INSTITUTO FEDERAL
Espírito Santo

Relatório Final de Auditoria nº 03/2024

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

2024

SUMÁRIO

I PLANEJAMENTO DOS TRABALHOS DE AUDITORIA

O presente trabalho trata do planejamento e operacionalização das Atividades de Auditoria Interna e tem por objetivo avaliar a aplicação da Lei Geral de Proteção de Dados Pessoais no âmbito do Instituto Federal do Espírito Santo (Ifes). A realização desta ação de auditoria está prevista no Plano Anual de Auditoria Interna (Paint) 2024 do Ifes, aprovado pelo Conselho Superior do Ifes.

1.1 Análise preliminar do objeto de auditoria

A Lei Geral de Proteção de Dados Pessoais (LGPD) representa um marco legal importante no Brasil, estabelecendo diretrizes claras para o tratamento de dados pessoais por instituições públicas e privadas. No âmbito do Instituto Federal do Espírito Santo (Ifes), a aplicação desta lei é de extrema relevância, considerando que a instituição lida diariamente com um grande volume de dados pessoais, especialmente de menores de idade, que constituem o maior público atendido pela instituição.

A proteção dos dados pessoais dos estudantes e demais membros da comunidade acadêmica é fundamental para garantir a privacidade e a segurança dessas informações, evitando o uso indevido ou o acesso não autorizado a dados sensíveis. A importância da LGPD no Ifes é ainda mais evidente quando se considera que a maior parte dos alunos são menores de idade, o que exige um cuidado redobrado no tratamento de suas informações pessoais, em conformidade com as exigências legais.

Inclusive o TCU ao realizar uma auditoria para avaliar a aderência das organizações públicas federais às diretrizes estabelecidas pela Lei Geral de Proteção de Dados - LGPD, enfatizou em seu **Acórdão nº 1384/2022 – Plenário** que instituições que realizam tratamento de dados pessoais de menores e adolescentes devem implementar controles internos mais rigorosos, a fim de se evitar o vazamento desses dados, in verbis:

> 56. A partir das respostas ao questionário, constatou-se que a maioria das organizações, 77% (31% não identificaram e 46% identificaram parcialmente), ainda não identificou todas as categorias de titulares de dados pessoais com os quais mantém relacionamento.

> 57. A identificação dessas categorias é importante para auxiliar as organizações a planejarem os controles que serão implementados levando em consideração as diferentes partes interessadas. **Por exemplo, organizações que realizam tratamento de dados de crianças e adolescentes devem implementar controles mais rigorosos nos processos que realizam o tratamento destes dados.**

A proteção de dados pessoais já estava implicitamente garantida pela Constituição da República Federativa do Brasil, uma vez que o artigo 5º assegura os direitos fundamentais à liberdade, privacidade, intimidade, honra e imagem. Esses direitos incluem a proteção contra violações que possam gerar danos materiais ou morais, o que refletia a base para a tutela dos dados pessoais.

Com a promulgação da Emenda Constitucional (EC) 115/2022, o direito à proteção de dados pessoais foi explicitamente incluído no rol dos direitos e garantias fundamentais. A emenda também atribuiu à União a competência privativa para legislar sobre proteção e tratamento de dados pessoais, proporcionando maior segurança jurídica à aplicação da Lei Geral de Proteção de Dados (LGPD). Isso reforça a proteção dos dados pessoais como um direito fundamental que a LGPD regulamenta de forma específica.

Portanto, a implementação da LGPD no Ifes não só cumpre uma exigência legal, mas também protege direitos constitucionais fundamentais dos alunos e demais membros da comunidade acadêmica. A instituição, ao adotar práticas que asseguram a conformidade com a LGPD, contribui para a construção de um ambiente educacional seguro e respeitador dos direitos de seus estudantes, especialmente aqueles que estão em fases mais vulneráveis da vida, como os menores de idade. Dessa forma, o Ifes reafirma seu compromisso com a proteção da privacidade e a dignidade de todos os seus membros, em consonância com os valores constitucionais brasileiros.

1.1.Objetivos e Escopo

1.1.1. Objetivo Geral

Avaliar a conformidade do IFES com os requisitos da LGPD, identificando potenciais riscos e áreas que necessitam de melhorias.

1.1.2. Objetivos Específicos e Escopo

Objetivo 1: Verificar o nível de adequação dos processos de tratamento de dados pessoais analisando a estrutura de governança para a proteção de dados pessoais no IFES. Verificar se houve a devida nomeação e atribuição de responsabilidades do Encarregado pelo Tratamento de Dados Pessoais pelo Ifes, conforme exigido pelos normativos vigentes.

Escopo: **1.1 Análise da Estrutura de Governança para a Proteção de Dados Pessoais:**

a) realizar o levantamento e estudo dos documentos institucionais relacionados ao tema, ou seja, verificar se há políticas, regulamentos, organogramas e demais documentos que definem a governança de dados no Ifes;
b) verificar se existem comitês ou grupos de trabalho específicos para a proteção de dados, suas funções e atribuições;
c) verificar se o Ifes estabeleceu e mapeou todos os processos que realizam o tratamento de dados pessoais, identificando responsáveis, atividades, dados manipulados e compartilhamentos de dados;
d) verificar se o Ifes realizou a identificação e análise de riscos, e se há um plano de resposta a incidentes relacionados à violação de dados pessoais; e
e) verificar se há nomeação oficial do Encarregado pelo Tratamento de Dados Pessoais, no DOU conforme exigido pela Instrução Normativa SGD/ME nº 117/2020 e verificar se houve a divulgação de forma clara e acessível das informações de contato do Encarregado no site institucional do Ifes.

Objetivo 2: Verificar se os processos eletrônicos do Ifes que contenham dados pessoais sensíveis estão em consonância com os critérios de sigilo estabelecidos pela LGPD.

Escopo: Utilizar o método não probabilístico para selecionar uma amostra de 23 processos eletrônicos no SIPAC que possam conter dados pessoais referentes aos alunos e informações relacionadas à saúde dos servidores e verificar se há dados sensíveis expostos.

1.2. Técnicas de Auditoria

Para a realização dos exames, foram aplicados procedimentos de rotina, também conhecidos como testes de auditoria, a fim de se obter resultados conclusivos sobre o objeto

analisado. Segundo a Resolução nº 780/98, do Conselho Federal de Contabilidade (CFC), os testes de auditoria subdividem-se em duas espécies:

a) Testes de observância – têm por finalidade verificar a segurança dos controles internos estabelecidos, quanto ao seu efetivo funcionamento e a sua aderência às normas em vigor.

b) Testes substantivos – objetivam comprovar a suficiência, exatidão e validade das informações produzidas, seja em sua totalidade ou por amostragem.

1.3. Legislação e normas aplicadas

Os trabalhos serão realizados em conformidade com a legislação e as normas vigentes abaixo relacionadas:

- **Constituição da República Federativa do Brasil de 1988** - Lei fundamental e suprema do Brasil, servindo de parâmetro de validade a todas as demais espécies normativas, situando-se no topo do ordenamento jurídico;

- **Lei n° 11.892, de 29 de dezembro de 2008** - Institui a Rede Federal de Educação Profissional, Científica e Tecnológica, cria os Institutos Federais de Educação, Ciência e Tecnologia, e dá outras providências;

- **Lei nº 12.527, de 18 de novembro de 2011** - Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.

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

- **Instrução Normativa SGD/ME nº 117 de 19 de novembro de 2020** - Dispõe sobre a indicação do Encarregado pelo Tratamento dos Dados Pessoais no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional;

- **Portaria SGD/MGI nº 852 de 28 de março de 2023 -** Dispõe sobre o Programa de Privacidade e Segurança da Informação - PPSI;

- **Resolução CD/ANPD nº 18 de 16 de julho de 2024 -** Aprova o regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais;

- **Acórdão nº 1384/2022 – TCU – Plenário** - Auditoria para avaliar a aderência das organizações públicas federais às diretrizes estabelecidas pela Lei Geral de Proteção de Dados - LGPD;

- **Guia de Elaboração de Programa de Governança em Privacidade, Versão 2.2 - 2024 -** Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos.

1.4. Riscos significativos

O objetivo da avaliação de riscos consiste em formar uma base prévia para o desenvolvimento de estratégias (resposta ao risco) e de como os mesmos serão administrados, de modo a diminuir a probabilidade de ocorrência e/ou a magnitude do impacto. A avaliação de riscos é feita por meio de análises qualitativas e quantitativas, ou da combinação de ambas.

No âmbito do Ifes, a partir da publicação da Política de Gestão de Riscos por meio da Resolução CS nº 27/2021 e da atualização da Matriz de Riscos constante no documento Gestão de Riscos do Ifes 2º Ciclo | 2024-2026, observou-se que o Instituto identificou alguns riscos relacionados ao tema ora auditado, conforme tratado no próximo tópico deste relatório. Os riscos identificados pelo Ifes são:

a) vazamento de dados pessoais e ou dados sigilosos do inventor;
b) publicação de informações pessoais dos envolvidos em documentos referentes aos Termos de Parcerias no site da Proex, o que pode comprometer a privacidade e segurança deste;
c) não ter a implementação de ações de capacitação para os servidores da Instituição;
d) não garantia dos direitos do usuário; e
e) formas inadequadas de obtenção e registro de evidências e a falta de tratamento de dados e informações de acesso restrito ou sigiloso.

Sendo assim, tendo por base os riscos já identificados pela Gestão do Ifes e ainda os conhecimentos adquiridos por esta Unidade de Auditoria Interna ao debruçar-se sobre o tema,

foram destacados como principais riscos os que seguem abaixo, os quais serão abordados no presente trabalho.

1. Divulgação ou vazamento de dados pessoais que comprometam servidores, alunos e demais usuários bem como comprometam a imagem do Ifes;

2. Responsabilização em face de ações judiciais movidas pelos titulares de dados em decorrência de violações da LGPD resultando em indenizações e responsabilização do Ifes;

3. Aplicação de sanções pela ANPD (advertências, multas, etc.) devido ao descumprimento de normas da LGPD.

Identificação de Eventos de Riscos		**Análise dos Riscos**			
Nº	**EVENTO DE RISCO**	**PROBABILIDADE INERENTE**	**IMPACTO INERENTE**	**/ERIDADE DO RISCO**	**DIDA DE RISCO INERENTE**
01	Divulgação ou vazamento de dados pessoais que comprometam servidores, alunos e demais usuários bem como comprometam a imagem do Ifes;	**Muito Provável**	**Grande**	**Risco Alto**	**16**
02	Responsabilização em face de ações judiciais movidas pelos titulares de dados em decorrência de violações da LGPD resultando em indenizações e responsabilização do Ifes;	**Provável**	**Grande**	**Risco Alto**	**12**

03	Aplicação de sanções pela ANPD (advertências, multas, etc.) devido ao descumprimento de normas da LGPD.	**Provável**	**Grande**	**Risco Alto**	**12**

TABELA DE SEVERIDADE

MATRIZ DE RISCOS				
Catastrófico	5	10	15	20	25
Grande	4	8	12	16	20
Moderado	3	6	9	12	15
Pequeno	2	4	6	8	10
Insignificante	1	2	3	4	5

Rara	Pouco provável	Provável	Muito provável	Praticamente certa
< 10%	<= 30%	<= 50%	<= 90%	

PROBABILIDADE

Tabela de Severidade	
Níveis	Pontuação
RC - Risco Crítico	13 a 25
RA - Risco Alto	7 a 12
RM - Risco Moderado	4 a 6
RP - Risco Pequeno	1 a 3

TRATAMENTO DE RISCO

Nível de Risco	Descrição do Nível de Risco	Parâmetro de Análise para Adoção de Resposta	Tipo de Resposta	ação de Controle
Risco Crítico	Indica que nenhuma opção de resposta foi identificada para reduzir a probabilidade e o impacto a nível aceitável	Custo desproporcional, capacidade limitada diante do risco identificado	**Evitar**	Promover ações que evitem/eliminem as causas e/ou consequências.
Risco Alto	Indica que o risco será reduzido a um nível compatível com a tolerância a riscos	Nem todos os riscos podem ser transferidos. Exemplo: Risco de Imagem, Risco de Reputação	**Reduzir**	Adotar medidas para reduzir a probabilidade ou impacto dos riscos, ou ambos
Risco Moderado	Indica que o risco será reduzido a um nível compatível com a tolerância a riscos	Reduzir probabilidade ou impacto, ou ambos	**Compartilhar ou Transferir**	Reduzir a probabilidade ou impacto pela transferência ou compartilhamento de uma parte do risco. (seguro, transações de hedge ou terceirização da atividade).
Risco Pequeno	Indica que o risco inerente já está dentro da tolerância a risco	Verificar a possibilidade de retirar controles considerados desnecessários	**Aceitar**	Conviver com o evento de risco mantendo práticas e procedimentos existentes

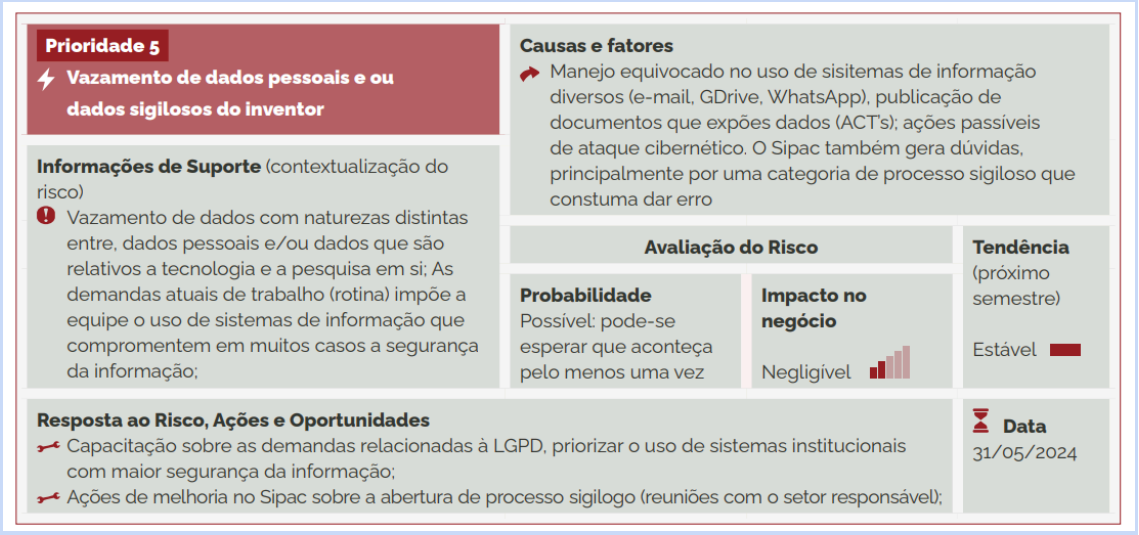
1.5. Adequação e a eficácia dos processos de governança, de gerenciamento de riscos e de controles internos da Unidade Auditada.

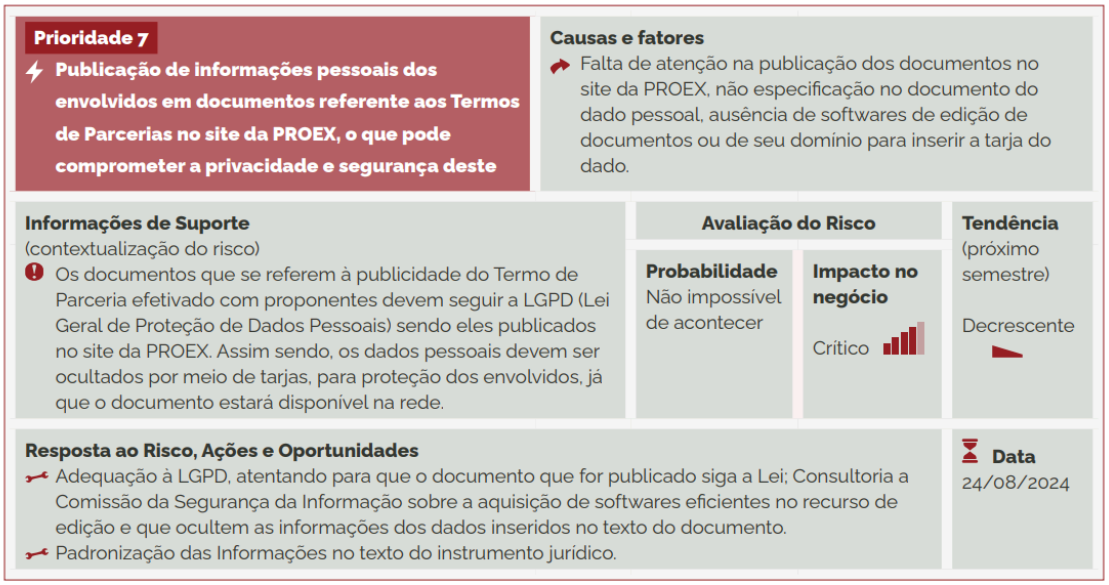
Com relação ao Gerenciamento de Riscos, consta na IN conjunta CGU-MP nº 01/2016 que se trata do "processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer razoável certeza quanto ao alcance dos objetivos da organização" bem

como ao Decreto nº 9.203/2017 que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional.

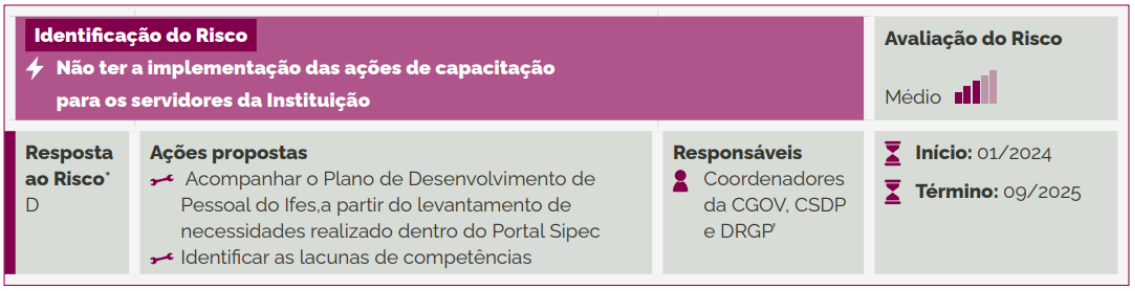
Quanto ao gerenciamento de riscos o Ifes possui, desde 2021, a Política de Gestão de Riscos instituída por meio da Resolução Consup nº 27/2021, e tem por objetivo estabelecer princípios, diretrizes, governança e responsabilidades a serem observadas no processo de gestão de riscos no Ifes. Como desdobramento da referida política, foi construída uma Matriz de Risco de todas as Pró-Reitorias e dos setores vinculados ao Gabinete do Reitor do Ifes, na qual foram traçados os principais riscos inerentes a cada setor e demais informações correlatas, essa Matriz foi recentemente atualizada, recebendo o nome de Gestão de Riscos do Ifes 2º Ciclo | 2024-2026.

Na Matriz de Riscos da Pró-Reitoria de Extensão foram identificados dois riscos relacionados diretamente ao tema: ‘vazamento de dados pessoais e ou dados sigilosos do inventor”; e “Publicação de informações pessoais dos envolvidos em documento referentes ao Termos de Parcerias no site da Proex, o que pode comprometer a privacidade e segurança deste.”



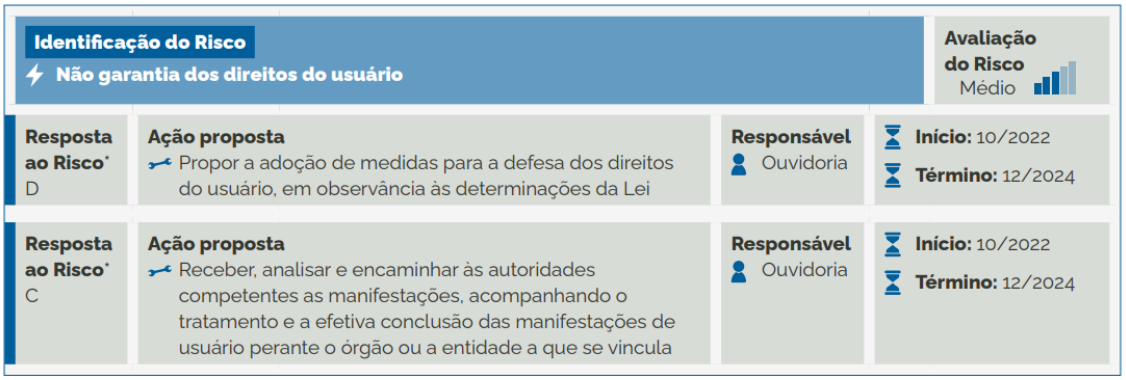


Na Matriz de Riscos da Pró-Reitoria de Desenvolvimento Institucional, mas precisamente na Diretoria de Gestão de Pessoas, foi identificado um risco que de maneira geral podemos relacionar ao tema, qual seja, "não ter a implementação de ações de capacitação para os servidores da Instituição". Esse risco pode ser relacionado ao tema auditado na medida que para adequar o Ifes à Lei Geral de Proteção de Dados Pessoais, é crucial que os servidores recebam a devida capacitação/treinamento para tal. Inclusive o TCU apontou em seu Acórdão nº 1384/2022 – Plenário que é conveniente que cada organização elabore um plano de capacitação para determinar as competências necessárias para os recursos humanos envolvidos em atividades que realizam o tratamento de dados pessoais. O referido plano deve mapear as lacunas de conhecimento associadas ao tema, bem como planejar ações de treinamento para redução dessas lacunas.

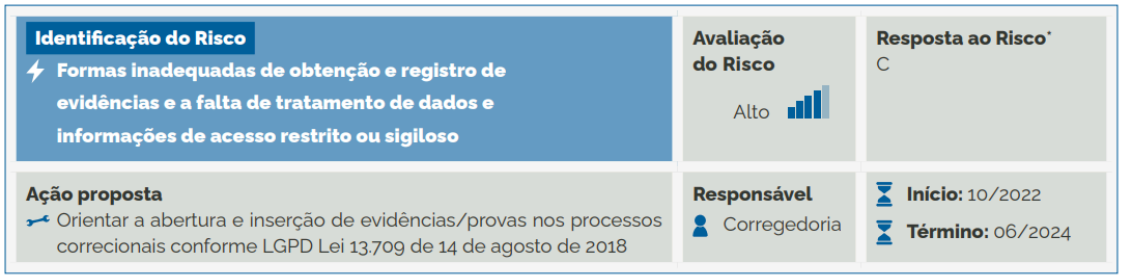


Na Matriz de Riscos do Gabinete do Reitor, encontram-se dois riscos que também podem ser relacionados ao tema, são eles: "Não garantia dos direitos do usuário" e "Formas inadequadas de obtenção e registro de evidências e a falta de tratamento de dados e

informações de acesso restrito ou sigiloso", sendo o primeiro no setor da Ouvidoria e o segundo no setor da Corregedoria, conforme verifica-se nos prints abaixo.



Ouvidoria



Corregedoria

Quanto à avaliação dos aspectos de Governança e adequação e eficácia dos controles internos foram realizadas análises de documentos institucionais, bem como testes de auditoria cujos resultados estão dispostos no Capítulo II - Execução dos Trabalhos de Auditoria.

1.6. Definição da amostra

Na realização do trabalho de auditoria, é crucial equilibrar a qualidade e a abrangência da análise com os recursos disponíveis, incluindo tempo e pessoal. Sendo assim, em função dos recursos humanos e do tempo disponíveis para a execução deste relatório, bem como para a consecução dos objetivos do presente relatório, foi selecionada uma amostra aleatória de processos eletrônicos. A amostragem seguiu critérios estabelecidos pelas Normas Internacionais para a Prática Profissional de Auditoria Interna, utilizando-se de uma técnica de **amostragem não probabilística**. Foram selecionados e analisados 23 processos eletrônicos no

período de 2021 a 2024, divididos em dois grupos: 13 processos relacionados à saúde, afastamentos ou licenças médicas de servidores e 10 processos referentes a alunos.

1.7. Programa de trabalho

Os trabalhos de avaliação foram realizados em estrita observância às normas de auditoria aplicáveis ao Serviço Público Federal e as técnicas de auditoria utilizadas foram:

- Análise processual/documental;
- Exame dos registros;
- Indagação oral ou escrita (questionário/solicitações de auditoria – SA);
- Correlação das informações obtidas;
- Consultas a sistemas informatizados: Site do Ifes, SIPAC.

1.8. Coordenação e Alocação da equipe de trabalho

A equipe de trabalho será composta da seguinte forma:

Nome	Formação	Função
Abdo Dias da Silva Neto	Direito	Supervisor
Cíntia Petri	Direito	Auditora
Rafael Barbosa Mariano	Admini	Auditor

Recursos humanos – 3 auditores

Tempo - 65 dias úteis

Total de horas trabalhadas – 912 horas

A coordenação dos trabalhos de auditoria foi designada a servidora Cintia Petri.

1.9. Papeis de trabalho

Os Papeis de Trabalho (PT's) dessa auditoria constituem um registro permanente do trabalho efetuado pela equipe de auditoria e é composto por um conjunto de documentos probatórios, registro de exames e anotações de informações que compõem as evidências obtidas ao longo da execução dos trabalhos e que contribuíram para a formação da opinião da

equipe. Essa documentação que deu suporte ao trabalho obedeceu aos seguintes preceitos básicos: lógica, concisão, correção linguística e clareza.

Assim, apresenta-se a seguir, os papeis de trabalho desta auditoria:

- E-mail contendo a resposta do Professor Presidente da Comissão designada pela Portaria nº 452/2021 responsável por definição de equipes, mapear os processos e os fluxos de trabalho que merecem tratamento para adequação à Lei Geral de Proteção de Dados Pessoais (LGPD);

- Resposta da gestão ao questionário de adequação do Ifes à Lei Geral de Proteção de Dados Pessoais;

- Prints de processos do SIPAC contendo evidências de exposição indevida de dados pessoais e;

- Planilha de dados pessoais - Ifes (no Google Drive).

II. EXECUÇÃO DOS TRABALHOS DE AUDITORIA

2.1 Análise da Estrutura de Governança para a Proteção de Dados Pessoais:

Para analisar a estrutura de Governança para a Proteção de Dados Pessoais no Ifes, foi realizado o levantamento e estudo dos documentos institucionais relacionados ao tema. O escopo era verificar:

a) se há políticas, regulamentos, organogramas e demais documentos que definem a governança de dados no Ifes;

b) se existem comitês ou grupos de trabalho específicos para a proteção de dados, suas funções e atribuições;

c) se o Ifes estabeleceu e mapeou todos os processos que realizam o tratamento de dados pessoais, identificando responsáveis, atividades, dados manipulados e compartilhamentos de dados;

d) se o Ifes realizou a identificação e análise de riscos, e se há um plano de resposta a incidentes relacionados à violação de dados pessoais; e

e) se há nomeação oficial do Encarregado pelo Tratamento de Dados Pessoais, no DOU conforme exigido pela Instrução Normativa SGD/ME nº 117/2020 e verificar se houve a divulgação de forma clara e acessível das informações de contato do Encarregado no site institucional do Ifes.

2.1.1 Comissões, comitês ou grupos de trabalho

Foram encontradas os seguintes portarias:

- Portaria Ifes nº 1, de 02 de Janeiro de 2023 que estabelece o Comitê Gestor de Segurança da Informação (CGSI);
- Portaria Ifes nº 452, de 19 de março de 2021 que designa a Comissão responsável por definição de equipes, mapear os processos e os fluxos de trabalho que merecem tratamento para adequação a Lei Geral de Proteção de Dados (LGPD) e;
- Portaria Ifes nº 1292, de 09 de maio de 2024 - Designa o Encarregado pelo Tratamento de Dados Pessoais.

A seguir serão avaliados os trabalhos realizados por esses grupos de trabalho.

2.1.2 Fluxo de Processo para Tratamento de Dados Pessoais

Identificou-se um documento intitulado **"Fluxo de Processo para o Tratamento de Dados Pessoais",** elaborado pela comissão designada pela Portaria nº 452, de 19 de março de 2021. Este documento foi criado com o objetivo de orientar e padronizar o tratamento de dados pessoais no âmbito do Instituto, garantindo a conformidade com a Lei Geral de Proteção de Dados (LGPD).

O referido documento traz orientações sobre como os dados pessoais devem ser identificados, coletados, tratados e armazenados. Neste documento consta que o Agente de Dados, ao coletar informações dos titulares, realize as seguintes ações prévias:

1. **Identificar e descrever os dados que serão coletados**: Inclui a observação dos dados que serão coletados, seu prazo de validade, e a classificação de acordo com a LGPD (dados pessoais ou dados sensíveis).
2. **Apresentar a finalidade e a forma de tratamento dos dados**: Especificar o motivo para o tratamento dos dados, que pode variar desde atender a uma

exigência legal até a realização de uma política pública, e descrever como esses dados serão processados (digital ou fisicamente).

3. **Apontar a hipótese legal para o tratamento dos dados**: Cada dado coletado deve ter uma base legal conforme as hipóteses previstas na LGPD, como consentimento do titular, cumprimento de obrigação legal, ou legítimo interesse.

Após os pré-requisitos, o documento detalha o fluxo operacional para o tratamento de dados pessoais no Ifes, dividido em etapas específicas:

1. **Organizar os dados recebidos**: Início do processo, onde os dados são organizados e documentados, considerando a hipótese legal e a finalidade do tratamento.
2. **Avaliar a forma adequada de armazenamento de dados**: Esta etapa envolve a verificação de alinhamento com as políticas internas de segurança da informação, incluindo a análise e indicação do sistema de armazenamento apropriado.
3. **Alimentar o sistema de armazenamento com os dados pessoais**: Após as avaliações, os dados são coletados e inseridos no sistema de armazenamento indicado, seguindo as diretrizes de segurança estabelecidas.
4. **Analisar e formalizar os dados tratados**: O Data Protection Officer (DPO) ou Gestor de Dados deve revisar o tratamento dos dados, garantindo a conformidade com as normas aplicáveis e propondo melhorias na proteção dos dados.
5. **Divulgar os dados tratados**: A última etapa do processo envolve a disponibilização dos dados tratados para os titulares, permitindo que estes possam solicitar modificações ou atualizações, garantindo a transparência do processo.

Ao analisar o "Fluxo de Processo para o Tratamento de Dados Pessoais" do Ifes, é possível identificar algumas possíveis falhas ou lacunas que podem comprometer a eficiência e a conformidade do processo com a LGPD. Os pontos críticos são:

O documento menciona diversas etapas do processo de tratamento de dados, mas não especifica claramente as responsabilidades de cada agente envolvido. Por exemplo, há menção ao "Agente de Dados" e ao "DPO", mas não fica claro quem exatamente são esses agentes,

suas qualificações, ou como são designados. Ressalta-se que a terminologia "Agente de Dados" utilizada no documento não parece muito acertada, pois, conforme a LGPD em seu Capítulo VI, os agentes de tratamento de dados são: o controlador, que no caso é a instituição (Ifes); o operador, que são os servidores ou até mesmo terceirizados responsáveis pela coleta e tratamento de dados; e o encarregado pelo tratamento de dados. Portanto, a terminologia "Agente de Dados" não deixa claro quem exatamente são esses agentes e quais são suas responsabilidades no processo. Essa falta de clareza pode gerar confusão na execução das tarefas, resultando em falhas no tratamento adequado dos dados pessoais.

O fluxo adotado também não estabelece mecanismos de monitoramento contínuo para verificar a conformidade com as etapas descritas e a eficácia dos controles implementados.

Não há menção específica a um plano de resposta a incidentes de segurança, como vazamentos de dados. O documento também não aborda como os incidentes devem ser reportados, investigados e solucionados. Destacamos que a ausência de um plano claro para lidar com incidentes pode resultar em respostas ineficazes a situações críticas, expondo o Ifes a sanções regulatórias e danos à reputação.

Embora o documento mencione a necessidade de consentimento do titular dos dados, não há um detalhamento sobre como esse consentimento deve ser obtido, registrado e gerido, especialmente em casos onde o titular deseja revogar o consentimento.

O documento aborda superficialmente os dados sensíveis, mas não fornece diretrizes específicas para o tratamento desses dados, que exigem proteções adicionais. Embora o documento faça referência à necessidade de alinhamento com as políticas internas de segurança da informação, ele não detalha como esse alinhamento deve ocorrer na prática ou como as outras políticas se integram ao processo de tratamento de dados.

A etapa de divulgação dos dados tratados é mencionada, mas sem detalhamento suficiente sobre como a transparência deve ser garantida e como as solicitações dos titulares serão geridas. As lacunas indicadas acima demonstram que este documento é incipiente, estabelecendo fluxos de forma muito generalizada. Dessa forma, as áreas destacadas precisam ser aprimoradas para garantir que o tratamento de dados pessoais no Ifes esteja em plena conformidade com a LGPD, minimizando riscos e fortalecendo a governança de dados na instituição.

2.1.3 Plano de Adequação do Instituto Federal do Espírito Santo à Lei Geral de Proteção de Dados

Ainda analisando a estrutura de governança para a proteção de dados pessoais no ifes, foi encontrado o **Plano de Adequação do Instituto Federal do Espírito Santo à Lei Geral de Proteção de Dados (LGPD)** também elaborado pela comissão designada pela Portaria nº 452/2021 e visa orientar o Ifes na conformidade com a LGPD, assegurando a privacidade e transparência no tratamento de dados pessoais.

O Plano estabelece as seguintes fases para a consecução da adequação às normas estabelecidas pela LGPD:

1ª- Mapeamento dos Dados Pessoais
2ª- Análise de conformidade e riscos
3ª- Governança de dados
4ª- Avaliação e monitoramento

O mapeamento dos dados pessoais é a etapa que envolve a identificação dos principais processos e a sensibilização dos servidores responsáveis pela coleta e tratamento dos dados. A análise de conformidade e riscos é outra etapa crucial, onde o Encarregado pelo Tratamento de Dados (DPO) identifica e gerencia os riscos associados ao tratamento dos dados pessoais, assegurando que medidas preventivas sejam implementadas para mitigar potenciais impactos negativos.

A terceira etapa trata da Governança de dados que se propõe a estabelecer uma estrutura organizacional robusta para gerenciar e proteger os dados pessoais no Ifes. Esta fase indica que a transparência e as boas práticas de gestão de dados devem ser incorporadas nas atividades diárias da instituição e indica que sejam realizadas atividades tais como: formalização das políticas de dados, suporte à segurança e tratamento de dados, e definição da importância dos dados para a instituição.

A quarta e última etapa prevê um processo contínuo de avaliação e monitoramento para garantir que o tratamento de dados seja executado com zelo e responsabilidade. O DPO desempenha um papel central neste processo, acompanhando o tratamento de dados, revisando e atualizando os procedimentos, e divulgando os resultados alcançados com a política de tratamento de dados.

Ao analisar o Plano de Adequação do IFES à LGPD, é possível identificar algumas possíveis falhas ou lacunas que podem comprometer a eficácia do plano e a plena conformidade com a LGPD. Abaixo estão os principais pontos de atenção:

O plano não apresenta um cronograma específico para a execução das atividades propostas em cada fase, nem define prazos para o cumprimento de cada uma dessas fases ou etapas. Sem um cronograma claro, há o risco de atrasos na implementação, o que pode resultar em não conformidade com a LGPD.

Sob esse aspecto vale ressaltar que a LGPD foi sancionada em agosto de 2018 e suas disposições começaram a valer a partir de setembro de 2020 para que houvesse tempo para que as instituições públicas se adequassem às suas exigências. A partir de agosto de 2021 as sanções administrativas previstas em lei passaram a ser aplicáveis para os órgãos que estivessem em desconformidade com a lei. Sendo assim, identifica-se que o Ifes está correndo um risco elevado de responsabilização. O plano não menciona indicadores de desempenho (Key Performance Indicators- KPIs) para medir o progresso e a eficácia das ações implementadas ao longo das fases. A falta de indicadores-chave de desempenho para medir o sucesso das atividades ou processos essenciais torna difícil avaliar se as medidas tomadas estão alcançando os resultados esperados, o que pode comprometer a capacidade de ajustar o plano conforme necessário.

Verifica-se a falta de estratégias de comunicação e treinamento, pois embora o plano mencione a necessidade de sensibilização e capacitação dos servidores, ele não detalha uma estratégia clara para comunicação interna e externa sobre as mudanças implementadas ou para treinamento contínuo dos envolvidos.

Semelhantemente ao documento Fluxo de Processo para o Tratamento de Dados Pessoais, o Plano de Adequação do Ifes à LGPD também não apresenta um plano detalhado de resposta a incidentes de segurança de dados, como vazamentos ou acessos não autorizados. A falta de um plano de resposta a incidentes pode resultar em reações lentas e ineficazes a violações de dados, aumentando o impacto negativo para a instituição e os titulares dos dados.

A governança de dados, embora mencionada, é tratada de forma genérica, sem a definição de uma estrutura específica de governança que inclua todos os níveis da organização e que se integre com outras políticas institucionais, como a segurança da informação. Essa

lacuna identificada parece ser, em parte, decorrente da delegação da criação dessa política ao Comitê Gestor de Segurança, entretanto, seria interessante que o plano de adequação incluísse diretrizes mais específicas para o desenvolvimento dessa política de governança de dados, estabelecendo por exemplo um cronograma, responsabilidades, e métodos de integração com outras políticas institucionais.

Verifica-se ainda a falta de diretrizes claras para o envolvimento da alta administração, apesar de mencionar o apoio da alta gestão como um fator condicionante, o plano não especifica como a alta administração será envolvida e responsável pela implementação das ações necessárias. A falta de envolvimento claro da alta administração pode resultar em falta de prioridade e comprometimento na implementação do plano, dificultando a sua eficácia e a conformidade com a LGPD.

O Plano de Adequação relaciona também algumas demandas ditas urgentes, essas demandas parecem ser complementares ao plano de adequação como um todo, pois tratam de ações imediatas que devem ser priorizadas para evitar riscos e garantir que as etapas subsequentes do plano possam ser implementadas de forma eficaz.

No entanto, o plano de adequação não detalha explicitamente as medidas ou o planejamento específico para tratar dessas demandas urgentes. Ele identifica as necessidades, mas não fornece um cronograma ou define responsabilidades claras para a execução dessas ações. Por exemplo:

- **Verificação de dados sensíveis**: O plano ressalta a necessidade de revisar como os dados sensíveis são divulgados nos sites institucionais e sistemas utilizados pelo Ifes, entretanto, não há detalhes sobre como e quando essa verificação será realizada, nem quem será responsável por essa tarefa.
- **Inventário de dados**: A importância do inventário é destacada, mas faltam diretrizes claras sobre como esse processo será conduzido e integrado aos outros aspectos do plano.

Essas lacunas indicam áreas onde o Plano de Adequação do Ifes à LGPD pode ser aprimorado para garantir uma implementação mais robusta e eficaz, assegurando a conformidade plena com a legislação e a proteção adequada dos dados pessoais tratados pela instituição.

2.1.4 Site Institucional

Verificou-se que no site institucional sistêmico do Ifes consta no menu lateral esquerdo um link que direciona para a página denominada “LGPD do Ifes” contendo seis seções, são elas: LGPD e as norma gerais; Integrantes; Plano de Ação do Ifes; Contato do Encarregado; e Documentos.

As segunda e terceira seções foram organizadas em blocos de pequenos tópicos onde é possível esclarecer algumas dúvidas acerca dos pontos básicos da Lei Geral de Proteção de Dados Pessoais. Na quarta seção consta o Plano de Adequação do Ifes, que já foi analisado acima. Na quinta seção nomeada de “Contado do Encarregado” não constam tais informações, conforme verifica-se na imagem abaixo:

Figura 01: Página da LGPD no Ifes - acesso em 21/08/2024

Link: Contato do Encarregado - Página 5 (ifes.edu.br)

Na sexta e última seção constam apenas links para acesso ao Plano de adequação e ao Fluxo de processos de tratamento de dados pessoais do Ifes, documentos já analisados acima. Constam também cinco Guias do governo federal que servem de orientação para a implementação de avaliação de riscos, programa de governança, termo de uso, política de privacidade e inventário de dados pessoais.

Verificou-se também no site institucional sistêmico uma página (Instituto Federal do Espírito Santo - Gestão Documental (ifes.edu.br)) que trata da **Gestão Documental do Ifes**. Ao analisar o texto disponível no site e a cartilha anexada sobre a gestão documental é possível verificar que os documentos não contêm informações específicas sobre como realizar a **classificação e o tratamento de dados pessoais** de acordo com a Lei Geral de Proteção de Dados Pessoais (LGPD).

A cartilha se concentra na classificação documental segundo os critérios do Conselho Nacional de Arquivos (Conarq), abordando como atribuir códigos de classificação aos documentos e como determinar o tempo de guarda de documentos físicos e digitais. A ênfase é colocada na organização e na preservação de documentos que têm valor para a instituição, garantindo o acesso adequado e organizado conforme a legislação de arquivos (Lei nº 8.159/1991).

Quanto à verificação se o Ifes estabeleceu e mapeou todos os processos que realizam o tratamento de dados pessoais, identificando responsáveis, atividades, dados manipulados e compartilhamentos de dados, conforme detalhado no próximo tópico, o instituto elaborou uma planilha denominada “Planilha de Inventário dados pessoais - Ifes” que apesar de conter algumas falhas, entende-se tratar de um início promissor no mapeamento dos processos que realizam o tratamento de dados pessoais.

No que concerne à verificação se o Ifes realizou a identificação e análise de riscos, e se há um plano de resposta a incidentes relacionados à violação de dados pessoais, verificamos que essa atividade trata-se da segunda etapa estabelecida no Plano de Adequação do Instituto à LGPD. Porém, conforme mencionado na análise desse Plano de Adequação, não foi apresentado um plano detalhado de resposta a incidentes de segurança de dados, como vazamentos ou acessos não autorizados. A falta de um plano de resposta a incidentes pode resultar em reações lentas e ineficazes a violações de dados, aumentando o impacto negativo para a instituição e os titulares dos dados.

E conforme informado pela gestão, o Ifes ainda não elaborou o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), que é uma obrigação importante para avaliar e mitigar os riscos associados ao tratamento de dados e também não estabeleceu procedimentos para comunicar à ANPD e ao titular dos dados a ocorrência de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares.

Assim, após análise da estrutura de governança para a proteção de dados pessoais no Ifes, verifica-se que a instituição já tomou medidas importantes, como a designação do Encarregado de Dados Pessoais, a criação de comissões e a elaboração de documentos voltados para a adequação à LGPD, incluindo o "Plano de Adequação à LGPD" e o "Fluxo de Processo para o Tratamento de Dados Pessoais". No entanto, existem diversas lacunas e pontos que precisam ser aprimorados, para fortalecer a governança de dados e garantir uma implementação bem-sucedida e contínua das diretrizes da LGPD.

2.2 Questionário de Conformidade à LGPD - IFES

Como não foram encontrados outros documentos elaborados pelo Ifes para a promoção da Governança em Proteção de Dados Pessoais, tais como: política de governança de dados; Plano de Resposta a Incidentes de Segurança; Programa de Privacidade e Segurança da Informação; Política de Classificação de Informações, etc., foi enviado um e-mail ao presidente da Comissão designada pela Portaria Ifes nº 452 de 19 de março de 2021, Prof. Gilberto Sudré, solicitando que nos informasse quais foram os trabalhos desenvolvidos e as equipes definidas para mapeamento dos processos e fluxos de trabalho que merecem tratamento para adequação à LGPD ao tempo em que esteve na Comissão.

Entretanto, o referido professor declarou, de forma restrita, não ter conhecimento sobre quem está à frente da comissão e que seu tempo de participação na mesma foi "muito curto". Tal afirmação nos causou grande estranheza, uma vez que, embora a comissão tenha de fato tido uma duração de apenas 60 dias, o mencionado professor ocupava a posição de presidente e, portanto, a incapacidade de fornecer informações acerca dos resultados dos trabalhos desenvolvidos nos pareceu incoerente.

Dessa forma, para dar seguimento a análise da Estrutura de Governança para a Proteção de Dados Pessoais no Ifes, foi necessário elaborar um questionário e enviar à Alta Administração do Ifes objetivando avaliar o nível de conformidade da instituição com a LGPD. O questionário foi elaborado com base no Acórdão nº 1384/2022 do TCU e abrangeu diferentes dimensões de adequação, buscando identificar áreas que precisam de melhorias.

Cumpre destacar que o método no qual é disponibilizado um questionário para que a Alta Gestão possa preencher as respostas que melhor refletem a situação atual do Instituto em relação a adequação à LGPD é denominado método de autoavaliação. Esse método de auditoria

também foi utilizado pelo TCU para a elaboração do Acórdão nº 1384/2022. Os resultados estão detalhados abaixo.

O Ifes elaborou um plano de adequação à LGPD, que embora seja incipiente e possua alguns pontos que carecem de melhorias, está publicado e disponível, o que demonstra compromisso com a transparência. Foi nomeado, por meio de portaria, o Encarregado de Dados que está em fase de treinamento, faltando apenas providenciar sua publicação no Diário Oficial da União (DOU) e disponibilizar as informações de contato no site institucional.

A gestão informou que **mapeou alguns dos processos que realizam o tratamento de dados pessoais**, e forneceu o link para acesso a uma planilha compartilhada do Google Drive chamada "Planilha de Inventário dados pessoais - Ifes". Nela constam informações como o custodiante do dado, qual dado é coletado e qual a sua categoria, qual **fundamento legal** e a justificativa para a sua coleta, como os dados são coletados e em quais sistemas estão armazenados, quem permite o acesso, a forma de proteção do dado e se existe consentimento do titular para o tratamento do dado.

A planilha apresentada demonstra um início promissor no mapeamento dos processos que realizam o tratamento de dados pessoais, mas ainda apresenta deficiências que precisam ser corrigidas. Foi observado que, em alguns dos processos mapeados, nem todas as informações solicitadas foram preenchidas, deixando campos em branco. Além disso, identificou-se uma prática preocupante, como no caso da planilha do CRA, onde alguns dados pessoais estão sendo armazenados em computadores de uso pessoal de servidores que atuam em regime de teletrabalho, o que pode comprometer a segurança e a proteção adequada dos dados, conforme exigido pela LGPD.

Quanto ao Registro de Atividades de Tratamento, a gestão informou que mantém logs das atividades de tratamento de dados pessoais, permitindo a identificação de quem, quando e quais dados foram acessados. A gestão informou que mantém registros dos logs do Sistema Integrado de Gestão (SIG) e de acesso às pastas da rede e caso necessário é possível gerar um relatório.

Com relação a segurança e acesso, houve uma contradição entre as respostas de duas questões. Na questão nº 15 o Ifes afirmou que adotou medidas de segurança técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados, vazamentos e outras ameaças, entretanto na questão nº 18 informou que não adotou e não pode comprovar a

implementação de medidas de segurança, técnicas e administrativas, para proteger os dados pessoais contra acessos não autorizados, destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado.

O Ifes informou que ainda não estabeleceu categorias específicas de titulares de dados pessoais, como cidadão, cliente, servidor público, representante de fornecedor e terceirizado (questão 2) e também não identificou todos os operadores que realizam o tratamento de dados pessoais em seu nome (questão 4), o que é uma falha importante, pois o controle dos operadores é essencial para assegurar a conformidade e a responsabilidade solidária prevista na LGPD.

Ainda com relação aos operadores (questão 5), a gestão informou que não foram firmados contratos adequados que estabeleçam suas responsabilidades e papeis em relação à proteção de dados pessoais. Situação que pode resultar em lacunas de responsabilidade e riscos à segurança de dados.

Na questão 8 foi perguntado se o Ifes possui uma política de proteção de dados pessoais distinta da política de privacidade e se ambas estão devidamente publicadas e disponíveis, ao que a gestão respondeu negativamente. Salienta-se que a distinção entre essas políticas é importante para definir claramente as diretrizes tanto para o público interno quanto externo.

No tocante aos Mecanismos para Atender Direitos dos Titulares, ao Plano de Resposta a Incidentes e ao Relatório de Impacto à Proteção de Dados Pessoais (RIPD) (questões 13, 14 e 17), a gestão informou que não possui.

A ausência de um **Plano de Resposta a Incidentes** compromete a prontidão da instituição em lidar com violações de dados, aumentando os riscos de danos aos titulares. A falta de **mecanismos para atender os direitos dos titulares**, por sua vez, limita a transparência e impede que os titulares possam exercer seus direitos de acesso, correção, ou eliminação de dados. O **RIPD**, por sua vez, é crucial para identificar e mitigar riscos potenciais antes que incidentes ocorram, atuando como uma ferramenta preventiva que poderia reduzir a necessidade de uma resposta reativa e garantir que os direitos dos titulares sejam respeitados de maneira proativa.

No que toca ao uso de Criptografia para proteger os dados pessoais sensíveis, o Ifes informou que não utiliza, mas que os acessos às bases de dados são restritos aos perfis que possuem acesso (questão 21). Vale salientar que embora não seja obrigatória a utilização de

Criptografia sua utilização diminui o risco de exposição indevida desses dados, especialmente no caso de dados de crianças e adolescentes.

O Ifes não adotou medidas que assegurem que os processos e sistemas sejam projetados desde a concepção em conformidade com a LGPD, seguindo os conceitos de Privacy by Design e Privacy by Default. Destaca-se que conforme o art. 46, § 2º, da LGPD os agentes de tratamento de dados devem adotar medidas de segurança desde a concepção do produto ou serviço até a sua execução.

Por fim verifica-se que não há um plano de capacitação implementado para os servidores envolvidos no tratamento de dados pessoais, o que pode resultar em falta de entendimento sobre as obrigações legais e os procedimentos a serem seguidos.

2.2.1 Análise da Exposição de Dados Pessoais em Processos Eletrônicos no SIPAC

Com o objetivo de verificar na prática a conformidade do Ifes às diretrizes da Lei Geral de Proteção de Dados Pessoais (LGPD) e avaliar se os controles implementados para a proteção dos dados pessoais manipulados pela instituição estão adequados, foi realizado um **teste de conformidade** baseado em uma amostra aleatória de processos eletrônicos. A amostragem seguiu critérios estabelecidos pelas Normas Internacionais para a Prática Profissional de Auditoria Interna, utilizando-se de uma técnica de **amostragem não probabilística**.

Foram selecionados e analisados 23 processos eletrônicos no período de 2021 a 2024, divididos em dois grupos: 13 processos relacionados à saúde, afastamentos ou licenças médicas de servidores e 10 processos referentes a alunos. Dos processos analisados, verificou-se que que apenas 6 tinham dados pessoais protegidos:

Os números dos processos analisados seguem nas tabelas abaixo:

Processos de Saúde, Afastamentos ou Licenças Médicas de Servidores
dados pessoais protegidos
.001645/2024-40
.003333/2024-97
.001308/2024-04

.001306/2024-15
.006309/2024-20

Processos de Saúde, Afastamentos ou Licenças Médicas de Servidores	
Com dados pessoais expostos	**Descrição do dado**
.000861/2022-73	ão de nascimento
.000755/2022-01	ro de CPF e RG
.001432/2022-72	ro de CPF
.001338/2021-49	ro de CPF e RG
.002030/2021-83	ro de CPF
.002012/2021-39	ão de nascimento
.000579/2021-75	ro de CPF e RG
.004299/2023-05	or laudo médico CID

Processos referentes aos alunos	
Com dados pessoais expostos	**Descrição do dado**
.002690/2021-11	ro de CPF e RG
.002677/2021-71	a de identidade
.001632/2024-14	RG
.000740/2024-63	ng e adoecida mentalmente
.003592/2022-08	a de identidade
.003621/2022-23	ro do CPF
.000435/2023-13	ro do CPF
.000573/2024-51	com autismo, TDAH e TAG
.000427/2024-35	com histórico de agressões

Processos referentes a alunos
Com dados pessoais protegidos
.005967/2023-13

Durante a análise, foram identificadas falhas significativas relacionadas à proteção de dados pessoais nos processos eletrônicos, as quais evidenciam a exposição indevida de informações sensíveis. Seguem as principais constatações:

2.2.1.1 Processos de Saúde, Afastamentos ou Licenças Médicas de Servidores

Dos 13 processos examinados, foram encontradas as seguintes exposições indevidas de dados pessoais:

- **2 processos** continham a **certidão de nascimento** dos servidores exposta.
- **5 processos** apresentavam o **número do CPF** dos servidores de forma desprotegida.
- Em **1 processo**, foi identificado um **laudo médico** com o **número do CID** (Classificação Internacional de Doenças), o que constitui exposição de **dados sensíveis**, conforme o art. 5º, inciso II, da LGPD.

2.2.1.2 Processos de Alunos

Entre os 10 processos analisados, verificamos as seguintes irregularidades:

- **6 processos** continham os **números de CPF e RG** dos alunos expostos.
- Em **2 processos**, havia a **cópia da cédula de identidade** dos alunos.
- **1 processo** incluía uma **ata de reunião** que mencionava que uma aluna havia sofrido bullying e apresentava problemas de saúde mental, caracterizando exposição de dados sensíveis.
- **1 processo** revelava que uma aluna apresentava **autismo, TDAH (Transtorno de Déficit de Atenção e Hiperatividade)** e **TAG (Transtorno de Ansiedade Generalizada)**.
- **1 processo** mencionava um aluno com **histórico de agressões físicas e verbais, gazeteamento e pichações**.

A análise evidenciou que os controles implementados pelo Ifes para proteger os dados pessoais nos processos eletrônicos analisados são insuficientes para garantir a conformidade com a LGPD. A exposição de dados pessoais como CPF, RG, certidões de nascimento sem o devido tarjamento ou descaracterização, além de informações sensíveis como laudos médicos e diagnósticos de saúde mental, demonstra fragilidade nos mecanismos de segurança e privacidade.

Ademais, a exposição de dados sensíveis referentes à saúde, como diagnósticos de autismo, TDAH, TAG, e questões relacionadas ao bullying e comportamentos agressivos, reforça a necessidade de implementação de medidas adicionais de proteção, conforme previsto no art. 13 da LGPD. A instituição não implementou adequadamente os mecanismos de anonimização ou pseudonimização desses dados, deixando vulneráveis informações altamente sensíveis.

Corroborando essas constatações, vale ressaltar que essa Auditoria Interna recebeu três denúncias pelo sistema FalaBr cujos objetos eram a divulgação de dados pessoais. As

reclamações realizadas pelos denunciantes estavam relacionadas a divulgação de dados pessoais, tais como: referente à saúde (tipo de doença), divulgação de documentos pessoais (CPF) e a caracterização de processos como “Restrito” - o que não possibilita o acesso ao mesmo - pela justificativa de conterem dados pessoais, em detrimento de estarem restritos apenas os documentos e/ou informações pessoais.

As falhas encontradas implicam em alto risco de violação dos direitos dos titulares de dados, podendo gerar consequências legais graves para o Ifes, como sanções administrativas pela Autoridade Nacional de Proteção de Dados (ANPD) e ações judiciais por parte dos titulares dos dados. A exposição de dados pessoais sensíveis não apenas viola os princípios da finalidade, necessidade e segurança, conforme o art. 6º da LGPD, mas também pode prejudicar a reputação da instituição e comprometer a confidencialidade e integridade das informações tratadas.

Dessa forma, diante das evidências obtidas nesta auditoria orienta-se que o Instituto fortaleça urgentemente os seus controles internos no que tange à proteção de dados pessoais, especialmente em processos eletrônicos que contenham informações sensíveis.

III. COMUNICAÇÃO DOS RESULTADOS DOS TRABALHOS DE AUDITORIA

A comunicação dos resultados dos trabalhos foi realizada por meio de reunião de busca conjunta com o Reitor, a Diretora Executiva do Ifes, a Pró-Reitoria de Desenvolvimento Institucional, a Encarregada de Dados e o Diretor de Tecnologia da Informação. Após conhecimento do relatório preliminar, os destinatários acima mencionados puderam se manifestar caso houvesse alguma informação relevante que pudesse vir a alterar as constatações e/ou recomendações decorrentes das análises realizadas pela equipe de auditoria.

A finalização deste trabalho se deu com a elaboração e encaminhamento do relatório final por esta Audin, que estará disponível aos órgãos de controle externo e à sociedade, conforme preceitua Instrução normativa nº 03/2017 do Ministério da Transparência, Fiscalização e Controle.

Embasamento de informações suficientes, confiáveis, relevantes e úteis

A obtenção de informações probatórias necessárias e suficientes à fundamentação objetiva de achados e conclusões de auditoria foi, em certa medida, adequada, pertinente e razoável, e se pautaram na aplicação de testes de auditoria, armazenados adequadamente nos papeis de trabalho, consideradas as circunstâncias que o envolveram.

Desempenho da unidade auditada quanto aos aspectos avaliados

O Desempenho do Ifes no que corresponde aos aspectos avaliados neste trabalho foi considerado insatisfatório pelas constatações apresentadas.

Recomendações:

Diante das constatações apresentadas neste relatório, destacam-se as seguintes recomendações, elaboradas com base no diagnóstico realizado pela equipe de Auditoria. Tais recomendações visam fortalecer a governança e aprimorar a proteção de dados pessoais no Ifes. Para auxiliar na implementação dessas recomendações, pode-se utilizar o **Guia de Elaboração de Programa de Governança em Privacidade, Versão 2.2, ano 2024**, elaborado pela Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos.

Recomendação 1: Recomenda-se ao Reitor, com assistência e orientação do encarregado de dados, a elaboração de uma Política Interna de Proteção de Dados pessoais, acompanhado de um cronograma para implementação de cada uma das fases e/ou etapas, contendo as diretrizes para o atendimento da Lei Geral de Proteção de Dados no âmbito do Ifes, abordando minimamente os tipos de dados utilizados no Ifes que carecem de proteção e devem ser tratados, qual é o tipo de tratamento/classificação adequados para cada tipo de dado, onde esses dados devem ser armazenados e quem poderá ter acesso a esses dados (Art. 50º da Lei nº 13.709/2018 e art. 16, VI da Resolução CD/ANPD nº 18/2024);

Recomendação 2: Recomenda-se ao setor de Tecnologia da Informação que adeque e parametrize os sistemas eletrônicos utilizados no Ifes de acordo com as diretrizes estabelecidas na LGPD de forma a proteger os dados pessoais. Para tanto recomenda-se as seguintes ações:

a) criação de mecanismos que permitam anonimizar ou pseudonimizar os dados pessoais, especialmente aqueles classificados como sensíveis, conforme o art. 13 da LGPD.

b) criação de mecanismos que garantam que informações sensíveis sejam restritas a documentos ou seções específicas, evitando a exposição de dados em processos completos
c) desenvolvimento de funcionalidades que permitam tarjar informações sensíveis (como CPF, RG, laudos médicos, e CID) em documentos visualizados ou compartilhados pelos sistemas.

Recomendação 3: Recomenda-se a Pró-Reitoria de Desenvolvimento Institucional em conjunto com o Encarregado de Dados, que promova treinamentos e capacitações para todos os servidores, terceirizados e/ou colaboradores que possam ser classificados como "agente de dados" para conhecimento da forma adequada de tratamento e armazenamento de dados pessoais bem como de suas responsabilidades (Acórdão TCU nº 1384/2022);

Recomendação 4: Recomenda-se ao Reitor, com assistência e orientação do encarregado de dados e em conjunto com o setor de Tecnologia da Informação, a elaboração de um plano de resposta a incidentes de segurança relacionados ao vazamento de dados detalhando os procedimentos para a comunicação de vazamentos e a mitigação de riscos potenciais antes que incidentes ocorram (art. 48 da Lei nº 13.709/2018 e art. 16, V da Resolução CD/ANPD nº 18/2024).

A Equipe de Auditoria Interna agradece a atenção dispensada.

Vitória, 23 de dezembro de 2024.

Atenciosamente,

Cintia Petri
Auditora

Rafael Barbosa Mariano
Administrador

Ciente do relatório,

Abdo Dias da Silva Neto
Chefe da Auditoria Interna do Ifes