nascimento	31/12/2024
3	31.6	O acesso físico aos dados e dispositivos é gerenciado?	Jobson Tenório do Nascimento	31/12/2024
3	31.11	O órgão descarta materiais impressos de forma segura?	Maria Dayana Lopes de Oliveira	31/12/2024
3	31.15	A organização ao 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, modificações ou exclusões), como um resultado do evento?	Jobson Tenório do Nascimento	31/12/2024
2	31.17	A organização possui sistema para o registro de incidentes de segurança da informação que envolvem violação de dados pessoais?	Jobson Tenório do Nascimento	31/12/2024

Fonte: Elaboração própria a partir das respostas apresentadas ao Programa de Privacidade e Segurança da Informação, encaminhadas via e-mail no dia 31/07/2024.

1.4 Análise e Adoção de Medidas de Segurança, Inclusive Diretrizes e Cultura Interna

As medidas de segurança adotadas estão definidas pela Política de Segurança da Informação e Comunicação (PoSIC) do IFPE, aprovada por meio da Resolução nº 11/2017, do Conselho Superior. A PoSIC tem como objetivo estabelecer mecanismos e controles para garantir a efetiva proteção dos dados, informações e conhecimentos gerados e a redução dos riscos de ocorrência de perdas, alterações e acessos indevidos, preservando a disponibilidade, integridade, confiabilidade e autenticidade das informações no IFPE.

Destaca-se que, como essa política foi aprovada anteriormente à publicação da Lei Geral de Proteção de Dados Pessoais (LGPD), faz-se necessária sua atualização para adequação à lei em análise.

1.5 Instituição de Estrutura Organizacional para a Governança e Gestão da Proteção de Dados Pessoais

Conforme o art. 12 da Política Geral de Proteção de Dados Pessoais do IFPE, foi criada a **Comissão Permanente de Gestão de Dados Pessoais (CPGDP)**, com ciclos de atuação e organização estabelecidos em regimento, com o objetivo de assessorar o/a encarregado/a no desenvolvimento de suas atribuições, sendo composta pelos seguintes membros:

- o/a diretor/a da Controladoria (encarregado/a de dados pessoais do IFPE);
- o/a ouvidor/a-geral do IFPE;
- o/a gestor/a do Serviço de Informação ao Cidadão (SIC);
- o/a diretor/a de Tecnologia da Informação e Comunicação;
- o/a diretor/a de Gestão de Pessoas;
- o/a pró-reitor/a de Integração e Desenvolvimento Institucional;
- o/a pró-reitor/a de Ensino;
- o/a pró-reitor/a de Pesquisa, Pós-Graduação e Inovação;
- o/a pró-reitor/a de Extensão;
- o/a pró-reitor/a de Administração;
- o/a diretor/a de Assistência ao Estudante; e
- os/as diretores(as)-gerais, em número mínimo de dois/duas, escolhidos(as) entre os pares.

A comissão foi instituída pela Portaria IFPE nº 1.327, de 11 de novembro de 2022, e atualizada pela Portaria IFPE nº 804, de 4 de junho de 2024, tendo caráter permanente, devendo ser renovada e/ou reconduzida anualmente, por meio de portaria expedida pelo/a reitor/a.

No art. 2º da referida portaria são apresentadas as competências da comissão, quais sejam:

- assessorar o/a encarregado/a de dados pessoais no desenvolvimento de suas atribuições;
- deliberar e aprovar o Inventário de Dados Pessoais, o Relatório de Impacto à Proteção de Dados Pessoais, o Mapeamento do Processo de Tratamento de Dados Pessoais e o Relatório de Gestão do Risco de Vazamento de Dados;
- elaborar orientações técnicas e outros normativos necessários à regulamentação da Política Geral de Proteção de Dados Pessoais do IFPE;
- estabelecer as categorias de usuários e procedimentos para tratamento de dados, conforme as hipóteses dispostas nos incisos VI, VII, IX e X do art. 7o da LGPD e nas alíneas “d”, “e” e “g” do inciso II do art. 11 da LGPD, definido em caráter especial e com finalidade específica;
- auxiliar no encaminhamento de denúncia ou reclamação a partir de titulares ou notificação de órgão de controle recebida pela Ouvidoria ou pelo/a encarregado/a de dados pessoais do IFPE;
- deliberar sobre os casos omissos de aplicação da LGPD não previstos em normativas do IFPE.

1.6 Inventário de Dados Pessoais

O IFPE adotará o modelo apresentado no *Guia de Elaboração de Inventário de Dados Pessoais do Programa de Privacidade e Segurança da Informação (PPSI)*, versão 2.0 (31/3/2023).

O referido guia é recomendado e dirigido aos órgãos e às entidades da administração pública federal e tem como objetivo auxiliar na elaboração do inventário de dados pessoais, em atendimento ao art. 37 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD)

O documento é de autoria exclusiva da Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos (MGI) e tem como referência fundamental o *Guia do Framework de Privacidade e Segurança da Informação*.

Conforme o próprio documento relata, o guia será atualizado frequentemente, de acordo com as novas diretrizes determinadas pelas autoridades em privacidade e segurança da informação ou segundo eventuais alterações que ocorram na legislação vigente relacionada a privacidade e segurança da informação e outras referências utilizadas no documento.

O inventário foi estruturado em formato de planilha eletrônica, disponível em link presente no próprio guia (versão 9/3/2023). No âmbito do IFPE, o link está disponível em: template_inventario_dados_pessoais (2).xlsx .

1.7 Levantamento dos Contratos Relacionados a Dados Pessoais

Por meio do levantamento dos serviços que tratam dados pessoais no Inventário de Dados, será possível fazer um cruzamento com os contratos que os suportam. Esse mapeamento dos contratos relativos ao tratamento de dados pessoais contribuirá para possíveis e necessárias adequações contratuais, tanto nos contratos existentes quanto nos futuros, conforme orienta o próprio de *Guia de Elaboração de Programa de Governança em Privacidade,* da SGD/MGI.

2. ETAPA 2 - Construção e Execução

Essa etapa aborda a implementação propriamente dita do PGP do IFPE por meio dos seguintes marcos:

1. Políticas e Práticas para a Proteção da Privacidade do Cidadão;
2. Cultura de Segurança e Proteção de Dados e Privacy by Design;
3. Relatório de Impacto à Proteção de Dados Pessoais (RIPD);
4. Política de Privacidade e Política de Segurança da Informação;
5. Adequação de Cláusulas Contratuais; e
6. Termo de Uso.

2.1 Políticas e Práticas para a Proteção da Privacidade do Cidadão

A Política Geral de Proteção de Dados Pessoais do IFPE, aprovada por meio da Resolução nº 124, de 30 de março de 2022, do Conselho Superior, objetiva, conforme dispõe seu art. 1º, disciplinar o tratamento e o uso de dados pessoais coletados e/ou mantidos em bancos de dados da instituição, bem como assegurar a proteção de dados pessoais nos termos da Lei nº 13.709, de 14 de agosto de 2018, e tem como finalidade direcionar, monitorar e avaliar a gestão do tratamento e da proteção dos dados pessoais, definir princípios e diretrizes sobre a governança, a aprovação ou a revogação do acesso aos dados pessoais, aos dados pessoais sensíveis e aos dados pessoais da criança, do adolescente e do idoso.

O regulamento do uso de dados pessoais de forma institucional, que dispõe sobre a implementação, desenvolvimento e aperfeiçoamento da LGPD no âmbito do IFPE, de modo a uniformizar os procedimentos gerais a serem observados no tratamento de dados pessoais, está em fase de conclusão.

2.2 Cultura de Segurança e Proteção de Dados e Privacidade desde a Concepção (Privacy by Design)

Conforme o *Guia de Elaboração do Programa de Governança em Privacidade*, a promoção de uma cultura de segurança e proteção de dados tem como objetivo comunicar os objetivos, metas e indicadores utilizados, além de divulgar o papel do IFPE como custodiante dos dados e sua responsabilidade ao tratar os dados pessoais dos cidadãos. As informações deste PGP devem ser disponibilizadas de forma clara e eficiente, além de estarem facilmente acessíveis.

Ademais, para desenvolver a cultura de segurança e proteção de dados no IFPE, devem ser realizadas campanhas de conscientização, além de capacitações sobre a temática. As campanhas de conscientização poderão ser continuamente desenvolvidas pelo Departamento de Comunicação (Dcom) em parceria com a Comissão Permanente de Gestão de Dados Pessoais.

O conceito de Privacidade desde a Concepção (Privacy by Design) significa que a privacidade e a proteção de dados devem ser consideradas desde a concepção e durante todo o ciclo de vida do projeto, sistema, serviço, produto ou processo.

Conforme o *Guia de Boas Práticas da LGPD*, tal privacidade pode ser alcançada por meio da aplicação dos 7 Princípios Fundamentais, listados a seguir:

● Proativo, e não reativo; preventivo, e não corretivo: a abordagem de Privacidade desde a Concepção (PdC) antecipa e evita eventos invasivos de privacidade antes que eles aconteçam. Desse modo, não espera que riscos de privacidade se materializem nem oferece soluções para as infrações de privacidade após a ocorrência, mas visa impedir que eles ocorram;

● Privacidade deve ser o padrão dos sistemas de TI ou práticas de negócio: busca-se oferecer o máximo grau de privacidade, garantindo que os dados pessoais sejam protegidos automaticamente em qualquer sistema de TI ou prática de negócios. É uma forma de evitar que qualquer ação seja necessária por parte do titular dos dados pessoais para proteger a sua privacidade, pois ela já estará embutida no sistema, por padrão;

● Privacidade incorporada ao projeto (design): a privacidade deve estar incorporada ao projeto e arquitetura dos sistemas de TI e práticas de negócios, não deve ser considerada como complemento adicional, após o sistema, projeto ou serviço já estar em implementação ou em execução. O resultado é que a privacidade se torna um componente essencial da funcionalidade principal que está sendo entregue. A privacidade é parte integrante do sistema, sem diminuir a funcionalidade;

● Funcionalidade total: a PdC não envolve simplesmente a formalização de declarações e compromissos de privacidade. Refere-se a satisfazer todos os objetivos do projeto, não apenas os objetivos de privacidade, permitindo funcionalidade total com resultados reais e práticos. Ao incorporar privacidade em uma determinada tecnologia, processo ou sistema, isso é realizado de uma forma que não comprometa a plena funcionalidade e permita que todas as exigências do projeto sejam atendidas;

● Segurança e proteção de ponta a ponta durante o ciclo de vida de tratamento dos dados: por ser incorporado ao sistema antes de o primeiro elemento de informação ser coletado, a PdC estende-se por todo o ciclo de tratamento dos dados envolvidos no projeto, sistema ou serviço. Medidas fortes de segurança são essenciais para a privacidade, do início ao fim;

● Visibilidade e Transparência: a PdC objetiva garantir a todos os interessados que, independentemente da prática ou tecnologia comercial envolvida, está de fato operando de acordo com as premissas e objetivos declarados, os quais devem ser objeto de verificação independente. Visibilidade e transparência são essenciais para estabelecer responsabilidade e confiança;

● Respeito pela privacidade do usuário: acima de tudo, a Privacidade desde a Concepção exige que as instituições respeitem os direitos dos titulares dos dados pessoais. Isso é alcançado por meio de medidas como padrões fortes de privacidade, avisos apropriados e interfaces amigáveis que empoderem o titular dos dados. Os melhores resultados da Privacidade desde a Concepção, geralmente, são aqueles projetados de acordo com os interesses e necessidades dos titulares dos dados pessoais, que têm o maior interesse em gerenciar seus próprios dados.

2.3 Relatório de Impacto à Proteção de Dados Pessoais

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD), conforme o inciso XVII do art. 5º da LGPD, é a documentação do/a controlador/a que contém a descrição dos 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.

O conteúdo mínimo do RIPD é indicado pelo parágrafo único do art. 38: a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do/a controlador/a com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

O IFPE adotará, na elaboração do RIPD, as orientações constantes no *Guia de Boas Práticas da LGPD* (versão 2.0, de 14/8/2020), em sua seção 2.5. Também para auxiliar os trabalhos, tomaremos como modelo o estudo de caso do Departamento de Segurança Pública.

2.4 Política de Privacidade e Política de Segurança da Informação

Conforme apresentado na Etapa 1 deste PGP, a Política de Segurança da Informação e Comunicação (PoSIC) do IFPE foi aprovada por meio da Resolução nº 11/2017, do Conselho Superior, e tem como objetivo estabelecer mecanismos e controles para garantir a efetiva proteção dos dados, informações e conhecimentos gerados e a redução dos riscos de ocorrência de perdas, alterações e acessos indevidos, preservando a disponibilidade, integridade, confiabilidade e autenticidade das informações na instituição.

2.5 Adequação de Cláusulas Contratuais

Com base no princípio da transparência, apresentado no art. 6° da LGPD, torna-se essencial que os contratos, convênios e outros instrumentos que impliquem no tratamento de dados pessoais apresentem informações claras e objetivas, abordando, se pertinente:

- delimitações claras e objetivas das responsabilidades do/a controlador/a e do/a operador/a;
- a forma como são realizados a coleta e o tratamento de dados;
- a existência da possibilidade de o titular acessar os seus dados coletados;
- a forma como são realizada a correção, o bloqueio ou a eliminação de dados mediante solicitação do titular;
- a existência da possibilidade de revogação do consentimento dado pelo 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;
- as medidas de proteção e segurança dos dados coletados e armazenados pela contratada.

A partir do inventário, realizado na Etapa 1 – Iniciação e Planejamento, serão identificados os contratos, convênios e outros instrumentos que impliquem no tratamento de dados pessoais. Assim, com o apoio da Coordenação de Contratos, em nível sistêmico, será analisada a necessidade de adequação das cláusulas contratuais firmadas.

2.6 Termo de Uso

De acordo com o *Guia de Elaboração de Termo de Uso e Política de Privacidade* (versão 2.0, de 31/3/2023), o Termo de Uso informa as regras a que o usuário está sujeito ao utilizar os serviços prestados por meio de aplicações, como sites, sistemas e aplicativos para os dispositivos móveis no âmbito institucional, enquanto a Política de Privacidade tem como objetivo descrever para o titular dos dados pessoais os procedimentos e processos adotados no tratamento de dados pessoais realizado pelo serviço, bem como informá-lo sobre as medidas de proteção de dados pessoais adotadas.

O Termo de Uso e a Política de Privacidade podem ser consolidados em um único documento ou constar em documentos separados. No IFPE adotaremos um único documento, intitulado Termo de Uso e Aviso de Privacidade, conforme consta no Anexo I**.**

A fim de garantir aos usuários amplo acesso às informações, o Termo de Uso deve:

- ser editado em linguagem acessível, clara e simples;
- apresentar informações precisas sobre as funcionalidades oferecidas aos usuários do serviço e os requisitos necessários para acessá-las;
- ser constantemente atualizado;
- apresentar um canal pelo qual o usuário pode apresentar eventual manifestação sobre a prestação do serviço.

Também é importante que o referido documento seja submetido à Procuradoria Federal junto ao IFPE, de modo a confirmar se as cláusulas escritas estão de acordo com a legislação vigente e se possuem validade jurídica.

Conforme o referido guia, são tópicos que devem constar no Termo de Uso: Aceitação dos Termos e Políticas; Definições; Arcabouço Legal; Descrição do Serviço; Direitos do Usuário; Responsabilidades do Usuário e da Administração Pública; Mudanças no Termo de Uso; Informações para Contato; Foro.

O termo deverá ser periodicamente atualizado, de forma que possa refletir, de modo claro e preciso, as finalidades de coleta, uso, armazenamento, tratamento e proteção dos dados pessoais dos titulares que comumente serão utilizados pela instituição no exercício de suas competências legais ou execução de políticas públicas.

Por fim, para verificar se o Termo de Uso e Aviso de Privacidade do IFPE atende às exigências previstas na LGPD, preenchemos o *Checklist para Verificação de Política de Privacidade*, elaborado pelo Tribunal de Contas da União – TCU.

3. ETAPA 3 - Monitoramento

O Monitoramento permanecerá após a implementação do Programa de Governança em Privacidade, para garantir seu aprimoramento contínuo e a implementação dos marcos estabelecidos, quais sejam:

1. Indicadores de Performance;

2. Gestão de Incidentes;

3. Análise e Reporte de resultados.

3.1 Indicadores de Performance

O IFPE utilizará os indicadores de Maturidade por Controle (iMC), de Maturidade de Privacidade (iPriv) e de Maturidade de Segurança da Informação (iSeg) — presentes no Capítulo 6 do *Guia do Framework de Privacidade e Segurança da Informação*, conforme resultados apresentados no Quadro 3 do item "1.3 Análise da Maturidade - Diagnóstico do atual estágio de adequação à LGPD" deste PGP.

3.2 Gestão de Incidentes

O Plano de Resposta a Incidentes do IFPE será elaborado a partir da construção do Relatório de Impacto à Proteção de Dados Pessoais (RIPD). O plano será divulgado numa versão posterior deste PGP.

O IFPE possui um procedimento de Comunicação de Incidentes de Segurança da Informação, conforme o Anexo II, que poderá ser atualizado sempre que necessário.

3.3 Análise e Reporte de Resultados

O reporte de resultados, nessa etapa de monitoramento, servirá para demonstrar o valor do PGP à alta administração. Pretende-se apresentar em reunião do Comitê de Governança, Riscos e Controles do IFPE a evolução das ações e os resultados obtidos, de modo a reforçar e fortalecer a cultura de privacidade dos dados.

REFERÊNCIAS

ANPD. **Guia Orientativo:** tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas. Brasília, DF: ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf. Acesso em: 6 maio 2024.

BRASIL. Comitê Central de Governança de Dados. **Guia de Boas Práticas:** Lei Geral de Proteção de Dados (LGPD). Versão 2.0. Brasília, DF 2020. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade_e_seguranca/guias/guia_lgpd.pdf. Acesso em: 26 fev. 2024.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Portaria SGD/MGI nº 852, de 28 de março de 2023. Dispõe sobre o Programa de Privacidade e Segurança da Informação (PPSI) e a instituição do Framework de Privacidade e Segurança da Informação. **Diário Oficial da União**: seção 1, Brasília, DF, edição 62, página 92, 30 mar. 2023a. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908. Acesso em: 7 maio 2024.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Guia de Elaboração de Inventário de Dados**. Versão 2.0. Brasília, MGI, 2023b. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade_e_seguranca/ppsi/guia_inventario_dados_pessoais.pdf. Acesso em: 23 fev. 2024.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Guia de Elaboração de Termo de Uso e Política de Privacidade**. Versão 2.0. Brasília, DF: MGI, 2023c. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade_e_seguranca/ppsi/guia_termo_uso_politica_privacidade.pdf. Acesso em: 23 fev. 2024.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Guia de Elaboração de Programa de Governança em Privacidade**. Versão 2.1. Brasília, DF: MGI, 2024a. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade_e_seguranca/ppsi/guia_programa_governanca_privacidade.pdf. Acesso em: 22 fev. 2024.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Guia do Framework de Privacidade e Segurança da Informação**. Versão 1.1.3. Brasília, DF: MGI, 2024b. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf.
Acesso em: 23 fev. 2024.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Ofício SEI nº 56508/2024/MGI**. Brasília, DF: MGI, 30 abr. 2024c.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Relatório de Impacto à Proteção de Dados Pessoais (RIPD)**. Brasília, DF: MGI, [2023 ou 2024]. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade_e_seguranca/templates-e-ferramentas/estudo_template_preenchido_ripd.pdf/view. Acesso em: 26 fev. 2024.

BRASIL. Receita Federal. **Termo de Uso e Política de Privacidade.** Brasília, DF: Receita Federal, 2022. Disponível em https://www.gov.br/receitafederal/pt-br/acesso-a-informacao/lgpd/termo-de-uso#section-9. Acesso em: 4 mar. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 maio 2024.

ENAP. **Termo de Uso e Aviso de Privacidade**. Brasília, DF: Enap, 2023. Disponível em: https://enap.gov.br/pt/termo-de-uso-e-aviso-de-privacidade. Acesso em: 4 mar. 2024.

BRASIL. Tribunal de Contas da União. **Checklist para Verificação de Política de Privacidade**. Brasília, DF: TCU, [entre 2018 e 2024]. Disponível em: https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/fiscalizacoes/auditoria-sobre-lgpd/. Acesso em: 25 jun. 2024.

IFPE. Conselho Superior. **Resolução nº 11/2017**. Aprova a Política de Segurança da Informação e Comunicação do IFPE. Recife: Consup, 2017. Disponível em: https://portal.ifpe.edu.br/wp-content/uploads/repositoriolegado/portal/documentos/resolucao-11-2017-aprova-a-politica-de-seguranca-da-informacao-e-comunicacao-do-ifpe.pdf. Acesso em: 22 maio 2024.

IFPE. Conselho Superior. **Resolução nº 57 de 30 de novembro de 2018.** Institui a Política de Gestão de Riscos do IFPE. Recife: Consup, 2018. Disponível em: https://portal.ifpe.edu.br/wp-content/uploads/repositoriolegado/portal/documentos/resolucao-57-2018-institui-a-politica-de-gestao-de-riscos-do-ifpe.pdf. Acesso em: 6 maio 2024.

IFPE. Conselho Superior. **Resolução nº 124, de 30 de março de 2022**. Aprova a Política Geral de Proteção de Dados Pessoais do IFPE. Recife: Consup, 2022. Disponível em: https://portal.ifpe.edu.br/wp-content/uploads/repositoriolegado/portal/documentos/resolucao-124-2022-aprova-a-politica-geral-de-protecao-de-dados-pessoais-do-ifpe.pdf. Acesso em: 22 maio 2024.

ANEXO I

TERMO DE USO E AVISO DE PRIVACIDADE

1 Informações gerais

Este Termo tem como objetivo dar maior clareza do compromisso do IFPE com a segurança, confidencialidade e integridade no uso dos dados pessoais. Nele o usuário encontrará informações sobre o funcionamento dos serviços fornecidos por meio de aplicações no site, sistemas e aplicativos para dispositivos móveis; o embasamento legal relacionado à prestação do serviço; as suas responsabilidades ao utilizar o serviço; as responsabilidades da administração pública ao fornecer o serviço; informações para contato; o foro responsável por eventuais reclamações, entre outras informações.

Por isso, é importante que o usuário leia e entenda o documento, de modo a estar ciente de todas as condições estabelecidas, e se comprometa a cumpri-las.

*Esta versão foi atualizada pela última vez em 21 de novembro de 2024. O IFPE poderá atualizá-la a qualquer momento, por isso o usuário deve consultar periodicamente o site institucional do Instituto.

1.1 Aceitação, Concordância ou Ciência do Termo de Uso e Aviso de Privacidade

Ao utilizar os serviços, o usuário confirma que leu, entende que seus dados pessoais serão tratados e compartilhados nas formas descritas no Aviso de Privacidade e concorda com seus termos. Assim, ao utilizar o serviço, o usuário manifesta sua livre, expressa e inequívoca concordância com relação ao conteúdo deste Termo de Uso/Aviso de Privacidade e estará legalmente vinculado a todas as condições e compromissos aqui previstos.

Para uso dos sistemas do IFPE: Se estiver de acordo com as condições apresentadas, manifestar o seu consentimento livre, expresso, informado e inequívoco, por meio da seleção do *checkbox* correspondente à opção “Li e concordo com o Termo de Uso e Aviso de Privacidade”.

1.2 Definições do Termo de Uso

Para os fins deste Termo de Uso, são aplicáveis as seguintes definições:

AGENTE PÚBLICO - todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da administração pública federal, direta e indireta;

ATIVOS DE INFORMAÇÃO - os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos a que a eles têm acesso;

CÓDIGO MALICIOSO - programa ou parte de um programa de computador projetado especificamente para atentar contra a segurança de um sistema computacional, normalmente através da exploração de alguma vulnerabilidade de sistema;

CONTROLADOR - pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

CRIPTOGRAFIA - arte de proteção da informação através de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno). A chave de decifragem pode ser igual (criptografia simétrica) ou diferente (criptografia assimétrica) da chave de cifragem;

DADO ANONIMIZADO - dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

DADO PESSOAL - informação relacionada a pessoa natural identificada ou identificável;

DADO PESSOAL SENSÍVEL - dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

ENCARREGADO - pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados;

Outras definições podem ser consultadas na Portaria nº 93, de 26 de setembro de 2019, do Gabinete de Segurança Institucional da Presidência da República, que aprovou o Glossário de Segurança da Informação:
https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663

1.3 Embasamento legal

Lei nº 13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados Pessoais (LGPD);

Lei nº 13.460, de 26 de junho de 2017: dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública.

Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet): estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação): regula o acesso a informações previsto na Constituição Federal.

Decreto nº 9.637, de 26 de dezembro de 2018: institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no artigo 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.

Decreto nº 7.724, de 16 de maio de 2012: regulamenta a Lei de Acesso à informação

Decreto nº 7.845, de 14 de novembro de 2012: regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

Outros atos legislativos e normativos de referência também podem ser buscados na página institucional na internet do Governo Digital do Brasil, especificamente na seção "Legislação, Privacidade e Segurança":
https://www.gov.br/governodigital/pt-br/privacidade_e_seguranca/legislacao-federal.

1.4 Descrição dos serviços

Este Termo de Uso e Aviso de Privacidade aplica-se aos serviços fornecidos por meio de aplicações no site do IFPE e aplicativos para dispositivos móveis, quais sejam:

Nº	Sistema	Descrição do objetivo do sistema
1	acesso.ifpe.edu.br	Acesso unificado aos sistemas do IFPE
2	api.ifpe.edu.br	Gateway que intermedeia requisições para APIs internas a fim de criar mais uma camada de segurança
3	atendimento.ifpe.edu.br	Sistema de atendimento on-line
4	atendimentoingresso.ifpe.edu.br	Sistema de atendimento de dúvidas e demandas específicas para o processo de ingresso de estudantes
5	biblioteca.ifpe.edu.br	Gerenciamento digital do acervo bibliográfico do Instituto
6	biserver.ifpe.edu.br	Ferramenta de Business Intelligence and Analytics para gerar relatórios e insights sobre os dados dos sistemas institucionais
7	cadastro.ifpe.edu.br	Permite o cadastro dos servidores para o sistema Acesso e o acompanhamento desses cadastros pela administração
8	caravana.ifpe.edu.br	Plataforma de submissão e publicação de edições da revista "Caravana"
9	certificadoencceja.ifpe.edu.br	Emissão e verificação de certificados de conclusão de ensino médio emitidos pelo Instituto
10	connepi2018.ifpe.edu.br	Portal do Congresso Norte-Nordeste de Pesquisa e Inovação (2018)
11	dados.ifpe.edu.br	Plataforma de Dados Abertos da instituição
12	depreciacao.ifpe.edu.br	Sistema que calcula o valor depreciado de bens móveis

13	eadflow.ifpe.edu.br	Geração e gerenciamento dinâmico de formulários e fluxos de trabalho. Atualmente lida com demandas específicas da EaD.
14	extratorsetec.ifpe.edu.br	Coleta de informações relevantes sobre o planejamento estratégico das instituições da Rede Federal e para realização da extração dos dados de seus indicadores, de forma automática e padronizada
15	florescer.ifpe.edu.br	Gerenciamento de editais de afastamento para pós-graduação
16	fluxo.ifpe.edu.br	Modela e executa os seguintes processos institucionais: Tutoria de Pares; Eleições internas; e Manutenção Acadêmica.
17	gitlab.ifpe.edu.br	Repositório de código fonte de sistemas mantidos pelo IFPE
18	hermes.ifpe.edu.br	Emissor de Relatórios e Certificados do IFPE
19	ingresso.ifpe.edu.br	Sistema de inscrição, avaliação e matrícula dos processos de ingresso on-line
20	integra.ifpe.edu.br	Portal da Inovação do IFPE
21	inventario.ifpe.edu.br	Sistema que auxilia na geração de relatórios do inventário
22	meuemail.ifpe.edu.br	Provê automaticamente e-mails institucionais para estudantes regularmente matriculados e servidores ativos do IFPE
23	pdf.ifpe.edu.br	Manipulação de arquivos no formato PDF
24	pgd.ifpe.edu.br	É utilizado para pactuação e monitoramento dos resultados do Programa de Gestão, seguindo as diretrizes da Instrução Normativa nº 65, de 30 de julho de 2020, do Ministério da Economia
25	portal.ifpe.edu.br	Centraliza informações e serviços relacionados à instituição
26	processos.ifpe.edu.br	Sistema para modelar e compartilhar processos de negócio (BPMN) da instituição
27	projetos.ifpe.edu.br	Plataforma para gerenciamento de projetos
28	remocao.ifpe.edu.br	Gerencia processo de movimentação de servidores entre os diversos *campi* do Instituto
29	repositorio.ifpe.edu.br	Local virtual que reúne a produção científica do IFPE
30	revistas.ifpe.edu.br	Plataforma de submissão e publicação de edições de revistas institucionais
31	sei.ifpe.edu.br	Permite a criação e tramitação de processos eletrônicos
32	senha.ifpe.edu.br	Permite o cadastro e recuperação de senha para acesso ao sistema SUAP
33	suap.ifpe.edu.br	Sistema de apoio à administração pública
34	suporte.ifpe.edu.br	Sistema de chamados de suporte a sistemas do IFPE
35	wiki.ifpe.edu.br	Plataforma para cadastro de informações e dúvidas frequentes
36	workflow.ifpe.edu.br	Geração e gerenciamento dinâmico de formulários e fluxos de trabalho. Atualmente lida com projetos de pesquisa da

		instituição.
37	cvest.ifpe.edu.br/	Sistema de vestibulares, concursos e processos seletivos simplificados

1.5 Direitos do usuário do serviço

A seguir, estão resumidos os direitos do usuário conferidos pela Lei Geral de Proteção de Dados Pessoais:

- Direito de confirmação e acesso (art. 18, I e II): é o direito de obter do serviço a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de acessar os seus dados pessoais;
- Direito de retificação (art. 18, III): é o direito de solicitar a correção de dados incompletos, inexatos ou desatualizados;
- Direito à limitação do tratamento dos dados (art. 18, IV): é o direito de limitar o tratamento de seus dados pessoais, podendo exigir a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei Geral de Proteção de Dados;
- Direito de oposição (art. 18, § 2º): é o direito de, a qualquer momento, se opor ao tratamento de dados por motivos relacionados com a sua situação particular, com fundamento em uma das hipóteses de dispensa de consentimento ou em caso de descumprimento do disposto na Lei Geral de Proteção de Dados;
- Direito de portabilidade dos dados (art. 18, V): é o direito de realizar a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
- Direito de não ser submetido a decisões automatizadas (art. 20): é o direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

1.6 Responsabilidades do usuário e da administração pública

1.6.1 RESPONSABILIDADE DO USUÁRIO

- O usuário se responsabiliza pela precisão e veracidade dos dados informados e reconhece que a inconsistência destes poderá implicar a impossibilidade de se utilizar o serviço solicitado.

- Durante a utilização do serviço, a fim de resguardar e de proteger os direitos de terceiros, o usuário se compromete a fornecer somente seus dados pessoais, e não os de terceiros.

- Seu login e sua senha não poderão ser utilizados por outra pessoa. O usuário se compromete a manter o sigilo da senha, que é pessoal e intransferível, não sendo possível, em qualquer hipótese, a alegação de uso indevido após o ato de compartilhamento.

- O usuário é responsável pela atualização das suas informações pessoais e pelas consequências da omissão ou de erros nas informações pessoais cadastradas.

- O usuário é responsável pela reparação de todos e quaisquer danos, diretos ou indiretos (inclusive decorrentes de violação de quaisquer direitos de outros usuários, de terceiros, direitos de propriedade intelectual, de sigilo e de personalidade), que sejam causados ao IFPE, a qualquer outro usuário ou, ainda, a qualquer terceiro, como também em virtude do descumprimento do disposto neste Termo de Uso e Aviso de Privacidade ou de qualquer ato praticado a partir de seu acesso ao serviço.

1.6.2 RESPONSABILIDADE DA ADMINISTRAÇÃO PÚBLICA

- O IFPE, no papel de custodiante das informações pessoais dos usuários, se compromete a cumprir toda a legislação inerente ao uso correto dos dados pessoais do cidadão, de forma a preservar a privacidade dos dados utilizados nos serviços fornecidos por meio de aplicações no site do IFPE e aplicativos para dispositivos móveis.

- Publicar e informar ao usuário as futuras alterações deste Termo de Uso e Aviso de Privacidade, por meio do site do IFPE, conforme o princípio da publicidade estabelecido no art. 37, caput, da Constituição Federal.

- Em nenhuma hipótese o IFPE será responsável pela instalação, no equipamento do usuário ou de terceiros, de códigos maliciosos (vírus, *trojans*, malwares, *worms*, *bots*, *backdoors*, *spywares*, *rootkits* ou quaisquer outros que venham a ser criados) adquiridos em decorrência da navegação na internet pelo usuário.

- Em hipótese alguma o serviço e seus colaboradores se responsabilizam por eventuais danos diretos, indiretos, emergentes, especiais ou imprevistos, ou multas causadas, em qualquer matéria de responsabilidade, seja contratual, objetiva ou civil (inclusive negligência ou outras), decorrentes de qualquer forma de uso do serviço, mesmo que advertida a possibilidade de tais danos.

- Tendo em vista que o serviço lida com informações pessoais, o usuário concorda que não usará robôs, sistemas de varredura e armazenamento de dados (como *spiders* ou scrapers), links escondidos ou qualquer outro recurso escuso, ferramenta, programa, algoritmo ou método coletor/extrator de dados automático para acessar, adquirir, copiar ou monitorar o serviço, sem permissão expressa por escrito do órgão.

- Em se tratando de aplicativos em dispositivos móveis, sua comercialização é expressamente proibida. Ao concordar com este Termo e utilizar o aplicativo móvel, o usuário receberá uma permissão do órgão para uso não comercial dos serviços oferecidos pelo aplicativo, o que, em nenhuma hipótese, fará dele proprietário do aplicativo móvel.

- Caso o usuário descumpra este Termo ou seja investigado em razão de má conduta, o órgão poderá restringir seu acesso. O usuário também deverá responder legalmente por essa conduta.

- O IFPE poderá, quanto às ordens judiciais de pedido de informações, compartilhar informações necessárias para investigações e tomar medidas relacionadas a atividades ilegais, suspeitas de fraude ou ameaças potenciais contra pessoas, bens ou sistemas que sustentam o serviço, bem como outras medidas necessárias para cumprir as obrigações legais. Caso ocorra o compartilhamento de informações, o IFPE notificará os titulares dos dados, salvo quando o processo estiver em segredo de justiça.

- O IFPE se compromete a preservar a funcionalidade do serviço ou aplicativo, utilizando um layout que respeite a usabilidade e navegabilidade, facilitando a navegação sempre que possível, e exibir as funcionalidades de maneira completa, precisa e suficiente, de modo que as operações realizadas no serviço sejam claras.

1.7 Aviso de Privacidade do IFPE

1.7.1 SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS

Conforme o art. 6º da LGPD, o tratamento de dados pessoais deve observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

1.7.2 CONTATOS

Caso o usuário necessite de suporte ou tenha alguma dúvida, pedido ou sugestão em relação a este Aviso, deve entrar em contato com um dos responsáveis abaixo, conforme o caso:

Controlador - Responsável pelas decisões sobre o tratamento de dados pessoais nos serviços do IFPE.
Nome: José Carlos de Sá Júnior – Reitor
Endereço: Av. Prof Luiz Freire, 500, Cidade Universitária, Recife-PE. CEP: 50740-545
E-mail: gabinete@reitoria.ifpe.edu.br
Telefone: (81) 2125.1608/1607

Operadores - A depender do serviço a ser prestado pelo IFPE, o tratamento dos dados coletados pode ser realizado por servidores, colaboradores ou pelas empresas contratadas para sua execução:
Qualidata (Q-Acadêmico)
ITExperts (Migração dos serviços para nuvem)
RNP (Cooperação)

Encarregada - indicada pelo controlador para atuar como canal de comunicação entre ele, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
Nome: Maria Dayana Lopes de Oliveira - Coordenadora da Controladoria
Endereço: Av. Prof. Luiz Freire, 500, Cidade Universitária, Recife-PE. CEP: 50740-545
Telefone: (81) 2125.1608/1607
E-mail: controladoria@reitoria.ifpe.edu.br

1.7.3 QUAIS DADOS SÃO TRATADOS

TITULARES	DADOS PESSOAIS TRATADOS PELO IFPE

Estudantes	Dados para identificação, dados acadêmicos, dados necessários à reserva de vaga e política de cotas, dados necessários a benefícios e direitos, dados necessários ao cumprimento de obrigação legal ou regulatória e políticas públicas.
Servidores	Dados para identificação, dados necessários à reserva de vaga e política de cotas, dados necessários a benefícios e direitos, dados necessários ao cumprimento de obrigação legal ou regulatória.
Fornecedores	Dados para identificação, dados necessários à classificação da organização, dados necessários ao cumprimento de obrigação legal, financeira ou regulatória.
Colaboradores	Dados para identificação, dados necessários à reserva de vaga e política de cotas, dados necessários a benefícios e direitos, dados necessários ao cumprimento de obrigação legal ou regulatória.
Candidatos em processos seletivos	Dados para identificação, dados necessários à reserva de vaga e política de cotas, dados necessários a benefícios e direitos.
Familiares de alunos	Dados para identificação do aluno, dados necessários à reserva de vaga e política de cotas, quando aplicável ao caso. Dados necessários ao cumprimento de obrigação legal ou regulatória e políticas públicas.
Usuários de serviços	Dados para identificação, dados necessários ao uso do serviço.

1.7.4 COMO COLETAMOS SEUS DADOS PESSOAIS

Pelo cadastro do usuário: os seus dados normalmente são coletados quando você preenche os campos de cadastro em algum dos nossos sistemas ou formulários;

Por meio de outros bancos de dados da administração pública: alguns dos dados podem ser coletados por meio de API (Application Program Interface) de banco de dados de sistemas de outros órgãos ou entidades da administração pública;

Por meio de cookies: também coletamos dados por meio de cookies, que são pequenos arquivos de texto enviados pelo site ao computador do usuário e que nele ficam armazenados. Assim, dados sobre o dispositivo utilizado pelo usuário, bem como o local e horário de acesso ao site, podem ser eventualmente armazenados.

Pela navegação do usuário nos nossos sites: também coletamos dados quando o usuário (i) utiliza os nossos serviços; (ii) preenche formulários, faz comentários, participa de votações, eventos online e sorteios, realiza buscas e demais interações nos nossos serviços; e (iii)

acessa nossos serviços pelo seu computador, telefone celular, smart TV e/ou outro dispositivo de acesso. Os dados coletados a partir do acesso aos serviços incluem: localização aproximada (latitude e longitude); endereço de IP; informações do dispositivo de acesso (como identificador da unidade, identificador de publicidade, nome e tipo de sistema operacional); informação da conexão de internet; tipo do navegador e as páginas e conteúdos que o usuário acessa em nossos serviços.

1.7.5 COMO USAMOS OS SEUS DADOS

Todos os dados solicitados pelo IFPE estão relacionados com os serviços de educação pública prestados e são utilizados para aperfeiçoar esses serviços e o desenvolvimento de novos serviços que sejam do interesse do usuário. Vejamos alguns exemplos:

- Estudantes: para a realização de políticas de assistência estudantil e iniciação científica; garantia do processo de ensino-aprendizagem e do tripé ensino-pesquisa-extensão do IFPE;
- Servidores: para o cumprimento de obrigações trabalhistas; controle de suas atividades laborais; verificação do atendimento a requisitos previstos na legislação para sua nomeação; atendimento de obrigações legais de natureza administrativa;
- Colaboradores terceirizados e estagiários: para o cumprimento de obrigações legais; controle de segurança; controle de suas atividades laborais.

Em razão da prestação dos serviços, o IFPE coleta e realiza o tratamento de dados pessoais de menores de idade. Nessa hipótese, o tratamento de dados pessoais é sempre realizado no melhor interesse dos menores de idade, nos termos da legislação aplicável.

1.7.6 COM QUEM COMPARTILHAMOS OS SEUS DADOS

O compartilhamento da base de dados poderá ser feito dentro dos limites e propósitos das atividades legais do IFPE. Assim, as bases poderão ser fornecidas e disponibilizadas para acesso e/ou consulta de órgãos ou entidades da administração pública, para cumprimento de obrigação legal ou regulatória ou para execução de políticas públicas.

O IFPE poderá, quanto às ordens judiciais de pedido de informações, compartilhar informações necessárias para investigações e tomar medidas relacionadas a atividades ilegais, suspeitas de fraude ou ameaças potenciais contra pessoas, bens ou sistemas que sustentam o serviço, bem como outras medidas necessárias para cumprir as obrigações legais. Caso ocorra o compartilhamento de informações, o IFPE notificará os titulares dos dados, salvo quando o processo estiver em segredo de justiça.

1.7.7 COMO PROTEGEMOS SEUS DADOS

O IFPE se compromete a aplicar boas práticas de segurança alinhadas aos padrões técnicos e regulatórios exigidos. Assim, buscamos proteger seus dados de possíveis vulnerabilidades.

No entanto, é importante ressaltar que nenhum sistema é completamente inviolável. Por isso, o IFPE se empenha em implementar políticas e medidas para preservar seus dados contra acesso, uso, alteração, divulgação ou destruição não autorizados, que incluem: proteção física e lógica dos ativos, ou seja, os sistemas internos têm o controle e registro de acesso individualizado, inclusive por meio de perfis específicos; exigência de login e senha, inclusive para acesso às estações de trabalho; cópias de segurança periódicas; comunicações criptografadas; registros de eventos; rastreabilidade e salvaguarda de *logs*; gestão sobre os acessos; soluções de segurança de redes (como firewalls e balanceadores de carga); cláusulas de responsabilidade nos contratos firmados com empresas e colaboradores que tratam dados pessoais pelo IFPE.

O IFPE se exime de responsabilidades por culpa exclusiva de terceiro, como em caso de ataques externos, ou por culpa exclusiva do usuário, como no caso em que ele mesmo transfere seus dados a terceiro. A instituição se compromete, ainda, a comunicar o usuário em prazo adequado caso ocorra algum tipo de violação da segurança de seus dados pessoais que possa gerar um alto risco para seus direitos e liberdades pessoais.

1.7.8 COOKIES

Cookies são pequenos arquivos de texto que os sites salvam no dispositivo enquanto o usuário navega. Trata-se de uma ferramenta importante para fornecer uma grande quantidade de informações sobre a atividade online dos usuários. Podem ser armazenados, por exemplo, dados sobre o dispositivo utilizado pelo usuário, bem como local e horário de acesso ao site.

Os cookies podem armazenar uma grande quantidade de dados, sendo alguns destes suficientes para identificar o titular de dados pessoais. Nesse cenário, e considerando o disposto na LGPD, não é indicado utilizar cookies sem hipótese legal que considere a prévia autorização do usuário ou qualquer outra hipótese que respalde a coleta de cookies, estando os sites obrigados a avisar sobre a utilização de cookies e informar a respeito de quais dados pessoais são coletados e armazenados, e para qual finalidade.

As informações eventualmente armazenadas em cookies também são consideradas dados pessoais, e todas as regras previstas neste Aviso de Privacidade também são aplicáveis a eles.

1.7.9 TRATAMENTO POSTERIOR DOS DADOS PARA OUTRAS FINALIDADES

Informações sobre os dispositivos, como modelo do hardware, tipo de sistema operacional, navegador utilizado para o acesso e identificador do dispositivo (incluindo a localização), podem ser coletados para a melhoria contínua dos serviços e aprimoramento da experiência do usuário no âmbito do IFPE.

Dados anonimizados ou pseudonimizados podem ser compartilhados como dados abertos, para fins de pesquisa e geração de estatísticas, podendo ser utilizados de maneira agregada na divulgação de informações por meios de comunicação e em publicações científicas e educacionais.

A transparência será proporcionada nos termos da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), e do Decreto nº 7.724, de 16 de maio de 2012.

1.7.10 MUDANÇA DO TERMO DE USO E AVISO DE PRIVACIDADE

Este Termo de Uso e Aviso de Privacidade tem validade indeterminada, mas está sujeito a alterações sem aviso prévio. O IFPE se reserva o direito de modificar esse documento a qualquer momento, especialmente para melhor adequá-lo à legislação vigente e adaptá-lo às evoluções dos serviços, seja pela disponibilização de novas funcionalidades, seja pela eliminação ou modificação daquelas já existentes.

Qualquer alteração ou atualização deste Termo de Uso e Aviso de Privacidade passará a vigorar a partir da data de sua publicação no site institucional do IFPE e deverá ser integralmente observada pelos usuários. Portanto, recomenda-se que o site seja periodicamente acessado.

1.7.11 INFORMAÇÕES PARA CONTATO

Sempre que desejar, você poderá entrar em contato pelo e-mail controladoria@reitoria.ifpe.edu.br ou por meio da Plataforma Fala.BR para esclarecer quaisquer dúvidas sobre este Termo de Uso e Aviso de Privacidade ou para obter as informações previstas no art. 18 da LGPD.

1.7.12 FORO

Quaisquer disputas ou controvérsias oriundas de quaisquer atos praticados no âmbito da utilização dos sites e/ou aplicativos, inclusive com relação ao descumprimento deste Termo de Uso e Aviso de Privacidade ou à violação dos direitos da administração pública federal, de outros usuários ou de terceiros, inclusive direitos de propriedade intelectual, de sigilo e de personalidade, serão processadas pela Justiça Federal Seção Judiciária de Pernambuco.

Sem prejuízo de qualquer outra via de recurso administrativo ou judicial, você tem direito de apresentar reclamação à Autoridade Nacional de Proteção de Dados (ANPD), com base no art. 18, § 1º, da LGPD, caso entenda que este Termo tenha sido violado.

Versão 1.0 Última atualização: 21 de novembro de 2024.

> Checklist para verificação de POLÍTICA DE PRIVACIDADE (ou documento similar)

#	Verificar se	S/N	Observações/evidências
1	Existe uma política de privacidade (ou instrumento equivalente) estabelecida	SIM	Termo de Uso e Aviso de Privacidade
2	A política de privacidade foi publicada para as	SIM	Será publicado no site do

	partes interessadas (públicos interno e externo)		IFPE e nos sistemas controlados pelo IFPE
3	A política de privacidade informa o titular de dados sobre os princípios aplicáveis ao tratamento de dados pessoais	SIM	Item 1.7.1 Sobre a Lei Geral de Proteção de Dados
4	A política de privacidade fornece informações sobre o controlador, o operador e o encarregado	SIM	1.7.2 Contatos
5	A política de privacidade informa como se dá a custódia de dados pessoais	SIM	1.7.7 Como protegemos seus dados
6	A política de privacidade informa sobre como o titular de dados pode obter as informações previstas no art. 18 da LGPD, quando aplicáveis	SIM	1.7.11 Informações para contato
7	A política de privacidade informa sobre como o titular de dados pode exercer seus direitos	SIM	1.7.12 Foro
8	A política de privacidade informa quais são as hipóteses em que, no exercício de suas competências, a organização realiza o tratamento de dados pessoais	SIM	1.7.3 Quais dados são tratados 1.7.5 Como usamos os seus dados
9	A política de privacidade fornece informações claras sobre a previsão legal, a finalidade, as informações de contato do controlador, os procedimentos e as práticas utilizadas no tratamento de dados	SIM	Termo de Uso e Aviso de Privacidade
10	A política de privacidade fornece informações acerca do uso compartilhado de dados pelo controlador e sua finalidade	SIM	1.7.6 Com quem compartilhamos os seus dados
11	A política de privacidade informa a data de sua última atualização	SIM	Versão 1.0 Última atualização: xx de xxxxx de 2024

ANEXO II

Procedimento: Procedimento de Comunicação de Incidentes de Segurança da Informação
Macroprocesso: (4) Avaliação, Monitoramento, Controle e Integridade.
Processo: (04.09) Proteção de Dados
Serviço: (04.09.02) Tratamento de Dados
Atividade/Assunto/Iniciativa: Comunicação de Incidentes de Segurança da Informação

Versão	Data	Autor/es
1.0	**26/06/2024**	Encarregada de dados pessoais do IFPE, Maria Dayana Lopes de Oliveira, e diretor de Tecnologia de Informação, Jobson Tenório do Nascimento
1.1	**06/09/2024**	Encarregada de Dados Pessoais do IFPE - Maria Dayana Lopes de Oliveira

I – OBJETIVO DO PROCEDIMENTO

Apresentar orientações com o intuito de auxiliar os servidores responsáveis pelo tratamento de incidentes de segurança da informação, bem como o/a encarregado/a pelo tratamento de dados pessoais no IFPE, a realizar a comunicação de incidentes de segurança da informação no âmbito institucional.

Observação: O escopo desse procedimento são os incidentes de segurança com dados pessoais, isto é, qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, que possa ocasionar risco para os direitos e liberdades do titular dos dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração, vazamento ou, ainda, qualquer forma de tratamento de dados inadequada ou ilícita.

II.A – BASE NORMATIVA

- Lei n° 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD);
- Resolução CD/ANPD nº 15, de 24 de abril de 2024 - Aprova o Regulamento de Comunicação de Incidente de Segurança.

II.B – BASE AUXILIAR

- *Guia de Resposta a Incidentes de Segurança*

III – OPERACIONALIZAÇÃO

1. **Avaliação interna do incidente;**
2. **Comunicação ao/à encarregado/a;**
3. **Comunicação aos titulares de dados;**
4. **Comunicação à ANPD;**
5. **Elaboração de relatório.**

1. **Avaliação interna do incidente**

1.1 Essa avaliação prévia, feita pela Diretoria de Tecnologia da Informação – DTI, tem como objetivo obter informações iniciais sobre o impacto do evento; natureza, categoria e quantidade de titulares de dados pessoais afetados; categoria e quantidade de dados afetados, consequências do incidente para os titulares e a entidade, criticidade e probabilidade. Além disso, é necessário preservar todas as evidências do incidente.

2. **Comunicação ao/à encarregado/a**

2.1 Após avaliação interna do incidente, a DTI deve comunicar o mais rápido possível, por e-mail, ao/à encarregado/a do IFPE a existência do incidente, caso envolva dados pessoais, para que ele/a tome as providências previstas na LGPD e no portal da ANPD sobre comunicação de incidentes de segurança.

3. **Comunicação aos titulares de dados;**

3.1 A comunicação aos titulares de dados, pela DTI, deve ser realizada em até 3 dias úteis, uma vez que seja constatado que o incidente pode causar risco ou dano relevante aos titulares. Isso permite aos titulares mitigarem eventuais impactos negativos decorrentes do incidente.

3.2 O incidente de segurança pode acarretar risco ou dano relevante aos titulares quando puder afetar significativamente interesses e direitos fundamentais dos titulares e, cumulativamente, envolver, pelo menos, um dos seguintes critérios:

I - dados pessoais sensíveis;
II - dados de crianças, de adolescentes ou de idosos;
III - dados financeiros;
IV - dados de autenticação em sistemas;
V - dados protegidos por sigilo legal, judicial ou profissional; ou
VI - dados em larga escala.

3.3 A comunicação deve ser feita de forma individual e diretamente aos titulares, sempre que possível (por meio do e-mail institucional).

3.4 Excepcionalmente, e de forma justificada, pode ser feita a comunicação indireta por meio de publicação em meios de comunicação.

3.5 O comunicado aos titulares deve fazer uso de linguagem clara e conter, ao menos, as seguintes informações:
- resumo e data da ocorrência do incidente;
- descrição dos dados pessoais afetados;
- riscos e consequências aos titulares de dados;
- medidas tomadas pelo/a controlador/a e as recomendadas aos titulares para mitigar os efeitos do incidente, se cabíveis;
- dados de contato do/a encarregado/a do/a controlador/a para que os titulares possam solicitar informações adicionais a respeito do incidente;

- os motivos da demora, no caso de a comunicação não ter sido feita no prazo de até 3 dias úteis.

3.6 Verificar o exemplo de comunicação por e-mail aos titulares de dados (Anexo A).
Obs.: Nesse exemplo, não foi possível determinar a data da ocorrência do incidente.

4. **Comunicação à ANPD**

4.1 A comunicação de incidentes de segurança à Autoridade Nacional de Proteção de Dados (ANPD) deve ser realizada em até 3 dias úteis pelo/a encarregado/a do IFPE em parceria com a DTI. O prazo será contado do conhecimento pelo/a controlador/a de que o incidente afetou dados pessoais.

4.2 As informações poderão ser complementadas, de maneira fundamentada, no prazo de 20 dias úteis, a contar da data da comunicação à ANPD.

4.3 A comunicação se dará por meio do preenchimento de formulário, que deverá ser protocolado por peticionamento eletrônico através do sistema SUPER, da ANPD: (https://anpd-super.mj.gov.br/sei/controlador_externo.php?acao=usuario_externo_logar&acao_origem=usuario_externo_logar&id_orgao_acesso_externo=0)

4.4 O/a encarregado/a deverá se cadastrar prévia e corretamente nos sistemas da ANPD.

4.5 Para comunicar um incidente de segurança, selecione, no menu esquerdo "Processo novo", em "Peticionamento", e, em seguida, o tipo de processo "ANPD – Comunicados de Incidentes à Autoridade Nacional de Proteção de Dados".

4.6 O formulário deve ser preenchido por um servidor da DTI e enviado por e-mail para o/a encarregada/o juntamente com as evidências de comunicação do incidente aos titulares dos dados. O formulário pode ser consultado através do seguinte link: Formulário ANPD de comunicação de incidente .

4.7 A cada novo peticionamento na ANPD deve ser anexada a portaria de designação do/a encarregado/a.

5. **Elaboração do Relatório**

5.1 O IFPE deverá manter o registro do incidente de segurança, inclusive daquele não comunicado à ANPD e aos titulares, pelo prazo mínimo de 5 anos, contado a partir da data do registro, exceto se constatadas obrigações adicionais que demandem maior prazo de manutenção.

5.2 O relatório, elaborado pela/o encarregado/a, deverá conter, no mínimo:

I - a data de conhecimento do incidente;
II - a descrição geral das circunstâncias em que o incidente ocorreu;
III - a natureza e a categoria de dados afetados;
IV - o número de titulares afetados;
V - a avaliação do risco e os possíveis danos aos titulares;
VI - as medidas de correção e mitigação dos efeitos do incidente, quando aplicável;
VII - a forma e o conteúdo da comunicação, se o incidente tiver sido comunicado à ANPD e

aos titulares; e
VIII - os motivos da ausência de comunicação, quando for o caso.

5.3 É importante que todas as informações e evidências coletadas e as ações do processo de tratamento de incidente de segurança à proteção de dados sejam documentadas, de modo a possibilitar a elaboração de um relatório final do incidente. Esse documento deve: a) conter as devidas considerações para a promoção da melhoria contínua dos processos de tratamento de incidentes; e b) estar disponível para consulta, em caso de atualização do relatório de impacto a proteção de dados (RIPD).

5.3 O modelo de relatório consta no Anexo B, e os relatórios serão divulgados por meio de processo SEI aberto anualmente.

5.3.1 Deve ser inserida como anexo do relatório a comprovação de comunicação aos titulares de dados. Para inserção no SEI, o arquivo deve estar no formato PDF ou compactado (ZIP), seguindo o procedimento de inclusão de um novo documento externo.

Ano	Processo SEI
2024	**23294.013464/2024-47**
202x	xxxxxxxxxx

ANEXO A - Exemplo de comunicação por e-mail aos titulares de dados

Prezado/a,

1. De acordo com informações recebidas de organização parceira, identificamos que suas credenciais (usuário e senha) em {{urls_sistemas}} podem ter sido comprometidas.

2. As contas podem ter sido comprometidas devido a infecções por vírus de computador, ataque de *phishing* ou outras atividades maliciosas.

3. Com a posse das suas credenciais comprometidas, terceiros podem acessar/alterar suas informações pessoais ou agir em seu nome.

4. Por precaução, já alteramos as senhas comprometidas no domínio IFPE.

5. Recomendamos:
- Trocar suas senhas assim que possível, incluindo outras credenciais pessoais, caso utilize a mesma senha em outros sistemas;
- Utilizar a verificação em duas etapas (https://cartilha.cert.br/) em todos os sistemas sempre que possível;

- Sempre manter seus dispositivos atualizados e com medidas adicionais de segurança, como, por exemplo, antivírus;
- Não executar programas recebidos como anexos de e-mails desconhecidos;
- Não preencher formulários recebidos por e-mail solicitando informações pessoais ou senhas.

Caso tenha alguma dúvida, entre em contato com a encarregada pelo Tratamento de Dados Pessoais no IFPE através do e-mail controladoria@reitoria.ifpe.edu.br .

Atenciosamente,

ANEXO B - Exemplo e Modelo de Relatório de Incidentes de Segurança da Informação

RISI nº 01/2024	
Descrição do incidente	Credenciais de acesso (usuários e senhas) de sistemas e de e-mails do IFPE comprometidas
Origem e data de conhecimento do incidente	O Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) enviou e-mail para cri.dadt@reitoria.ifpe.edu.br no dia 7/5/2024 notificando sobre possíveis comprometimentos das credenciais de sistemas do IFPE. O Centro Integrado de Segurança Cibernética do Governo Digital (CISC Gov.br) enviou e-mail para netadmin@ifpe.edu.br no dia 15/4/2024 notificando sobre possíveis comprometimentos das credenciais dos e-mails dos *campi* do IFPE.
Dados afetados	Dados pessoais não sensíveis: e-mail, CPF, SIAPE e senha.
Número de titulares afetados	Foram enviados 445 e-mails, porém nesse quantitativo pode haver titulares replicados por constarem diferentes sistemas.
Avaliação do risco e os possíveis danos aos titulares	Com a posse das credenciais possivelmente comprometidas, terceiros podem acessar/alterar informações pessoais dos titulares dos dados ou agir em seu nome.
Medidas de correção e mitigação dos efeitos do incidente, quando aplicável	Através da notificação aos titulares de dados foram apresentadas recomendações/orientações que podem evitar o comprometimento de suas credenciais.
Comunicação do incidente aos titulares de dados	Em relação aos possíveis comprometimentos das credenciais dos e-mails dos *campi* do IFPE, a notificação foi repassada, por e-mail, no dia 16/4/2024 para as Coordenações de Gestão de Tecnologia da Informação dos

	campi para que comunicassem aos titulares dos dados. Quanto aos possíveis comprometimentos das credenciais dos sistemas do IFPE, a notificação foi repassada, por e-mail individualizado, no dia 5/6/2024 aos titulares de dados.
Comunicação do incidente à ANPD	https://anpd-super.mj.gov.br/sei/controlador_externo.php?acao=usuario_externo_logar&id_orgao_acesso_externo=0 **Processo:** **00261.004018/2024-95** **Tipo:** ANPD: Comunicados de Incidentes à Autoridade Nacional de Proteção de Dados **Data de Geração: 7/6/2024** **Interessados:** Maria Dayana Lopes de Oliveira
Motivo da ausência de comunicação, quando for o caso	O incidente não foi comunicado tempestivamente aos titulares de dados nem à ANPD porque não tínhamos um procedimento automatizado de troca de credencial, de confirmação de sua validade e de notificação por e-mail. Além disso, a encarregada pelo tratamento de dados pessoais no IFPE foi designada recentemente, e foi a primeira vez que esta realizou essa comunicação de incidentes.