Universidade Federal do Espírito Santo

PLANO DE ADEQUAÇÃO DA UFES À LGPD

Controlador:

Universidade Federal do Espírito Santo, por meio de seu reitor, Paulo Sérgio de Paula Vargas

Operador:

Comitês Operadores de Dados Pessoais, por meio de seus presidentes (em definição)

Encarregado:

Ouvidoria da Ufes, por meio de seu Ouvidor, Renato Carlos Schwab Alves

2021

ADMINISTRAÇÃO SUPERIOR

Reitor
Paulo Sergio de Paula Vargas

Vice-reitor
Roney Pignaton da Silva

Pró-reitor de Planejamento e Desenvolvimento Institucional
Rogério Naques Faleiros

Pró-reitora de Administração
Teresa Cristina Janes Carneiro

Pró-reitor de Assuntos Estudantis e Cidadania
Gustavo Henrique Araújo Forde

Pró-reitor de Extensão
Renato Rodrigues Neto

Pró-reitora de Gestão de Pessoas
Josiana Binda

Pró-reitora de Graduação
Cláudia Maria Mendes Gontijo

Pró-reitor de Pesquisa e Pós-Graduação
Valdemar Lacerda Júnior

Superintendente de Educação a Distância
Maria Auxiliadora de Carvalho Corassa

Superintendente de Comunicação
Ruth de Cássia dos Reis

Superintendente de Infraestrutura
Alessandro Mattedi

Superintendente de Tecnologia da Informação
Renan Teixeira de Souza

Secretária de Avaliação Institucional
Leila Massaroni

Secretário de Cultura
Rogério Borges

Secretário de Relações Internacionais
Yuri Luiz Reis Leite

Comissão instituída pela Portaria 693-R, de 14 de dezembro de 2020 e alterada pela portaria 177, de 07 de abril de 2021.

- Rogério Naques Faleiros – Presidente (PROPLAN)
- Alexandre Severino Pereira (DDP/PROGEP)
- Cássia Gisele de Morais Rizzo (DDI/PROAD)
- Josiana Binda (PROGEP)
- Marcelo Rosa Pereira (Ouvidoria/UFES)
- Mirella Tofano Cuzzuol (CPI/PROPLAN)
- Noéle Bissoli Perini de Souza (CPI/PROPLAN)
- Patrícia Alcântara Cardoso (Gabinete da Reitoria/UFES)
- Rafael Petri (DCOS/PROAD)
- Renan Teixeira de Souza (STI)
- Renata Alves Campos (STI)
- Renato Carlos Schwab Alves (Ouvidoria/UFES)
- Silas Adolfo Potin (CPI/PROPLAN)
- Vandré de Castro Toffoli (DPI/PROAD)
- Vinícius Rossi Oliveira (CPI/PROPLAN – DDI/PROAD)
- Welington Batista Pereira (Ouvidoria/UFES)

LISTA DE FIGURAS

Figura 1 – Atores, processos e procedimentos relacionados à proteção de dados.....20
Figura 2 – Escala de Percepção do Grau de Maturidade 23
Figura 3 – Comitês Operadores por tipologia documental 30
Figura 4 – Plano de Comunicação relacionado à LGPD 32

LISTA DE TABELAS

Tabela 1 – Faixas de índices. Diagnóstico de adequação à LGPD/SGD.....8
Tabela 2 – Instruções Normativas GSI/PR quanto à Maturidade Institucional para a LGDP.18
Tabela 3 – Descritivo IDP-UFES 34
Tabela 4 – Modelo de taxonomia de dados 36
Tabela 5 – Ações executivas do modelo de implementação LGPD 38
Tabela 6 – Políticas e Práticas para proteger a privacidade dos cidadãos 44
Tabela 7 – Práticas para proteger a privacidade dos cidadãos.....45

SUMÁRIO

APRESENTAÇÃO E ALINHAMENTO DE EXPECTATIVAS COM A ALTA GESTÃO 5

1 GOVERNANÇA EM PRIVACIDADE 6

1.1 DIAGNÓSTICO INICIAL 6

1.1.1 Do Diagnóstico Inicial 7

1.1.2 Considerações sobre o Diagnóstico Inicial e Sensibilização 13

1.2 ANÁLISE DO GRAU DE MATURIDADE DA UFES EM RELAÇÃO À LGPD 14

1.2.1 Análise Inicial do Grau de Maturidade da UFES em relação à LGPD 14

1.2.2 Modelo metodológico para futuras Análises do Grau de Maturidade em Relação à LGPD 24

1.3 ESTRUTURA ORGANIZACIONAL PARA GOVERNANÇA E GESTÃO DA PROTEÇÃO DE DADOS PESSOAIS 26

1.4 PROMOÇÃO DE UMA CULTURA DE SEGURANÇA, PROTEÇÃO DE DADOS E PRIVACIDADE 31

2 INVENTÁRIO DE DADOS 33

2.1 FASES DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS 38

3 TERMOS DE USO E POLÍTICA DE PRIVACIDADE 41

4 RISCOS DE SEGURANÇA E PRIVACIDADE 44

4.1 POLÍTICAS E PRÁTICAS PARA PROTEGER A PRIVACIDADE DO CIDADÃO 44

4.2 DIRETRIZES DE PROTEÇÃO DE DADOS PESSOAIS E PRIVACIDADE 46

4.3.1 Avaliação de riscos de segurança e privacidade 50

5 ADEQUAÇÃO DE CONTRATOS 52

6 RELATÓRIO DE IMPACTO E PROTEÇÃO DE DADOS 54

7 RESPOSTA A INCIDENTES DE SEGURANÇA EM DADOS PESSOAIS 55

8 AÇÕES DE CAPACITAÇÕES 55

8.1 PLANO DE CAPACITAÇÃO 55

8.2 METAS E RESULTADOS ESPERADOS 56

8.3 PÚBLICO ALVO 56

8.4 MODALIDADES E CLASSIFICAÇÃO DAS AÇÕES 56

8.5 EXECUÇÃO DAS AÇÕES 56

8.6 PLANEJAMENTO E ACOMPANHAMENTO DOS RESULTADOS 57

8.7 QUADRO DE ATIVIDADES PROGRAMADAS 58
9 CRONOGRAMA DE EXECUÇÃO 60
ANEXO I – LISTAGEM GERAL DO INVENTÁRIO DOS SERVIÇOS E PROCESSOS, TIPOS DE DADOS E TAXONOMIAS 61
ANEXO II – MAPA DE RISCO 76
ANEXO III – CÁLCULO DO RISCO INERENTE 77
ANEXO IV – PLANO DE AÇÃO 78
ANEXO V – TERMO DE CONSENTIMENTO PARA PARTICIPANTES DE PROJETOS INSTITUCIONAIS 79

APRESENTAÇÃO E ALINHAMENTO DE EXPECTATIVAS COM A ALTA GESTÃO

A Lei Geral de Proteção de Dados (LGPD) do Brasil (Lei nº 13.709, de 14 de agosto de 2018) entrou em vigor em agosto de 2020 e estabelece regras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais, impondo mais proteção e penalidades para o não cumprimento. Sua criação visa o controle e a proteção de dados pessoais, buscando garantir todos os direitos possíveis dos titulares, além de dar o máximo de autonomia possível, não excluindo situações específicas. A lei ambiciona criar um cenário de segurança jurídica, com a padronização de normas e práticas, para promover a proteção de forma igualitária dentro do país e no mundo, aos dados pessoais de todo cidadão que esteja no Brasil.

A LGPD também inaugura uma nova cultura de privacidade e proteção de dados no país, o que demanda a conscientização de toda a sociedade, inclusive a comunidade universitária, acerca da importância dos dados pessoais e os seus reflexos em direitos fundamentais como a liberdade, a privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Em face desse desafio, fora constituída uma comissão (Portarias n. 693-R, de 14 de dezembro de 2020, e n. 177, de 07 de abril de 2021) com vistas à elaboração de Plano de Adequação da Universidade Federal do Espírito Santo, produto que ora apresentamos. Subdividido em oito tópicos, o plano ambiciona adequar procedimentos institucionais acerca da privacidade e segurança de dados, como também estabelecer nova governança de dados pessoais, sejam eles provenientes de público interno (alunos, servidores docentes e servidores técnico-administrativos) ou de público externo (comunidade externa, entes contratantes, convênios e acordos de cooperação).

Para o desenvolvimento do projeto institucional de adequação da Ufes à LGPD, faz-se necessário conhecer as expectativas da alta administração para a partir de então, priorizar as ações e propor uma estrutura de governança adequada. Considera-se como alta administração o Comitê de Governança Digital, composto pelo Reitor, Pró-Reitor de Administração, Pró-Reitor de Assuntos Estudantis e Cidadania, Pró-Reitor de Gestão de Pessoas, Pró-Reitor de Graduação, Pró-Reitor de Extensão, Pró-Reitor de Pesquisa e Pós-Graduação, Pró-Reitor de Planejamento e Desenvolvimento Institucional, Superintendente de Tecnologia da Informação e Ouvidor.

Esperamos que este Plano de Adequação da Ufes à LGPD possua o condão de coordenar uma série de ações institucionais com vistas à construção de uma cultura de tratamento de dados, fator que agregará maior refinamento na modelagem e tratamento dos dados pessoais, os quais tenham como finalidade propósitos legítimos, específicos e explícitos, de modo que os procedimentos de tratamento sejam conhecidos pelos titulares dos dados.

Paulo Sérgio de Paula Vargas, reitor da Ufes.

Roney Pignaton da Silva, Vice-reitor da Ufes.

1 GOVERNANÇA EM PRIVACIDADE

1.1 DIAGNÓSTICO INICIAL

Trata-se de texto introdutório ao Plano de Adequação da Ufes à Lei Geral de Proteção de Dados (Lei 13.709/2018, com nova redação dada pela Lei 13.853/19), doravante LGPD, objeto de construção de comissão estabelecida pelo reitor da UFES, conforme vimos acima. Tal plano visa à adequação do funcionamento da Universidade aos critérios definidos em lei, construindo processos eficazes para a transparência pública e para o gerenciamento dos direitos dos titulares de dados pessoais. A adequação à LGPD justifica-se por i) garantir ao público usuário a transparência e acesso aos seus dados registrados na Ufes; ii) a proteção aos direitos fundamentais de liberdade e de privacidade; iii) o livre desenvolvimento da personalidade da pessoa natural; iv) a defesa do público usuário.

A adequação da Instituição à LGPD redundará em peças de gestão absolutamente necessárias nesta seara, tais como um Programa de Governança em Privacidade, num Inventário de Dados Pessoais, na elaboração de termos de uso mais pertinentes, na constante avaliação dos riscos, em adequações de contratos, num Relatório de Impacto de Proteção de Dados (RIPD), em protocolos de respostas a incidentes e em ações de capacitação, a partir das quais pretende-se difundir entre os servidores da Ufes uma cultura organizacional ainda mais calcada nos princípios da transparência e da defesa dos dados dos usuários.

Se exitoso, o Plano trará diversos benefícios à sociedade e à Instituição, tais como o próprio Inventário de Dados, a ampliação de privacidade de dados nas operações, e uma mais precisa identificação dos riscos de segurança da informação, elemento sempre presente no atual contexto, onde cada vez mais os dados pessoais circulam em meio digital, compondo bases hospedadas em sistemas de complexa gestão. Assim, partimos da premissa de que a adequação à LGPD se caracteriza como desafios transdisciplinares, envolvendo as Tecnologias da Informação, técnicas e conceitos advindos da Arquivologia, Direito e Administração. Deve-se destacar que a adequação à esta normativa é processo perene e de evolução constante, no qual a instituição paulatinamente promoverá aprimoramentos em sua política de gestão de dados pessoais.

A Universidade Federal do Espírito Santo é formada por uma comunidade de aproximadamente trinta mil pessoas. São cerca de vinte mil alunos matriculados em mais de cem cursos de graduação, e quatro mil alunos matriculados em seus mais de sessenta cursos de pós-graduação. Em relação ao seu corpo técnico e docente, a Ufes possui cerca de quatro mil servidores públicos, dedicados às atividades administrativas, de ensino, de pesquisa e de extensão. Mobiliza ainda uma série de contratações de serviços, licitações de obras, fornecedores, bem como o estabelecimento de intercâmbios com instituições nacionais e internacionais. Em exemplificação, há hoje em curso mais de setenta acordos de cooperação/intercâmbio internacionais entre a Ufes e universidades de todos os continentes. Nossos projetos de extensão alcançam mais de dois milhões de pessoas em todos os municípios do Estado do Espírito Santo e regiões circunvizinhas, imputando à Instituição uma grande responsabilidade na gestão de dados e informações de seu público usuário. Assim, a Ufes conta hoje com extenso e sensível banco de dados criptografado e protegido por uma série de recursos tecnológicos. A instituição também já opera em processo eletrônico (Lepisma), tendo sido, inclusive, citada positivamente no item n. 75 do Acórdão 484/21 TCU/Plenário, que trata da norma regulamentadora de processo administrativo eletrônico[1].

1.1.1 Do Diagnóstico Inicial

Baseamos nosso diagnóstico em dois instrumentos de análise, um disponibilizado em 2020 pela Secretaria de Governo Digital (SGD) e outro disponibilizado pelo Tribunal de Contas da União (TCU) em 2021, ambos, devidamente preenchidos pela Instituição.

Em julho de 2020 (atualizado em setembro), a Secretaria de Governo Digital (SGD) disponibilizou um questionário com o intuito de fornecer ao órgão respondente as informações necessárias para um diagnóstico do atual estágio de adequação à LGPD. O objetivo deste questionário era o de apresentar um índice de maturidade, possibilitando aos órgãos e entidades direcionar esforços e priorizar as ações necessárias para conformidade em relação à LGPD. O próprio questionário indica que a adequação dos órgãos envolve uma transformação cultural que deve alcançar os níveis estratégico, tático e operacional da instituição. Essa transformação abrange: i) considerar a privacidade dos dados pessoais do cidadão, desde a fase de concepção do serviço ou produto até a sua execução (*Privacidade by Design*); e ii) promover ações de conscientização de todo corpo funcional, no sentido de incorporar o respeito à privacidade dos dados pessoais nas atividades institucionais cotidianas[2].

[1] Disponível em: https://pesquisa.apps.tcu.gov.br/#/documento/acordao-completo/484%252F2021/%2520/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0/%2520. Acesso em 17/04/2021.

[2] Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/diagnostico-de-adequacao-a-lgpd). Acesso em 17/04/21.

À época, os servidores Renan Teixeira de Souza (Superintendente de Tecnologia da Informação/UFES) e Rogério Naques Faleiros (Pró-Reitor de Planejamento e Desenvolvimento Institucional/UFES) elaboraram conjuntamente o preenchimento do questionário disponibilizado. O instrumento apresentava um índice (definido pelo conjunto das respostas registradas, visando medir o nível de adoção por parte da Instituição, de práticas relacionadas à LGPD, em especial o tratamento de dados, programa de privacidade, conhecimento dos guias de boas práticas disponibilizados[3], dentre outros assuntos. Abaixo as faixas de índice pertinentes ao instrumento:

Tabela 1 – Faixas de índices. Diagnóstico de adequação à LGPD/SGD

Índice	Nível de Adequação
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: Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/diagnostico-de-adequacao-a-lgpd. Acesso em 30/03/21.

Neste questionário, preenchido em setembro de 2020, na Dimensão 1 – Governança, a Ufes atingiu **0,03**, figurando em nível inicial. Este grupo de questões abordava o conhecimento acerca dos materiais disponibilizados pela SGD, e se a Instituição já havia desenvolvido Programa Institucional de Privacidade de Dados, ou mesmo um plano de comunicação a ele relacionado. Abordou-se também o tema da definição de um Encarregado de Dados com conhecimento, experiência e autonomia suficientes para implementar a LGPD na Instituição e a questão dos recursos a ele disponibilizados pela alta administração. Destarte, segundo a Lei 13.709/18, o encarregado é definido, conforme Artigo n. 05, como "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). A temática da Governança, no questionário, também abordou a questão dos líderes responsáveis por cada frente de atuação no tratamento dos dados, a definição de indicadores, a elaboração (baseada no Guia de Boas Práticas) do Relatório de Impacto à Privacidade de Dados Pessoais (RIPD), e mesmo se já fora disponibilizado às áreas envolvidas algum treinamento ou capacitação.

[3] Disponível em: (https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd. Acesso em 18/04/21

Na Dimensão 2 – Conformidade Legal e respeito aos princípios, a Ufes obteve o índice **0,05**. Aqui foram abordados temas como a implementação de ações para não tratar e coletar de forma inadequada ou excessiva os dados pessoais dos cidadãos, tratando-se a mínima quantidade de dados necessários para atingir a finalidade legal desejada, ou mesmo a realização de mapeamento de dados processados e suas respectivas bases legais. O instrumento questiona também acerca do respeito aos princípios da LGPD durante o desenvolvimento de serviços relacionados ao tratamento dos dados (nas ocasiões em que cabe consentimento, ou não, do titular dos dados), tanto para clientes dos serviços públicos fornecidos quanto servidores, funcionários e/ou colaboradores da Instituição. Foi questionado, ademais, sobre a adoção de sistemas e procedimentos relacionados ao direito de retificação de informações do titular dos dados, algo previsto em lei, e se o órgão dá publicidade à sua metodologia de tratamento de informações e suas finalidades.

Na Dimensão 3 – Transparência e direitos do Titular, a Instituição obteve o índice **0,00**, o que decorre, justamente, do estágio inicial diagnosticado nas dimensões anteriores. Neste quesito as questões abordavam aspectos mais funcionais da política de privacidade, ausentes, por evidente, pois ainda não estabelecidos pela Ufes. Na Dimensão 4 – Rastreabilidade, a Universidade obteve o índice **0,13**, dado que ainda não desenvolveu o Inventário de Dados e Serviços, peça fundamental de operacionalização da LGPD.

Na Dimensão 5 – Adequação de contratos e de relações com parceiros obteve-se o índice **0,00**. O questionário abordava neste momento aspectos como a adequação de instrumentos convocatórios, revisão de contratos em vigência no sentido de adequá-los à LGPD, algo ainda não desenvolvido à época pela Ufes. Na Dimensão 6 – Segurança da Informação, obteve-se o índice **0,00**. O instrumento indagava sobre a efetiva implementação de controle de segurança para os riscos identificados no RIPD e se havia instituído equipe para a realização de monitoramento das vulnerabilidades técnicas dos serviços que realizam o tratamento de dados pessoais. Embora a instituição tenha feito investimentos consideráveis em Tecnologias da Informação, softwares e criptografia nos últimos anos, as ferramentas precisam ainda ser adequadas aos marcos da LGPD, por exemplo, gerando evidências que comprovem a tomada de medidas de segurança necessárias à proteção dos dados pessoais contra as ameaças internas e externas.

Na Dimensão 7 – Violação de Dados, obteve-se o índice **0,22.** O instrumento, nesta etapa, aborda o estabelecimento de um processo de comunicação das possíveis violações de dados pessoais, e se o órgão realizava gestão de incidentes para tratar possíveis violações dos dados de forma efetiva, estabelecendo-se um canal para recebimento de denúncias e de alertas de ocorrências de irregularidades, como denúncias de possíveis vazamentos de dados e falhas de segurança.

Assim, por este instrumento disponibilizado pela Secretaria de Governo Digital e preenchido pela Ufes em setembro de 2020, fora atribuída à instituição o Índice de Adequação à LGPD de **0,06**, denotando-se, assim, o diagnóstico de nível de adequação **Inicial**, conforme parâmetros expostos na tabela 01. Tal resultado fora extremamente importante na sensibilização da alta gestão ao conjunto de demandas colocadas pela adequação à LGPD, engendrando ações mais sistemáticas da gestão, tais como a participação em webinários, formação de grupos de estudo e composição de comissão para elaboração de plano de adequação da Ufes à LGPD, pois a avaliação das dimensões analisadas pelo instrumento acima descrito foram sobejamente prejudicadas pela ausência de governança e conformidade legal, até então não definidas pela Instituição.

Outro instrumento relevante ao diagnóstico sobre a adequação das organizações públicas federais à LGPD foi a Auditoria realizada pelo Tribunal de Contas da União (TCU), respondida pela instituição em 29 de março de 2021, novamente pelos servidores Renan Teixeira de Souza (STI) e Rogério Naques Faleiros (PROPLAN). Por se tratar de recente instrumento aplicado por aquele órgão, ainda não dispomos dos resultados da auditoria. De certo, já indica a preocupação dos órgãos de controle com a adequação e tratamento de dados no âmbito do serviço público federal.

O instrumento do TCU fora subdividido em 10 itens. No primeiro, fora feita a **identificação do respondente**, e no segundo as questões giram em torno de aspectos relacionados à **preparação**, identificação e planejamento das medidas necessárias à adequação. As respostas, neste quesito, já indicavam movimentação institucional, tais como portaria de nomeação de comissão e o próprio Termo de Abertura de Projeto (TAP), agora concluído como Plano de Adequação da Ufes à LGPD.

No terceiro item, **contexto organizacional**, foram abordados aspectos relacionados à identificação de normativos correlatos à proteção de dados pessoais que devem ser respeitados pela organização: iniciativas de identificação de comandos relativos à LGPD, identificação de categorias de titulares, identificação de operadores que realizam tratamento de dados, existência de controlador conjunto, armazenamento de dados e avaliação de riscos. Destarte, como a Ufes encontrava-se em processo de elaboração da política, as respostas indicaram que estas definições foram parcialmente executadas. No quarto item, **liderança**, supõe-se a existência de liderança e comprometimento com a iniciativa de adequação à LGPD, com a demonstração de Política de Segurança da Informação (ou instrumento similar) e a nomeação do encarregado (nos termos da Lei n. 13.709). Nas respostas, fora encaminhada ao TCU a Política de Segurança da Informação e Comunicações (POSIC)[4], que se encontra em revisão/atualização por meio de comissão instituída pelo Reitor da Ufes por meio da Portaria n. 399, em 13 de julho de 2020. As respostas a este instrumento indicaram também que o Reitor já procedeu à indicação do Ouvidor Geral como encarregado de dados à SGD, por meio do Ofício 447/2020/GR/UFES, de 22 de dezembro, enviado à SGD.

[4] Disponível em: https://npd.ufes.br/sites/npd.ufes.br/files/posic_20111216final.pdf. Acesso em 19/04/2021.

O item 5, **capacitação**, visa conscientizar as organizações para a necessidade de capacitação dos colaboradores para conhecimento das políticas organizacionais relacionadas à proteção de dados pessoais e para que reconheçam a importância de suas ações na preservação da privacidade dos titulares. As ações de capacitação a serem empreendidas devem considerar diferentes níveis de envolvimento dos colaboradores no tema, de forma que aqueles que ocuparão funções de alta responsabilidade relacionadas à proteção dos dados recebam treinamento diferenciado, além do nível básico fornecido aos demais. Embora a Ufes ainda não tivesse realizado ação própria de capacitação, nossa Diretoria de Desenvolvimento de Pessoas (DDP/PROGEP) já procedeu à divulgação de cursos sobre a matéria ofertados pela ENAP (Escola Nacional de Administração Pública). Ademais, processos de capacitação são previstos neste Plano de Adequação, sob responsabilidade direta de nossa DDP/PROGEP.

No item 6, **conformidade de tratamento**, a expectativa do documento era de comprovar que os tratamentos de dados pessoais são lícitos à luz dos princípios estabelecidos na LGPD e fundamentados, ao menos, em uma das bases legais descritas na legislação. Também se esperava a elaboração de registros para a documentação das atividades de tratamento. Temas como: i) identificação de finalidades de tratamento de dados; ii) coleta de dados estritamente necessários; iii) temporalidade de armazenamento dos dados pessoais; iv) identificação de bases legais; v) registro das atividades de tratamento; e vi) elaboração de RIPD. Nestes quesitos, as respostas da Instituição figuraram à época entre negativas e parcialmente cumpridas, visto que o Plano de Adequação da Ufes à LGPD encontrava-se em elaboração.

Com o item 7, **direitos do titular**, vem à tona um princípio fundante da LGPD: os dados pessoais pertencem aos seus titulares, e como tal, devem ter acesso ao tratamento que seus dados receberão. Para isso, a organização precisa publicar de maneira clara e concisa as informações atinentes aos tratamentos e dados pessoais, bem como estar preparada para atender a todos os direitos dos titulares elencados na LGPD. As questões, neste item, versavam sobre se a organização possuía alguma política de privacidade ou instrumento similar, bem como a sua publicação na internet. As respostas da Ufes foram positivas, encaminhando ao TCU nossa Política de Privacidade[5], contudo, deve-se atentar que ainda não haviam sido adotados mecanismos para atender aos direitos dos titulares elencados no artigo n. 18 da LGPD.

[5] Disponível em: https://npd.ufes.br/sites/npd.ufes.br/files/field/anexo/politica_de_privacidade_sites_ufes.pdf#:~:text=A%20Ufes%20n%C3%A3o%20garante%20a,maliciosos%2C%20erros%20ou%20outros%20problemas.&text=Eventuais%20d%C3%BAvidas%20sobre%20as%20condi%C3%A7%C3%B5es,ouvidoria%40ufes.br%E2%80%8B. Acesso em 30/04/2021

O item 8, **compartilhamento de dados pessoais**, refere-se ao compartilhamento de dados com terceiros, que também deve seguir controles adequados para mitigar riscos que possam comprometer a proteção dos dados pessoais. A LGPD estabelece que as partes envolvidas no compartilhamento sejam formalizadas em contrato e que cuidados especiais devem ser adotados no caso de transferências internacionais de dados. A Ufes, como contratante, contratada e como manancial de informações a diversos órgãos públicos, em especial os Ministérios da Educação e da Economia, deverá desenvolver política neste quesito, mitigando possíveis falhas, tal como veremos adiante.

No item 9, **violação de dados pessoais**, o instrumento do TCU abordou o gerenciamento de incidentes de segurança relacionados à violação de dados pessoais, bem como se a organização dispunha de mecanismo de notificação à ANPD, e os titulares no caso de incidentes que possam acarretar em danos ou riscos aos titulares. Como o Plano de Adequação da Ufes à LGPD ainda se encontrava em elaboração, a instituição ainda não possuía Plano de Resposta a Incidentes ou documento similar; contudo já possui sistema para registro de incidentes de segurança da informação, e de suas respectivas ações. Embora disponha de sistemas com relativa segurança (criptografia), a Ufes ainda não monitorava proativamente a ocorrência de eventos que podem ser associados à violação de dados pessoais, o que vem a reboque de desenvolvimento de uma cultura de tratamento dos dados em desenvolvimento. Deve-se considerar aqui que os procedimentos de comunicação com a ANPD não haviam sido estabelecidos em função da própria constituição desta Agência, cuja estrutura fora criada em agosto de 2020 (Decreto 10.474/20), e sancionada pela presidência da república em dezembro de 2020. A convocação para a formação de seu conselho consultivo (CNPD) fora divulgada em fevereiro de 2021.

O item 10 do instrumento, **medidas de tratamento**, versava sobre a adoção de medidas de segurança, técnicas e administrativas, visando à proteção dos dados pessoais, em especial sobre os controles capazes de mitigar riscos que possam resultar em violação de privacidade. Em suas respostas, a Ufes demonstrou que é capaz de comprovar a adoção de medidas de segurança, técnicas e administrativas, bem como a utilização de criptografia, contudo, ainda carecia de estabelecer a relação de tais práticas aos pressupostos da LGPD, como por exemplo o registro de eventos de atividades de tratamento de dados pessoais. A organização ainda não havia adotado medidas para assegurar que os processos e sistemas fossem projetados, desde a concepção, em conformidade com a LGPD (*Privacy by Design e Privacy by Default*), entretanto, como opera por meio de sistemas e protocolo eletrônico, dispõe de certa vantagem comparativa neste aspecto. Tais medidas irão demandar prazo mais estendido, exigindo a revisão de diversas rotinas administrativas a serem implementadas após a elaboração do Plano de Adequação da Ufes à LGPD, como veremos adiante.

Como dito anteriormente, ainda não dispomos de devolutiva relacionada a esta auditoria do TCU, no entanto, participar do questionário fora um interessante exercício de reflexão acerca dos limites e possibilidades de adequação da Ufes à LGPD.

1.1.2 Considerações sobre o Diagnóstico Inicial e Sensibilização

Como vimos acima, foram dois os instrumentos de diagnóstico utilizados pela Instituição até o momento: i) ferramenta de diagnóstico disponibilizada pela Secretaria de Governo Digital (SGD), cujo preenchimento fora realizado em setembro de 2020; e ii) Auditoria do TCU para avaliação de adequação das organizações públicas federais à LGPD, realizada em março de 2021.

No intervalo existente entre ambos os preenchimentos, pode-se perceber avanços na sensibilização da alta gestão da Universidade para com a necessária adequação à LGPD, visto que fora emitida Portaria do Reitor visando constituição de Comissão para elaboração de Plano de Adequação (Portaria n. 693, de 14 de dezembro de 2020), bem como a definição do encarregado de dados por meio do ofício supracitado. Desde então, tal comissão trabalhou sistematicamente na produção deste plano de adequação, cuja implementação está prevista para agosto de 2021.

Evidentemente, a adequação à LGPD não é procedimento trivial. Em face da própria complexidade da Instituição e do volume de dados (sensíveis) que por ela circulam, diversas operações de mapeamento, de tratamento, de comunicação e de melhoria de infraestrutura tecnológica deverão ser empreendidas, contudo, como premissa, acreditamos dispor de recursos humanos e tecnológicos para implementação deste Plano de Adequação à LGPD, tarefa para a qual também deverão contribuir os guias disponibilizados pela SGD. Contudo, deve-se observar que restrições orçamentárias, de recursos e de pessoal podem vir a prejudicar esta implementação.

Como veremos adiante, faz-se mister a definição de estrutura de governança e a definição do controlador e do operador pelo Comitê de Governança Digital da Ufes, presidido pelo Reitor, bem como a elaboração de Inventário de Dados e de Relatório de Impacto de Proteção de Dados, peças fundamentais na operacionalização da LGPD. São também tarefas deste Plano a adequação de contratos com parceiros, a definição de procedimentos para gestão de riscos, e a definição de Plano de Comunicação Interna e Externa relacionada à LGPD, diretamente vinculados às medidas de tratamento de dados pessoais a serem implementadas, como também a definição de política de capacitação dos servidores envolvidos nesta operação.

Os diagnósticos realizados indicaram que a maturidade institucional era **baixa** no momento de seu preenchimento, no que se refere à adequação à LGPD, contudo, já se pode detectar a sensibilização da alta gestão e de nossa comunidade ante ao desafio colocado.

1.2 ANÁLISE DO GRAU DE MATURIDADE DA UFES EM RELAÇÃO À LGPD

Feito o diagnóstico inicial a partir dos instrumentos acima listados, tornava-se necessário, nos termos dos Guias Operacionais disponibilizados pela Secretaria de Governo Digital[6], a análise do grau de maturidade da Instituição em relação à LGPD, observando-se fatores como a rastreabilidade de dados, a comunicação com o cidadão e a transparência. Como ferramenta para a análise da maturidade, a Secretaria de Governo Digital (SGD), com o intuito de fornecer um diagnóstico do atual estágio de adequação à LGPD, trazendo subsídios para a formalização e cálculo de um índice de maturidade, oferece um questionário aos órgãos do SISP (Sistema de Administração dos Recursos de Informação e Informática). Esse diagnóstico disponível no portal gov.br tem o propósito de auxiliar constantes medições do índice de maturidade do órgão ou entidade em relação à LGPD. Além de retratar o nível de adequação à LGPD, o índice de maturidade pode também ser utilizado como um índice de performance, importante ferramenta de monitoramento.

1.2.1 Análise Inicial do Grau de Maturidade da UFES em relação à LGPD

No que trata da fundamentação legal da análise inicial de maturidade destaca-se que sua base é a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei n° 13.709, de 14 de agosto de 2018), que foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo, como vimos acima. Destaca-se que a LGPD estabelece o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado e engloba um amplo conjunto de operações efetuadas em meios manuais ou digitais.

Para o bom entendimento da LGPD, e definição do Grau de Maturidade da UFES, é preciso, em etapa preliminar, conhecer os conceitos, atinentes à matéria, apresentados no artigo n. 05 da Lei, que estabelece o seguinte entendimento e considera:

> **"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;
>
> **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;

[6] Disponível em https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd. Acesso em 09/05/2021.

Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

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

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

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

Agentes de tratamento: o controlador e o operador;

Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

Relatório de impacto à proteção de dados pessoais: documentação do controlador 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;

Órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e (Redação dada pela Lei nº 13.853, de 2019)

Autoridade nacional: autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (Redação dada pela Lei nº 13.853, de 2019) (BRASIL, 2018, p. 2-4)"

1.2.1.1 Requisitos de Governança em Privacidade na LGPD

Os requisitos de Governança em Privacidade estabelecidos na LGDP, que deverão ser analisados para a identificação do Grau de Maturidade, constam dos artigos 49 a 51 da lei.

"Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Seção II

Das Boas Práticas e da Governança

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.

§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

I - implementar programa de governança em privacidade que, no mínimo:

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

> b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
>
> c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
>
> d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
>
> e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
>
> f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
>
> g) conte com planos de resposta a incidentes e remediação; e
>
> h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;
>
> II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.
>
> § 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.
>
> Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais. (Brasil, 2018. p. 15-16)".

Outras normas federais para esta avaliação estão presentes no Guia de Boas Práticas LGPD para Implementação na Administração Pública Federal editado pelo Comitê Central de Governança de Dados do Governo Federal, que estabelece no Item 4.2.7

> "Os normativos do GSI/PR são de cumprimento obrigatório pelos órgãos e entidades da Administração Pública Federal, direta e indireta. Tais normas estão estruturadas em Instruções Normativas, cuja implantação auxilia no aumento da maturidade da Segurança da Informação e elevação dos níveis de proteção dos dados. As Instruções Normativas do GSI/PR podem ser encontradas no link <http://dsic.planalto.gov.br/assuntos/editoria-c/instrucoes-normativas>. (BRASIL, 2020, p. 56)"

O referido Guia[7], no qual constam também as Instruções Normativas listadas na tabela abaixo, indica itens de maturidade que devem ser observados e desenvolvidos pelas Instituições Públicas e Privadas, mediante a operacionalização dos conceitos acima descritos:

[7] Disponível em https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guia-boas-praticas-lgpd. Acesso em 05/05/2021.

Tabela 2 – Instruções Normativas GSI/PR quanto à Maturidade Institucional para a LGDP

Instrução Normativa GSI Nº 1 - 27 de maio de 2020.	Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal. (Publicado em: 28/05/2020 | Edição: 101 | Seção: 1 | Página: 13)
Instrução Normativa GSI Nº 2 - 24 de julho de 2020.	Altera a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal. (Publicado em: 27/07/2020 | Edição: 142 | Seção: 1 | Página: 3)
Instrução Normativa GSI Nº 2 - 5 de fevereiro de 2013	Dispõe sobre o Credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal. (Publicada no DOU Nº 32, de 18 Fev 2013- Seção 1)
Instrução Normativa GSI Nº 3 - 6 de março de 2013	Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal. (Publicada no DOU Nº 50, de 14 Mar 2013- Seção 1)
Instrução Normativa GSI Nº 4 - 26 de março de 2020	Dispõe sobre os requisitos mínimos de Segurança Cibernética que devem ser adotados no estabelecimento das redes 5G. (Publicada no DOU Nº 60, de 27 Mar 2020- Seção 1)
Instrução Normativa Nº 4 - SLTI/MPOG -12 de novembro de 2010	Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP) do Poder Executivo Federal. (Publicada no DOU Nº 218, de 16 Nov 2010- Seção 1)

Fonte: adaptado de http://www4.planalto.gov.br/legislacao/. Acesso em 05/05/2021

1.2.1.2 Metodologia utilizada

Para a análise do Grau de Maturidade da UFES em relação à Lei Geral de Proteção de Dados – LGPD e a partir das orientações constantes no guia, com a devida observação do Atos Normativos acima listados, expedidos pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR), é importante destacar que são instrumentos legais de cumprimento obrigatório pelos órgãos e entidades da Administração Pública Federal, direta e indireta. Assim, propomos os seguintes passos metodológicos:

Para a confirmação da definição e designação dos principais atores no processo de implantação da LGPD na UFES, conforme descrito na lei, cabe ao reitor proceder com a formalização das designações, do Controlador e Operadores de Dados. O Encarregado já foi formalmente designado, como vimos acima.

Considerando que a análise do Grau de Maturidade não é um ato estanque e único, mas uma operação perene que deve ocorrer com certa periodicidade (um ano), com vistas a subsidiar a análise de riscos, bem como a atualização do Plano de Adequação à LGPD, propõe-se a realização de consulta, por meio de formulário eletrônico, aos Gestores Estratégicos da UFES, com especial destaque para aqueles que irão compor os Comitês Operadores de Dados, cuja estrutura de composição será adiante apresentada. Tal consulta deverá promover a atualização da avaliação do Grau de Maturidade de adequação à LGPD, sendo que o formulário proposto deverá atentar-se às Instruções Normativas constantes na tabela acima.

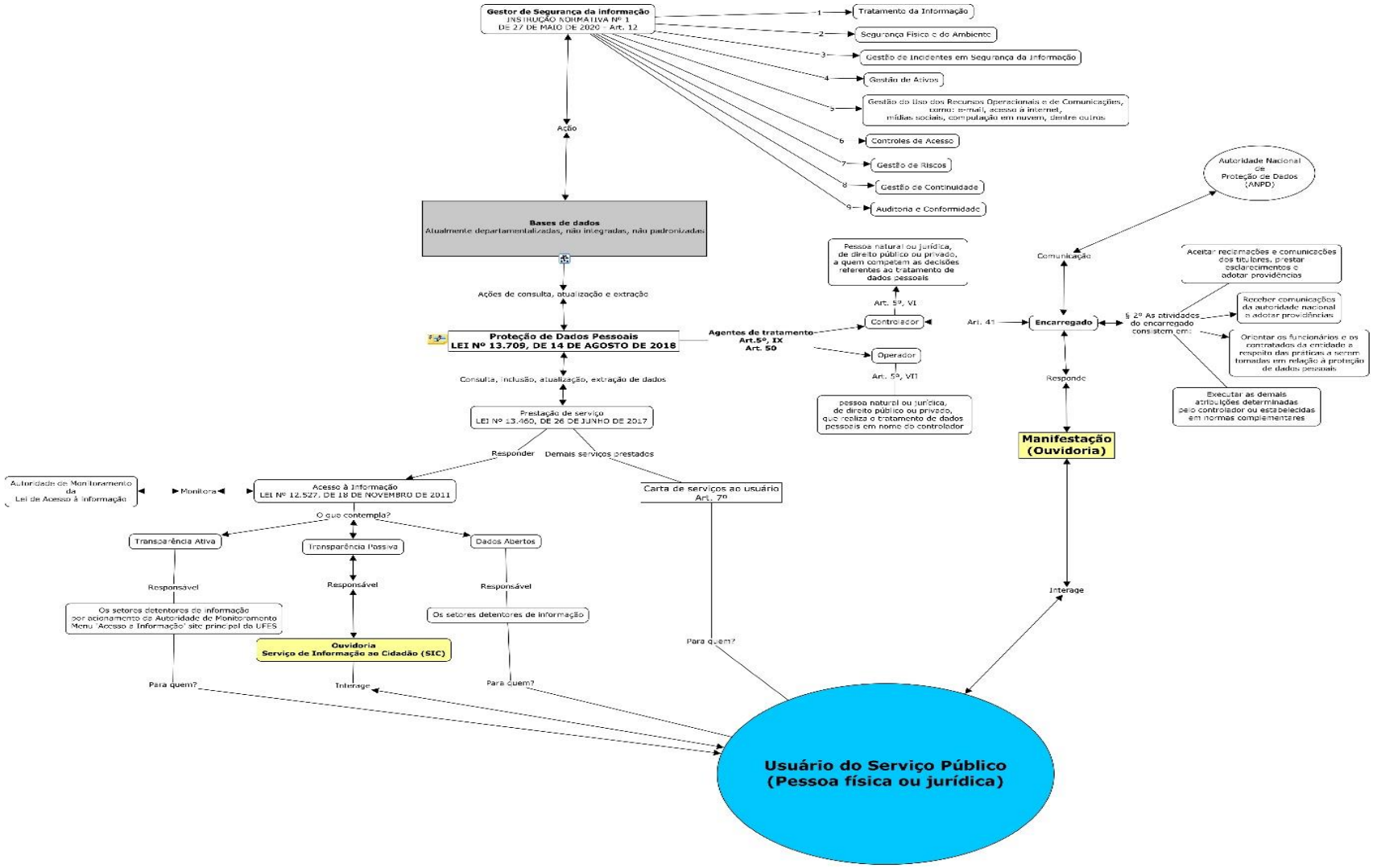
Cabe salientar que as ações de Proteção de Dados e seu grau de maturidade devem considerar a fundamental segregação de funções entre os agentes por ela responsáveis e aqueles responsáveis pela segurança da informação. Tal segregação consiste na separação de funções de autorização, aprovação, execução, controle e contabilização das operações, evitando o acúmulo de funções por parte de um mesmo servidor. As atividades segregadas compreendem àquelas atribuídas ao:

- Gestor de Segurança da Informação, cuja atividades são estabelecidas pela IN 01/2020[8];
- Controlador, Operador e Encarregado de Dados, cuja funções estão estabelecidas pela Lei 13.709/2018;
- Autoridade de Monitoramento da Lei de Acesso à Informação (LAI), cuja atribuições foram estabelecidas pela Lei 12.527/2011.

Faz-se necessário neste ponto uma rápida descrição dos atores, processos e motivações das operações relacionadas à proteção de dados pessoais, em face das normativas e regulações pertinentes. Observemos a figura abaixo:

[8] Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215 . Acesso em 05/05/2021.

Figura 1 – Atores, processos e procedimentos relacionados à proteção de dados



Fonte: elaboração própria

O ponto de partida da figura acima é o Banco de Dados (ainda pouco integrado e não padronizado), ou seja, o local físico ou digital onde a instituição armazena os dados coletados durante a prestação do serviço à sociedade e gestão de suas atividades, incluindo os dados pessoais e dados pessoais sensíveis, conforme definição já apresentada, referentes a cidadãos que utilizam os serviços prestados pela instituição e/ou os próprios servidores e funcionários terceirizados em exercício profissional na instituição. A partir daí identificamos os seguintes atores diretamente relacionados com a incumbência de aplicação prática dos preceitos da Lei Geral de Proteção de Dados:

a) *Gestor de Segurança da Informação:* a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal, identifica a necessidade de designação de um Gestor de Segurança da Informação em cada órgão e entidades da administração pública federal. Em seu artigo n. 19 atribuem-se as competências ao Gestor de Segurança da Informação, dentre as quais destacamos a de coordenar a elaboração da Política de Segurança da Informação e das normas internas de segurança da informação do órgão, que deve possuir diretrizes gerais sobre a implementação de algumas operações, no mínimo, dos seguintes temas[9] (Art. 12, IV);

b) *Controlador, Operador e Encarregado de Dados*: descritos na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais (LGPD). Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. O inciso IX identifica o controlador e o operador como agentes de tratamento; o terceiro ator presente na LGPD é o encarregado[10] (inciso VIII) pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

[9] São eles: a) Tratamento da Informação; b) Segurança Física e do Ambiente; c) Gestão de Incidentes em Segurança da Informação; d) Gestão de Ativos; e) Gestão do Uso dos Recursos Operacionais e de Comunicações, como: e-mail, acesso à internet, mídias sociais, computação em nuvem, dentre outros; f) Controles de Acesso; g) Gestão de Riscos; h) Gestão de Continuidade; e i) Auditoria e Conformidade. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215. Acesso em 05/05/2021. Ver artigo 12, inciso IV.

[10] São atribuições do encarregado: I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

A Ouvidoria é o canal responsável pelo controle e participação social no âmbito da UFES, operacionalizando suas ações por meio da Plataforma de Ouvidoria e Acesso à Informação - Plataforma Fala.Br. Considerando esta expertise, poderá também se estabelecer como canal de recepção das manifestações dos titulares de dados nos termos preconizados pela LGPD, garantindo, assim, um canal de comunicação efetivado pelo encarregado junto ao Controlador e a Autoridade Nacional de Proteção de Dados (ANPD).

No que se refere à prestação de serviços ao cidadão, a Lei nº 13.460, de 26 de junho de 2017[11], dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública. Dentre outros quesitos, traz a Carta de Serviços ao Usuário (Art. 7º), que tem por objetivo informar o usuário sobre os serviços prestados pelo órgão ou entidade, as formas de acesso a esses serviços, e seus compromissos e padrões de qualidade de atendimento ao público. Durante a prestação de serviços, estando estes cadastrados ou não na Carta de serviços da UFES[12], os atores da LGPD e de Segurança da Informação devem atuar pela ótica da proteção de dados, pois será neste momento que o servidor que prestará o serviço fará a coleta dos dados do cidadão e seu armazenamento nos bancos de dados sob responsabilidade da instituição.

Em síntese, A LAI, como ordenamento jurídico e administrativo, visa promover diversas modalidades de transparência pública: a transparência ativa, a transparência passiva e dados abertos, sendo esta lei, a partir de agora, aplicada e gerida a partir das condicionantes estabelecidas pela LGPD. Como exemplo, na aplicação da LAI, os setores detentores das informações demandadas, em consulta às bases de dados com vistas ao fornecimento da informação solicitada, deverão considerar o disposto na LGPD em complemento ao que já estava disposto nas regras atinentes à transparência pública, cabendo ponderar que a publicidade é a regra e o sigilo a exceção.

1.2.1.3 Principais Indicadores para o Nível de Maturidade

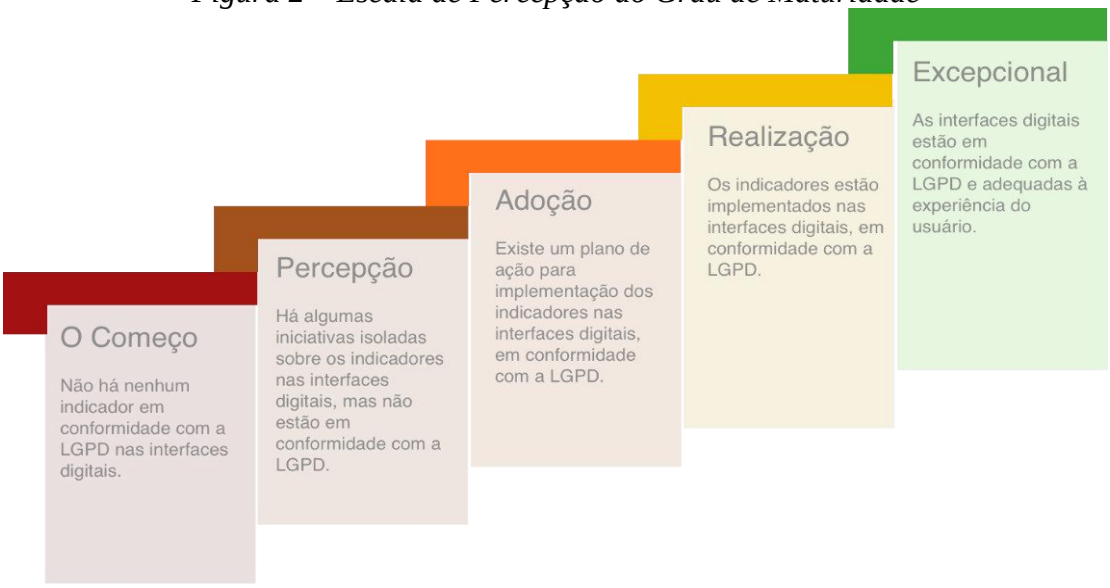
A avaliação do nível de maturidade de uma organização em relação à LGPD, considerando suas interfaces digitais devem se pautar, conforme Brito (2020) em seis indicadores. Estes indicadores se manifestam no processo de trabalho de gestão dos dados e envolvem diretamente o direito do usuário dos dados quanto ao livre acesso, atualização, correção e eliminação dos dados, assim como uma política de privacidade de dados, em conformidade com a LGPD[13]. A autora propõe que sejam considerados os seguintes indicadores, os quais são cruciais para que se verifique a conformidade das interfaces digitais à LGPD:

[11] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13460.htm Acesso em 06/05/2021.
[12] Disponível em: https://www.ufes.br/sites/default/files/anexo-pagina/carta_de_servicos_ao_usuario_13-09.pdf Acesso em 07/05/2021.
[13] BRITO, Priscila. Escala de maturidade para *compliance* de Interfaces Digitais com a LGPD. UX *Collective*. 2020. Disponível em: < https://brasil.uxdesign.cc/escala-de-maturidade-para-compliance-de-interfaces-digitais-com-a-lgpd-ffbc5e282dfb> . Acesso em: março de 2021.

- *Consentimento*: é a solicitação da permissão do usuário sobre o tratamento dos dados fornecidos, no que se refere à coleta, utilização, armazenamento, eliminação e compartilhamento dos dados.
- *Níveis de consentimento*: trata-se de uma boa prática para obtenção de consentimento granular do usuário. Como exemplo, podemos ter um consentimento básico para viabilidade de um produto, um outro nível para solicitação da localização do usuário, com intuito de melhorar sua experiência e, um último nível, para demais iniciativas que podem potencializar ações de marketing para o produto, mas que são opcionais para a comodidade e escolha do usuário, sem imposições.
- *Retirada do consentimento*: o usuário pode a qualquer momento retirar o consentimento para o tratamento de dados.
- *Transparência*: informação para o usuário sobre como a empresa trata os dados de seus usuários. Como serão utilizados e armazenados? Serão compartilhados? Com quem? Até quando serão mantidos?
- Direitos do usuário: os usuários possuem direito ao livre acesso, atualização, correção e eliminação de seus dados.
- Política de privacidade de dados: é onde constam todas as informações sobre o tratamento dos dados que precisam ser informados ao usuário, conforme especificado na lei.

Considerando- se então que o grau de maturidade de conformidade à LGPD está relacionado à experiência de acesso aos dados pelo Usuário, conforme preconiza a LAI e, utilizando-se dos indicadores acima descritos a autora propõe uma escala de maturidade, tendo em vista a excelência na relação organização x usuário em relação à *Compliance* de Interfaces Digitais com a LGPD. Esta escala pode ser melhor compreendida com a observação da Figura abaixo:

Figura 2 – Escala de Percepção do Grau de Maturidade



Fonte: Adaptado de Brito, 2020.

1.2.1.4 Considerações sobe análise do Grau de Maturidade e Conformidade à LGPD na UFES

Em síntese, a análise do Grau de Maturidade e Conformidade da Ufes à LGPD, considerando sua interface com a LAI, indica que a avaliação aqui apresentada no Diagnóstico Inicial do Projeto LGPD, conforme citado anteriormente no item 1.1 deste documento, é válida. Identificamos que à luz da escala proposta por Brito (2020) na figura acima, a UFES avançará do nível da Percepção para o nível da Adoção, pressupondo a implementação deste Plano e seus desdobramentos.

1.2.2 Modelo metodológico para futuras Análises do Grau de Maturidade em Relação à LGPD

Gomide e Pires[14] e Santos e Ferreira[15], constituem referenciais teóricos que fundamentam modelos de maturidade utilizados em outras áreas do governo federal, sendo recorrentemente utilizados pela Controladoria Geral da União (CGU[16]) em suas publicações. Assim, constituem balizas fundamentais para qualquer proposição metodológica acerca da maturidade nas organizações, às quais aqui faremos extenso uso.

Para proposição de uma metodologia de avaliação periódica do Grau de Maturidade da UFES em relação à implementação da LGPD, o primeiro ponto a ser observado é a necessidade de definição clara do escopo de elementos a serem mensurados nesse tipo de avaliação. Estes elementos componentes do escopo do grau de maturidade devem estar vinculados à capacidade de gestão dos dados a serem protegidos. Assim, ao avaliar o grau de maturidade, direcionamos nosso olhar para a melhoria dos processos de gestão, visando ampliar a governança institucional sobre a proteção de dados pessoais.

A leitura de Gomide e Pires nos permite compreender que a metodologia para análise e mensuração do grau de maturidade na implantação de políticas públicas requer aprofundamento nos arranjos institucionais que dão sustentação à sua implementação. Desta forma, para o estabelecimento desta metodologia é necessária a atuação e a atenção sobre o conjunto de processos de trabalho que serão estabelecidos pelos Comitês Operadores de Dados, que veremos adiante, os mecanismos de gestão destes e o conjunto de normas internas aprovadas que regularão seu funcionamento. Assim, segundo os autores, o grau de maturidade na implantação de políticas resulta dos arranjos institucionais construídos.

---

[14] GOMIDE, Alexandre de Ávila; PIRES, Roberto Rocha C. **Capacidades estatais e democracia: arranjos institucionais de políticas públicas**. Brasília, Ipea, 2014. Disponível em: https://www.ipea.gov.br/portal/index.php?option=com_content&view=article&id=22066 Acesso em 06/05/2021.

[15] SANTOS, Fábio Antonio dos; FERREIRA, Rodrigo. **Avaliação de maturidade em gestão de projetos**. 2017. Disponível em: http://www.fgp.edu.br/wp-content/uploads/2017/01/P%C3%93S-Maturidade-em-Gest%C3%A3o-de-Projetos-Fabio-Santos.pdf Acesso em 06/05/2021.

[16] Disponível em: https://www.gov.br/ouvidorias/pt-br/ouvidorias/modelo-de-maturidade-em-ouvidoria-publica/referencial-teorico Acesso em 07/05/2021.

No contexto democrático, entende-se que tal capacidade pode ser entendida a partir de dois componentes: o técnico-administrativo e o político. O primeiro deriva do conceito weberiano de burocracia, contemplando as competências dos agentes do Estado para levar a efeito suas políticas, produzindo ações coordenadas e orientadas para a produção de resultados. O segundo, associado à dimensão política, refere-se às habilidades da burocracia do Executivo em expandir os canais de interlocução e negociação com os diversos atores sociais, processando conflitos e prevenindo a captura por interesses específicos (Pires e Gomide, 2014. p.20).

Pode-se compreender que a aferição do grau de maturidade futuro precisa contemplar os elementos técnicos/burocráticos em conjunto com aqueles que permitam a inclusão democrática dos titulares de dados no processo de avaliação da Adequação da UFES à LGPD. Destarte, o grau de maturidade crescerá na mesma proporção da participação ativa da sociedade na vida pública, de forma a permitir ao cidadão o constante contato, fiscalização, exposição e denúncia quanto aos processos de gestão de dados pessoais armazenados e geridos pela Universidade.

Em relação à periodicidade, será feita pelos gestores responsáveis um primeiro diagnóstico a partir da vigência deste Plano de adequação, valendo-nos da ferramenta disponibilizada pela Secretaria de Governo Digital[17], reavaliando os itens de conformidade descritos no tópico 1.1 deste plano e buscando identificar avanços e desafios ainda inconclusos. Na sequência, já na fase de implantação do Plano de Adequação da UFES à LGPD a partir do dia 01 de agosto de 2021, deverá ser realizada pelo Controlador e Encarregado, uma avaliação a cada 6 meses, durante dois anos, precedida, também, por análise de riscos a ser realizada pelos Comitês Operadores de Dados. Já em fase avançada de consolidação, após o biênio inicial, preconiza-se uma avaliação do nível de maturidade a partir de diagnóstico realizado a cada doze meses, acompanhada, também, pela avaliação de riscos realizada pelos Comitês Operadores de Dados.

A escolha por este instrumento de avaliação, pelo menos nos anos iniciais de implementação do plano de adequação da Ufes à LGPD, justifica-se pela possibilidade de medirmos a evolução institucional a partir de métrica já consolidada, avaliando a aderência da UFES aos padrões de avaliação propostos pelo Governo Federal, em especial pelo Órgão Interno de Controle, a CGU. Ademais, considerando tratar-se de ferramenta utilizada em diagnóstico inicial, permitirá o acompanhamento dos indicadores de adequação e conformidade, nas dez dimensões aferidas pelo instrumento. Feita a avaliação geral da Ufes, o Encarregado de Dados, por meio do sistema enquetes Ufes, conduzirá pesquisa junto aos gestores das Unidades de nível estratégico visando aprimorar a percepção dos usuários e melhorias atinentes à LGPD na instituição, tais como a avaliação de riscos e futuras adequações no plano de capacitação e comunicação, ferramentas fundamentais para a consolidação de uma cultura organizacional pautada na proteção de dados pessoais.

[17] Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/diagnostico-de-adequacao-a-lgpd. Acesso em 07/05/2021.

Para além da ferramenta de diagnóstico acima citada, deve-se observar a interface deste Plano de adequação da Ufes à LGPD com o Plano de Desenvolvimento Institucional Ufes 2021-30, prevendo-se ações específicas de proteção de dados nos Planejamentos Estratégicos Setoriais das Unidades Organizacionais, mediante orientações dos Comitês Operadores, do Controlador de Dados e do Encarregado.

1.3 ESTRUTURA ORGANIZACIONAL PARA GOVERNANÇA E GESTÃO DA PROTEÇÃO DE DADOS PESSOAIS

O Decreto nº 9.203, de 22 de novembro de 2017, trata a governança pública como um "conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade[18]". No âmbito organizacional, a governança é definida pelo Tribunal de Contas da União como a "aplicação de práticas de liderança, de estratégia e de controle, que permitem aos mandatários de uma organização pública e às partes nela interessadas avaliar sua situação e demandas, direcionar a sua atenção e monitorar o seu funcionamento, de modo a aumentar as chances de entrega de bons resultados aos cidadãos, em termos de serviços e de políticas públicas.[19]"

Tais mecanismos visam garantir princípios fundamentais à Instituição pública e à sociedade, como a capacidade de resposta, a integridade, a confiabilidade, a melhoria regulatória, a prestação de contas e a responsabilidade, e a transparência, aspectos intrinsicamente relacionados à Lei Geral de Proteção de Dados (LGPD). Nunca se deve perder de vista que o objetivo da Lei 13.709, de 14 de agosto de 2018, é o de "proteger os direitos fundamentais de liberdade e de privacidade, como também o livre desenvolvimento da personalidade de pessoal natural", de modo que o titular dos dados, deve ter ciência de todos os processos aos quais seus dados serão submetidos no âmbito da Ufes (tratamento, anonimização, transferências, metodologias de eliminação, etc.), fornecendo o seu consentimento mediante conhecimento de todas estas operações.

[18] Guia da Política de Governança Pública, 2018. Disponível em: https://www.gov.br/casacivil/pt-br/centrais-de-conteudo/downloads/guia-da-politica-de-governanca-publica. Acesso em 10/05/2021.
[19] (Disponível em: https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-de-governanca/. Acesso em 10/05/2021.

Por sua dimensão e complexidade de sua missão institucional, circulam pela Ufes um expressivo número de dados pessoais de estudantes, servidores técnicos e docentes, como também de colaboradores terceirizados, contratantes, público externo e mesmo colaboradores internacionais, sendo muitos destes dados de natureza sensível, ou, nos termos da LGPD, "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião pública, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural", conforme vimos acima na apresentação de conceitos.

Objetivando a melhor gestão dos dados sob sua responsabilidade e visando garantir os princípios de governança acima elencados, este Plano de Adequação propugna a estrutura organizacional que se segue, partindo-se das seguintes definições:

I. Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Em reunião do Comitê de Governança Digital da Ufes, definiu-se a figura do dirigente máximo, o Reitor, como representante da Instituição;

II. Encarregado: pessoa indicada para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Novamente, em reunião do Comitê de Governança Digital da Ufes, definiu-se a figura do Ouvidor como representante da Ouvidoria, considerando a expertise desta unidade na precípua função de comunicação com o público e no seu conhecimento de diversas normativas relacionadas à informação;

III. Operador: pessoa natural ou jurídica de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Nesta definição, a Comissão instituída pela Portaria 693, de 14 de dezembro de 2020, não encontrou no âmbito dos guias operacionais de adequação à LGPD[20] nenhuma estrutura organizacional compatível aos nossos propósitos, sobretudo, em função do volume e da **diversidade** de dados circulantes pela Instituição, de modo que, submetemos ao Comitê de Governança Digital da Ufes uma estrutura organizacional na qual seriam criados por meio de Portaria do Reitor os chamados Comitês Operadores de Dados Pessoais, divididos em função da tipologia e natureza dos dados, tal como se segue:

[20] Disponíveis em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd. Acesso em 10/05/2021.

a) **Comitê Operador de Dados Pessoais – Estudantes**: Sob responsabilidade do presidente deste comitê, agrupar-se-ão representantes das unidades administrativas que manejam mais diretamente os dados relacionados aos estudantes de graduação e pós-graduação da Ufes, em suas atividades de ensino presenciais e à distância, de pesquisa, de extensão, de alunos estrangeiros envolvidos em intercâmbios, crianças vinculadas ao CEI-CRIARTE e a Diretoria de Documentação Institucional (DDI/PROAD). Aqui também se agrupam os dados sensíveis dos estudantes vinculados à Assistência Estudantil e às Ações Afirmativas. Assim, comporão este comitê representantes da PROGRAD, PRPPG, PROEX, PROAECI, PROPLAN, SRI, SEAD, e os já citados DDI/PROAD e CEI-CRIARTE. Tal comitê possui como atribuição o desenvolvimento das operações de tratamento preconizadas no artigo n. 05 da LGPD, bem como a elaboração de termos de uso (vide exemplo constante a este Plano), observando a finalidade, adequação, necessidade, livre acesso (consulta facilitada sobre a integridade de seus dados pessoais), qualidade dos dados, transparência, segurança, prevenção, a não discriminação e a responsabilização e prestação de contas.

b) **Comitê Operador de Dados Pessoais – Servidores**: Sob responsabilidade do presidente deste comitê, agrupar-se-ão representantes das unidades administrativas que manejam mais diretamente os dados relacionados aos Servidores da Ufes, tais como documentação pessoal de servidores efetivos, dados sobre condições de saúde, análises de desempenho, transferência de informações a instituições estrangeiras, etc., de modo que comporão este comitê representantes da PROGEP, PROPLAN, DDI/PROAD (considerando o arquivamento destas informações) e SRI. Novamente, tal comitê terá como atribuição o desenvolvimento das operações de tratamento preconizadas no artigo n. 05 da LGPD, bem como a elaboração de termos de uso, observando a finalidade, adequação, necessidade, livre acesso (consulta facilitada sobre a integridade de seus dados pessoais), qualidade dos dados, transparência, segurança, prevenção, a não discriminação e a responsabilização e prestação de contas.

c) **Comitê Operador de Dados Pessoais – Contratos**: Sob responsabilidade do presidente deste comitê, agrupar-se-ão representantes das unidades administrativas que manejam mais diretamente os dados relacionados aos entes contratantes, tais como colaboradores terceirizados, ou informações pessoais atinentes a contratos e licitações, como também os dados pessoais de colaboradores temporários (substitutos e voluntários), objetivado a conformidade dos contratos como um todo. Tal comitê agrupará representantes da PROAD, PROGEP, SI, PROPLAN e DGR/PROAECI. Novamente, tal comitê terá como atribuição o desenvolvimento das operações de tratamento preconizadas no artigo n. 05 da LGPD, bem como a elaboração de termos de uso, observando a finalidade, adequação, necessidade, livre acesso (consulta facilitada sobre a integridade de seus dados pessoais), qualidade dos dados, transparência, segurança, prevenção, a não discriminação e a responsabilização e prestação de contas.

d) **Comitê Operador de Dados Pessoais – Público Externo (Pessoa Natural)**: Sob responsabilidade do presidente deste comitê, agrupar-se-ão representantes das unidades administrativas que manejam mais diretamente os dados relacionados ao Público Externo, àquele envolvido em ações de pesquisa, ensino e extensão, que de alguma forma incide em algum cadastro de informações da Ufes, tais como usuários de serviços odontológicos, da Clínica Escola / CCS, de projetos de extensão, de atendimento veterinário, de estudantes de outras instituições em intercâmbio, cooperações tecnológicas e de inovação, validação de diplomas e certificações, avaliações institucionais que envolvam dados pessoais, arquivamento, etc. Agrupar-se-ão neste comitê representantes da Ouvidoria, PROGRAD, PROEX, PRPPG, SEAVIN, IOUFES, ITUFES, HOVET, PRPPG, DDI/PROAD, Clínica Escola e outras representações que vierem a manejar dados pessoais de público externo no âmbito da Ufes. Conforme decisão do Comitê de Governança Digital, os dados de público externo relacionados ao HUCAM estarão sob governança da EBSERH. Novamente, tal comitê terá como atribuição o desenvolvimento das operações de tratamento preconizadas no artigo n. 05 da LGPD, bem como a elaboração de termos de uso, observando a finalidade, adequação, necessidade, livre acesso (consulta facilitada sobre a integridade de seus dados pessoais), qualidade dos dados, transparência, segurança, prevenção, a não discriminação e a responsabilização e prestação de contas.

e) **Comitê Operador de Dados Pessoais – Colaboradores Institucionais Externos (Pessoa Natural ou Jurídica)**: Sob responsabilidade do presidente deste comitê, agrupar-se-ão representantes das unidades administrativas que manejam mais diretamente os dados **pessoais** transacionados no âmbito de convênios e termos de cooperação estabelecidos entre a Ufes e outras instituições, e pessoas naturais nacionais e internacionais. Agrupar-se-ão neste comitê representantes da Ouvidoria, PRPPG, PROAD, PROEX, PROPLAN, Gabinete, SEAVIN. Novamente, tal comitê terá como atribuição o desenvolvimento das operações de tratamento preconizadas no artigo n. 05 da LGPD, bem como a elaboração de termos de uso, observando a finalidade, adequação, necessidade, livre acesso (consulta facilitada sobre a integridade de seus dados pessoais), qualidade dos dados, transparência, segurança, prevenção, a não discriminação e a responsabilização e prestação de contas.

A seguir, figura síntese dos Comitês Operadores acima apresentados:

Figura 3 – Comitês Operadores por tipologia documental

Fonte: elaboração própria

Conforme indicamos acima, objetiva-se com esta tipologia de dados obter ganhos de escala no tratamento de dados e na busca de conformidade dos contratos e termos de cooperação. Objetiva-se também maior organicidade, de modo que um mesmo comitê abarcará a totalidade das ações relacionadas a estudantes, servidores e público externo, por exemplo. A prerrogativa legal para tal forma de organização pode ser encontrada no artigo n. 50 da LGPD, segundo o qual "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 e as normas de segurança.

Destaca-se também o relevante papel a ser assumido pela Superintendência de Tecnologia da Informação, que ocupará funções na garantia da segurança, nas diretrizes de privacidade e na gestão de incidentes, em subsídio aos trabalhos a serem desenvolvidos pelo controlador, pelos Comitês Operadores e pelo encarregado. Será fundamental o desenvolvimento e/ou contratação de ferramentas e/ou soluções compatíveis com as demandas relacionadas à adequação da Ufes à LGPD.

Faz-se mister também, como veremos adiante, a definição de uma política de capacitação dos agentes envolvidos nestas funções, com a definição de cursos e iniciativas a serem desenvolvidas pelo Departamento de Desenvolvimento Pessoal – DDP/PROGEP, bem como a difusão de uma cultura de segurança, proteção de dados e privacidade.

1.4 PROMOÇÃO DE UMA CULTURA DE SEGURANÇA, PROTEÇÃO DE DADOS E PRIVACIDADE

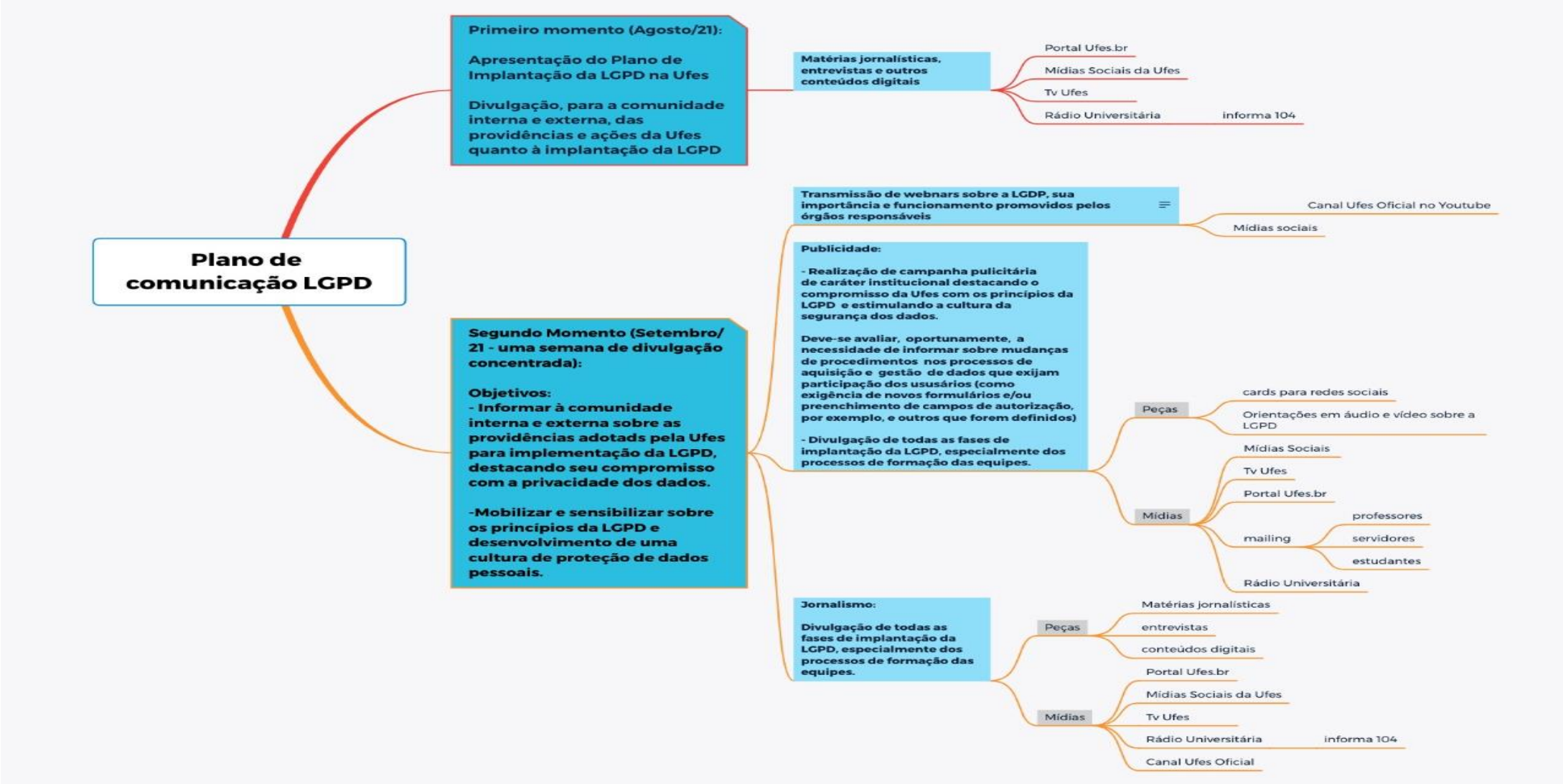
A implementação da Lei Geral de Proteção de Dados prevê alterações nos procedimentos de gerenciamento e proteção de dados pessoais, o que exigirá mobilização de segmentos técnicos diretamente implicados nas adaptações formais de documentos e de procedimentos que regem a relação entre a instituição e cada um dos seus usuários. Também será necessário o desenvolvimento, junto à comunidade interna, de uma cultura de privacidade de dados, entendendo-a como fator de fortalecimento da cidadania.

Além disso, coerente com seu compromisso de transparência dos atos da gestão universitária, é de fundamental importância dar publicidade a todo o processo de implementação da LGDP na Ufes, destacando essa ação como mais um valor positivo que se agrega à imagem da universidade. Segue-se, portanto, um diagrama contendo a síntese do Plano de Comunicação definido para esta ação a ser executado pela Superintendência de Comunicação (Supec).

Num primeiro momento, já em agosto de 2021, se prevê a divulgação deste Plano de Adequação a toda a comunidade da Ufes, bem como ao público externo, indicando as providências e ações em curso. A partir do segundo momento, com início previsto para setembro de 2021, buscar-se-á, por meio dos instrumentos na figura listados, a mobilização e sensibilização da comunidade em relação à importância da preservação da privacidade de dados pessoais a partir da LGPD. Entrementes, a promoção de uma cultura de segurança e de sensibilização dos titulares de dados e demais atores envolvidos no processo, não é tarefa estanque, prevendo-se, certamente, a perenidade de ações de comunicação em acompanhamento à LGPD e seu desenvolvimento na instituição

Neste sentido, de um acompanhamento perene às questões atinentes à LGPD na Ufes, avaliar-se-á juntamente ao controlador e ao encarregado de dados, a possibilidade de criação de um sítio eletrônico, no qual seriam publicadas informações acerca dos procedimentos de adequação da instituição à lei, bem como material de sensibilização, dados técnicos, política de privacidade, dentre outros instrumentos constantes neste plano e relacionados à matéria. Vejamos a figura abaixo:

Figura 4 – Plano de Comunicação relacionado à LGPD



Fonte: Elaboração própria

2 INVENTÁRIO DE DADOS

O Inventário de Dados Pessoais (IDP) visa atender à determinação da Lei 13.709/2018 no que se refere à manutenção e/ou tratamento de registros de dados pessoais realizados pela instituição. É um instrumento de governança essencialmente descritivo, que deve ser mantido atualizado para permitir o controle da entrada de dados pessoais e atendimento de sua finalidade, e seu monitoramento enquanto utilizado pela instituição.

Segundo o Guia de Elaboração de Inventário de Dados Pessoais[21], "a instituição pode documentar as atividades de tratamento de dados pessoais da sua organização de muitas maneiras, desde modelos básicos até pacotes de software especializados. A forma como o órgão mantém sua documentação dependerá de fatores como o tamanho da instituição, o volume de dados pessoais tratados e a complexidade das operações de tratamento".

Na proposta do modelo IDP Ufes para controle e monitoramento dos dados pessoais nas bases de dados da Universidade foram considerados fatores como o tamanho da instituição, o volume de dados pessoais tratados e a complexidade das operações de tratamento devido às características específicas da gestão universitária. Por esse motivo, foram necessárias adaptações ao modelo proposto pelo Guia LGPD para a operacionalização do inventário.

No planejamento executivo do IDP Ufes considerou-se a estrutura de governança de dados existente, pois ela já provê suporte e possui procedimentos de documentação que podem se sobrepor aos requisitos de manutenção de registros da LGPD. Assim, dentre as estratégias de implantação, está a verificação do modelo de Governança de Dados da Ufes e a proposta de implementação do IDP Ufes a partir de ajustes na estrutura de governança de dados em vigor, organizada por tipologias documentais para inventariar os dados pessoais e garantir o cumprimento dos requisitos do art. 37 da LGPD.

Seguindo o modelo proposto pelo Guia LGPD e a organização dos dados atualmente no Sistema de Informações para o Ensino (SIE), a proposta de registro descritivo do IDP-Ufes segue o disposto no quadro abaixo:

[21] Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf, acessado em junho de 2021.

Tabela 3 – Descritivo IDP-UFES

Requisito	Descrição do Requisito	Exemplos
Tipo documental	Descreve o tipo de documento ou cadastro que contém dado pessoal	Formulário de cadastro auxílio financeiro; Assentamento acadêmico; Formulário de Solicitação de Licença Capacitação;
Tipo de assinatura eletrônica	Descreve o tipo de assinatura eletrônica em cada documentos considerando que a geração ou validação da assinatura nos documentos requer base específica de dados pessoais e compartilhamento com outras bases de dados governamentais	1.Assinatura Simples 2.Assinatura Avançada 3.Assinatura Qualificada 4.Assinatura Múltipla em documento
Atores envolvidos	Cadastro individual do controlador, do encarregado e dos agentes de tratamento para delimitação de responsabilidade	
Finalidade da coleta do dado pessoal	Descreve o motivo da coleta do dado pessoal pela Ufes, registrando o que a Universidade faz com o dado pessoal contido nos documentos e cadastros em sistemas	
Hipótese legal	Identifica a(s) hipótese(s) legal(is) conforme Tabela do Guia LGPD	**Hipótese 1:** Mediante consentimento do titular; **Hipótese 2:** Para o cumprimento de obrigação legal ou regulatória ; **Hipótese 3:** Para a execução de políticas públicas ; **Hipótese 4:** Para a realização de estudos e pesquisas ; **Hipótese 5:** Para a execução ou preparação de contrato ; **Hipótese 6**: Para o exercício de direitos em processo judicial, administrativo ou arbitral ; **Hipótese 7:** Para a proteção da vida ou da incolumidade física do titular ou de terceiro; **Hipótese 8**: Para a tutela da saúde do titular; **Hipótese 9:** Para atender interesses legítimos do controlador ou de terceiro; **Hipótese 10**: Para proteção do crédito ; **Hipótese 11**: Para a garantia da prevenção à fraude e à segurança do titular;
Previsão legal	Identifica a previsão legal de acordo com especificidades e finalidade dos dados coletados	Leis, Decretos, Resoluções, Normas internas, etc.;
Comitê LGPD por categoria de dados pessoais	Descreve os agrupamentos de dados para tratamento pelos operadores	1. Estudantes; 2. Servidores; 3. Contratos; 4. Público Externo - Pessoa Natural; 5. Colaboradores Institucionais Externos - Pessoa Natural ou Jurídica;

Titular do Dado Pessoal	Categorização ou classificação descritiva dos titulares dos dados pessoais. Podem ser criadas subcategorias.	1. Beneficiários; 2. Discentes intercambistas; 3. Contribuintes; 4. Dependentes; 5. Eleitores; 6. Participante de pesquisa; 7. Discentes/Estudantes; 8. Motoristas; 9. Pacientes; 10. Docentes; 11. Servidor Técnico-Administrativo; 12. Colaboradores Terceirizados; 13. Estudantes; 14. Outros;
Dados Pessoais nos documentos (Categorias e Subcategorias)	Categorização ou classificação descritiva dos tipos de dados pessoais contidos nos documentos. Cada categoria de dado pessoal possui subcategorias e tempo de armazenamento específicos. Ver Guia LGPD.	1. Dados de Identificação Pessoal; 2. Dados financeiros; 3.Características Pessoais; 4. Hábitos pessoais; 5. Características Psicológicas; 6. Composição Familiar; 7. Interesses de Lazer; 8. Associações; 9. Processo Judicial ou Administrativo ou Criminal; 10. Hábitos de Consumo; 11. Dados Residenciais; 12. Educação e Treinamento; 13. Profissão e emprego; 14. Registros - gravações de vídeo, imagem ou voz; 15. Outros;
Dados Pessoais Sensíveis	Categorização ou classificação descritiva dos tipos de dados sensíveis contidos nos tipos documentais.	1. Origem racial ou ética; 2. Convicção religiosa; 3. Opinião política; 4. Filiação a sindicato; 5. Filiação a organização de caráter religioso; 6. Filiação ou crença filosófica; 7. Filiação ou preferências política; 8. Saúde ou vida sexual; 9. Dados genéticos; 10. Dados biométricos;
Dados Pessoais Vulneráveis	Categorização ou classificação descritiva dos documentos que contêm dados pessoais de titular em situação de vulnerabilidade.	1. Crianças e adolescentes/ 2. Outro grupo vulnerável/ 3. Não se aplica;
Tempo de retenção dos dados pessoais	Registro do tempo de armazenamento do dado pessoal.	Para cálculo do tempo de retenção verificar: 1) se existe alguma definição legal de tempo de retenção/guarda/arquivamento de documentos e/ou dos dados tratados pelo órgão e/ou entidade; 2) tabela de temporalidade de documentos do CONARQ;
Compartilhamento de dados pessoais e dados pessoais sensíveis entre instituições	Cadastro de todas as instituições que recebem dados pessoais e dados pessoais sensíveis da Ufes	

Transferência internacional de dados	Cadastro de todas as organizações internacionais que recebem dados pessoais da Ufes por meio de qualquer tipo de transferência ou meio compartilhamento	
Medidas de segurança atualmente adotadas durante todo o processo de governança de dados pessoais	Identificar as atuais medidas de segurança/privacidade aplicadas à estrutura de dados dos sistemas da Ufes	
Gestão de Contratos	Identificar as contratações de serviços ou soluções de TIC que realizam algum tipo de operação de tratamento com os dados pessoais do serviço/processo de negócio	

Fonte: elaboração própria

Devido à necessidade de ajustes na estrutura ontológica do Sistema SIE de modo a promover melhorias na parametrização dos dados e a elaboração do novo modelo de diagrama de entidade-relacionamento para estruturar a governança de dados a uma nova perspectiva de gerenciamento e segurança **(privacidade)**, propõe-se o modelo de taxonomia de dados conforme quadro abaixo:

Tabela 4 – Modelo de taxonomia de dados

Taxonomia	Tipo	Exemplos
Dados Nominais (valores multinominais ou valores binominais)	Dado estruturado – categórico/discreto	Estado civil, etnia/raça, sexo nacionalidade, naturalidade, nível educacional, opções de sim/não; verdadeiro/falso
Dados ordinais (códigos atribuídos a objetos ou eventos)	Dado estruturado – categórico/discreto	Dados para ranking, baixo/médio/alto; variáveis em grupos, ex.: grupo etário, nível de escolaridade
Dados intervalares (medido em escala intervalar)	Dado estruturado – numérico/contínuos	Temperatura
Dados racionais (escala de razão, valor zero não arbitrário)	Dado estruturado - numérico/contínuo	Medidas de massa, comprimento, ângulo planar, carga elétrica
Dados textuais	Dados não estruturado ou semiestruturado (**CONVERSÃO**)	OCR (mineração de texto)

Dados multimídia	Dados não estruturado ou semiestruturado (**CONVERSÃO**)	Imagem, áudio, vídeo e voz, espaciais (**descrição**)
XML / JSON	Dados não estruturado ou semiestruturado (**CONVERSÃO**)	Web (mineração da web)

Fonte: elaboração própria

Sendo assim, propõem-se as seguintes metas para a elaboração do Inventário de Dados Pessoais da Ufes, cujos prazos estão previstos no cronograma ao final deste Plano:

1. Elaborar meio de cadastro e/ou coleta eletrônica de informações de modo a gerar relatórios automatizados, e implementar ferramentas de gerenciamento e tratamento dos dados pessoais contidos nos documentos;
2. Analisar a estrutura de dados do SIE (Protocolo) e elaborar o Modelo ontológico e o Modelo de dados;
3. Elaborar um meio de cadastro e/ou coleta eletrônica de informações das bases de dados dos sistemas da Ufes. Verificar diagrama de dados do SIE e demais sistemas utilizados;
4. Elaborar procedimentos operacionais para cada fase de tratamento dos dados pessoais, considerando que essa etapa subsidia o papel do operador em relação ao tratamento do dado pessoal e deverá ser apresentada no Relatório de Impacto à Proteção de Dados Pessoais (RIPD):
    a. Coleta;
    b. Retenção;
    c. Processamento;
    d. Compartilhamento;
    e. Eliminação.
5. Definir o escopo e natureza dos dados pessoais tratados a serem futuramente descritos no RIPD mediante identificação da abrangência e da fonte de dados pessoais;
6. Definir os parâmetros para o tratamento dos dados pessoais e dados pessoais sensíveis e vulneráveis, considerando a necessidade de parametrizar o sistema para identificar hipóteses legais e registrar ações de consentimento, bem como associar a previsão legal do conteúdo informacional de cada tipo de documento que contém dado pessoal;
7. Promover melhorias no ambiente de cadastro de Tipologias Documentais do Sistema SIE;
8. Criar um ambiente para gestão dos dados pessoais da Ufes com implementação de *dashboards* e indicadores das fases de tratamento dos dados pessoais.

2.1 FASES DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

O modelo de implementação ou operacionalização do IDP-Ufes obedece às fases descritas no Guia para elaboração do Inventário – LGPD, sendo definidas ações executivas para o cumprimento de cada fase, conforme quadro a seguir:

Tabela 5 – Ações executivas do modelo de implementação LGPD

1 – Identificação do Serviço/Processo	
Ação 1	Levantamento das tipologias documentais cadastradas no Banco de Dados (BD) do Sistema SIE
Ação 2	Levantamento dos serviços ao cidadão que contém dado pessoal em cadastros ou execução
Ação 3	Levantamento dos processos de negócio nos Portais da Ufes
2 – Identificação dos Agentes de tratamento e Encarregado	
Ação 1	Emissão de portaria identificando o Controlador na Ufes
Ação 2	Emissão de portaria identificando o Encarregado na Ufes
Ação 3	Emissão de portarias por Comitê LGPD identificando os Agentes de tratamento
Ação 4	Cadastro de cada agente por perfil em módulo/portal de gestão LGPD
3 – Atuação do operador no ciclo de vida do dado pessoal	
Ação 1	Definir papel do operador na fase de coleta, após associar a cada tipo documental
Ação 2	Definir papel do operador na fase de retenção, após associar a cada tipo documental
Ação 3	Definir papel do operador na fase de processamento, após associar a cada tipo documental
Ação 4	Definir papel do operador na fase de compartilhamento, após associar a cada tipo documental
Ação 5	Definir papel do operador na fase de eliminação, após associar a cada tipo documental
4 – Fluxo de tratamento dos dados pessoais	
Ação 1	Descrever “passo a passo” como os documentos que contêm dados pessoais são produzidos e os dados pessoais coletados, retidos/armazenados, processados/usados e eliminados
Ação 2	Elaborar um fluxo de dados e/ou modelagem do processo de trabalho para auxiliar a modelagem e/ou ajustes do sistema
5 – Escopo e natureza dos dados pessoais	
Ação 1	Identificar a abrangência ou alcance geográfico do tratamento dos dados pessoais
Ação 2	Identificar a fonte de obtenção dos dados pessoais e definir procedimentos para assegurar os princípios da qualidade dos dados e segurança dos dados pessoais

6 – Finalidade do tratamento dos dados pessoais	
Ação 1	Identificar a hipótese legal que autoriza o tratamento dos dados pessoais ou dados pessoais sensíveis (conforme tabela do Guia LGPD)
Ação 2	Especificar a finalidade de cada serviço/processo de negócio que contém dados pessoais
Ação 3	Identificar a previsão legal de cada tipo documental que contém dados pessoais (Lei, Decreto, Resolução, Normativa Interna, etc.)
Ação 4	Após identificação e análise da hipótese legal, da finalidade e da previsão legal descrever os resultados pretendidos para o titular dos dados pessoais e os benefícios esperados pela Ufes
Ação 5	Parametrizar o sistema para atendimento das hipóteses legais: permitir o registro de consentimento do titular, permitir o registro de dispensa do consentimento do titular; permitir a verificação de autorização de compartilhamento de dados quando coletado de *Application Programming Interface* (API), identificar especificidades de obrigação legal ou regulatória, identificar a competência legal do órgão como ente regulatório, anonimizar dados pessoais de estudos ou pesquisas, etc.
7 – Categoria de dados pessoais	
Ação 1	Identificar e categorizar os dados pessoais tratados pela Ufes nas fontes: portal de serviços ao cidadão; portais administrativos e acadêmicos; banco de dados dos sistemas
Ação 2	Desenvolver formulário eletrônico a fim de cadastrar as especificidades dos dados pessoais e permitir vínculo com os tipos documentais da Ufes
Ação 3	Descrever para cada tipo documental as especificidades dos dados pessoais de acordo com as subcategorias de dados pessoais, registrando o tempo retenção do dado, a fonte de retenção ou armazenamento e o nome da base de dados de acordo com o Sistema de Catálogo de Dados mantido pela Secretaria de Governo Digital – SGD, se for o caso
8 – Categoria de dados pessoais sensíveis	
Ação 1	Identificar em cada tipo documental que contém dados pessoais a existência de dados pessoais sensíveis
Ação 2	Elaborar estratégia tecnológica para maior segurança dos processos e/ou serviços que contenham dados pessoais sensíveis
9 – Frequência e Totalização das categorias de dados pessoais tratados	
Ação 1	Parametrizar os sistemas de recebimento e/ou registro dos tipos documentais com informações sobre a disponibilidade e horário de funcionamento do sistema automatizado ou processo manual que trata os dados pessoais;
Ação 2	Parametrizar os sistemas para mensurar quantitativamente os dados pessoais tratados, em sua totalidade e por categorias
10 – Categorias de Titulares de Dados Pessoais	
Ação 1	Cadastrar os tipos e subtipos de categorias de titulares de dados pessoais
Ação 2	Identificar as categorias (tipos) de titulares a quem pertencem os dados pessoais; e se são tratados dados pessoais de crianças/adolescentes, bem como de outro grupo vulnerável em cada tipo documental

11 – Compartilhamento de dados pessoais	
Ação 1	Cadastrar todas as instituições que recebem dados da Ufes
Ação 2	Identificar todos os tipos de compartilhamento de dados pessoais e dados pessoais sensíveis por tipologia documental e/ou cadastro
Ação 3	Analisar as hipóteses legais e previsão legal para o compartilhamento de dados pessoais e justificar cada um
12 – Medidas de segurança/privacidade	
Ação 1	Identificar as atuais medidas de segurança/privacidade aplicadas a estrutura de dados dos sistemas da Ufes
Ação 2	Analisar e incluir novas medidas de segurança/privacidade considerando gestão de riscos e mitigação de incidentes
Ação 3	Cadastrar todas as técnicas administrativas implementadas e passíveis de serem implementadas para tratar incidentes de segurança/privacidade
Ação 4	Descrever os controles de segurança e elaborar fluxo dos processos que visam assegurar a integridade dos dados pessoais
Ação 5	Automatizar o processo de segurança, identificação e tratamento de incidentes
13 – Transferência internacional de dados pessoais	
Ação 1	Cadastrar as organizações internacionais que recebem dados pessoais da Ufes através de qualquer tipo de transferência ou meio compartilhamento
Ação 2	Verificar se o país estrangeiro para o qual a Ufes está transferindo dados pessoais detém legislação de proteção de dados e é reconhecida como adequada pela Autoridade Nacional de Proteção de Dados – ANPD
Ação 3	Identificar o tipo de dado pessoal ou dado pessoal sensível compartilhado
Ação 4	Identificar o tipo de garantia para transferência de dados conforme Lista do Guia LGPD
14 – Contratos	
Ação 1	Identificar as contratações de serviços ou soluções de TIC que realizam algum tipo de operação de tratamento com os dados pessoais do serviço/processo de negócio
Ação 2	Identificar os NUPs de todos os processos referentes a essas contratações
Ação 3	Identificar o contato dos gestores responsáveis por esses contratos
Ação 4	Incluir nos novos contratos cláusula para atendimento à LGPD
15 – Manutenção e atualização	
Ação 1	Revisar e atualizar anualmente, ou sempre que houver mudanças que afetem o tratamento dos dados pessoais do serviço/processo de negócio registrado no inventário

Fonte: elaboração própria

A fim de proporcionar uma visão geral dos dados pessoais coletados para elaboração do Plano de Ação do IDP-Ufes elaboramos uma Listagem Geral do inventário dos serviços/processos de negócio que tratam dados pessoais no âmbito da Ufes, conforme Anexo I, utilizando como referências o portal de serviços da Ufes e as instruções para formalização processual nas páginas eletrônicas institucionais.

Essa listagem geral identifica também o Controlador e o Encarregado da LGPD na Ufes, bem como os Comitês Operadores, de acordo com o conjunto de dados pessoais a serem tratados. Este inventário geral preliminar servirá como base e/ou guia para as ações de análise, revisão e adequação dos serviços e processos de negócio pelos Comitês Operadores, bem como para a elaboração das políticas e demais instrumentos normativos necessários à estruturação da governança dos dados pessoais.

3 TERMOS DE USO E POLÍTICA DE PRIVACIDADE

A LGPD define em seu Art 7º, Inciso I, que o tratamento de dados pessoais somente poderá ser realizado mediante o fornecimento de consentimento pelo titular. O Art. 8º ainda destaca que o "consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular".

Dessa necessidade, surge a demanda para a criação de Termos de Uso ou Contrato de Termo de Uso, que consiste num documento que estabelece as regras e condições de uso de determinado serviço. Caso o Termo de Uso seja aceito pelo usuário, a utilização do serviço será vinculada às cláusulas nele dispostas. Já a Política de Privacidade é um documento informativo pelo qual o prestador de serviço transparece ao usuário a forma como o serviço realiza o tratamento dos dados pessoais e como ele fornece privacidade ao usuário.

A Política de Privacidade tem como objetivo descrever ao usuário o método, os processos e os procedimentos adotados no tratamento de dados pessoais pelo serviço e informá-lo sobre as medidas de privacidade empregadas. Para isso, o serviço deve informar ao titular do dado como será fornecida a privacidade necessária para que a confidencialidade dos dados prestados pelos titulares dos dados seja garantida de forma eficiente, indicando as formas pelas quais os princípios previstos no Art. 6º da LGPD serão atendidos.

No conjunto de "Guias operacionais para adequação à Lei Geral de Proteção de Dados Pessoais (LGPD)", disponibilizado pela Secretaria de Governo Digital, existem importantes orientações, guias e, sobretudo, uma oportuna ferramenta para elaboração de Termo de Uso e Política de Privacidade[22]. Essa Ferramenta consiste em um modelo responsivo, estruturado para que ao final do processo de preenchimento seja gerado o Temo de Uso e Políticas de Privacidade para o serviço em questão. O preenchimento é dividido nas seguintes etapas:

1ª Informações do serviço

Onde será preenchido o nome do serviço para o qual o Termo de Uso será elaborado e os detalhes do serviço, contendo responsável pela prestação do serviço, escopo e finalidade.

2ª Definições

[22] Disponível em: https://limesurvey.sgd.nuvem.gov.br/index.php/759958?lang=pt-BR. Acesso em 19/05/2021.

Para melhor compreensão do usuário do serviço, é necessário definir termos relevantes que devem constar no Termo de Uso. Para padrão de escolha, o questionário possui definições pré-estabelecidas para: Dado pessoal, Titular, Controlador, Operador, Encarregado, Agentes de Tratamento, Tratamento, Uso compartilhado de dados, Autoridade nacional, Agente público, Agentes de Estado, Códigos maliciosos, Internet, Sítios e aplicativos, Terceiro, Usuários (ou "Usuário", quando individualmente considerado). A Ferramenta ainda permite acrescentar novas definições para adequar o termo ao serviço em questão.

3ª Base Legal

Semelhante à etapa anterior, a Ferramenta apresenta uma lista de instrumentos legais que devem ser selecionados de acordo com os que apresentam relação direta com a utilização de sítios, sistemas ou aplicativos para dispositivos móveis do serviço. Também é possível acrescentar legislação não presente na listagem pré-estabelecida.

4ª Controlador, Operador e Encarregado

Etapa de preenchimento com as informações do Controlador, Operador e Encarregado do serviço. Em relação aos Comitês Operadores, deverá ser lançado na ferramenta o nome de seu presidente, em consonância com a estrutura de governança acima apresentada.

5ª Política de Privacidade

Nesta etapa, são apresentados dados que deverão ser selecionados na medida em que forem tratados pelo serviço. Na listagem pré-estabelecida é possível selecionar os dados: Nome completo, Nome social, Data de nascimento, Sexo, Filiação, Nacionalidade, Naturalidade, Número de inscrição no CPF, Situação cadastral no CPF, Estado civil, Endereço de e-mail, Endereço, Número de telefone, RG, Dados do dispositivo (modelo de hardware, sistema operacional), Localização do usuário, Registro de acesso, Foto do usuário. Também é possível acrescentar dados não presentes na listagem pré-estabelecida.

6ª Política de Privacidade - Coleta, finalidade e tratamento

Etapa destinada ao preenchimento de:

- Forma de coleta dos dados;
- Finalidade dos dados coletados;
- Tratamento realizado com os dados.

7ª Dados de crianças e adolescentes

Etapa destinada a identificar se o serviço faz algum tratamento de dados pessoais de crianças e adolescentes.

8ª Compartilhamento

Etapa destinada a identificar se os dados pessoais utilizados no serviço são compartilhados.

9ª Segurança

Etapa destinada a identificar se o serviço utiliza criptografia em toda comunicação que realiza com o titular dos dados, de forma a fornecer confidencialidade dos dados pessoais e informações que trafegam entre o titular e o provedor.

10ª Cookies

Etapa destinada a identificar se o serviço utiliza cookies.

11ª Alterações

Etapa destinada a identificar, com relação à alteração nos Termos de Uso, como será procedida a notificação ao usuário, sendo permitida uma resposta entre: i) O usuário será notificado pelo serviço a caso haja alterações em seu Termo de Uso ou Política de Privacidade; ou ii) O usuário NÃO será notificado pelo serviço a caso haja alterações em seu Termo de Uso ou Política de Privacidade, e é responsabilidade do usuário consultá-los frequentemente.

12ª Foro

Etapa destinada a identificar a comarca responsável por dirimir qualquer reclamação ou controvérsia com base no Termo elaborado.

13ª Transferência internacional de dados

Etapa destinada a identificar se o serviço a realiza transferência internacional de dados.

14ª Documento Final

Etapa na qual o documento contendo o Termo de Uso e Política de Privacidade, gerados a partir das respostas, com o auxílio da ferramenta, será definido pelos Comitês Operadores de Dados. Como vimos acima, tais comitês possuem como atribuição o desenvolvimento das operações de tratamento preconizadas no artigo n. 05 da LGPD, bem como a elaboração de termos de uso, observando a finalidade, adequação, necessidade, livre acesso (consulta facilitada sobre a integridade de seus dados pessoais), qualidade dos dados, transparência, segurança, prevenção, a não discriminação e a responsabilização e prestação de contas, em consonância com a Carta de Serviços da Organização.

4 RISCOS DE SEGURANÇA E PRIVACIDADE

4.1 POLÍTICAS E PRÁTICAS PARA PROTEGER A PRIVACIDADE DO CIDADÃO

Com o intuito de organizar e melhor apresentar as metas e tarefas relacionadas ao estabelecimento de uma política para a proteção de dados pessoais, apresentamos as tabelas abaixo, cujo objetivo é especificar as ações relacionadas à construção de uma política e de práticas (instrumentos operacionais). Tais ações envolvem a elaboração de resoluções específicas por parte do Conselho Universitário, como também a definição de conceitos e princípios (muitos dos quais já apresentados neste plano) por parte do Comitê de Governança Digital, da Superintendência de Tecnologia da Informação e dos Comitês Operadores da LGPD. O cronograma destas ações segue ao final do Plano:

Tabela 6 – Políticas e Práticas para proteger a privacidade dos cidadãos

POLÍTICAS PARA PROTEÇÃO DE DADOS PESSOAIS	
RESOLUÇÃO DO CUn	**Meta 1: Elaborar Minutas para submeter ao CUn**
1. Política de Governança e Proteção de Dados	Tarefa 1.1: Declaração institucional – (OBS: resolução direcionada ao público externo)
2. Política de Privacidade e Proteção de dados pessoais	Tarefa 1.2: Estabelecer o conjunto de conceitos, princípios, diretrizes, delimitações e responsabilidades aplicáveis à privacidade e proteção dos dados pessoais tratados na Ufes a fim de guiar o fluxo de informações: - abranger qualquer operação de tratamento de dados pessoais sob a responsabilidade da universidade (dados pessoais sensíveis e não-sensíveis) - informar quais dados serão coletados e as categorias de dados pessoais (Comitês) - estabelecer como os dados serão processados (Comitês) - informar princípios seguidos no tratamento de dados pessoais, conforme LGPD: *finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas* - informar as diretrizes para adequação de processos e procedimentos existentes e para aprovação de novos processos - informar as ações de conscientização da comunidade universitária - informar instrumentos operacionais - informar mecanismos de tratamento dos dados (sugere-se utilizar taxonomia dos dados) - informar sobre requisitos de segurança e boas práticas - informar as responsabilidades da comissão/comitê de proteção de dados pessoais da Ufes - estabelecer os processos de mitigação dos riscos (OBS: resolução direcionada principalmente aos servidores)
3. Política de Segurança da Informação (POSIC) ou Política de Segurança Cibernética	Tarefa 1.3: Minuta em elaboração pela STI

4. Política de *Cookies* para Sites Institucionais	Tarefa 1.4: Sugere-se minuta para complementar a Política de Governança e Proteção de Dados
5. Política de Gestão e Preservação de Documentos Arquivísticos (digitais e não digitais)	Tarefa 1.5: Minuta em elaboração pela DDI/Proad e Comissão própria)
INSTRUÇÕES NORMATIVAS	**Meta 2: Elaborar minutas de instruções normativas a serem publicizadas pelos Portais e UE**
1. Instrução Normativa LGPD para os Comitês Operacionais	Tarefa 2.1: Considerar tipologia documental, termos de uso e políticas de privacidade por serviços
2. Instrução Normativa LGPD para cada medida de segurança	Tarefa 2.2: Considerar indicação de ações técnicas e administrativas para cada medida
3. Instrução Normativa LGPD para inclusão de novo dado pessoal no Inventário Dados Pessoais	Tarefa 2.3: Sugerir formulário para cadastro de novas ações que necessitem de coleta de dados pessoais
4. Instrução Normativa LGPD para Uso das Tecnologias Internas da Ufes	Tarefa 2.4: Usar como referência inventário dos Sistemas que tratam dados pessoais

Fonte: elaboração própria

Tabela 7 – Práticas para proteger a privacidade dos cidadãos

PRÁTICAS PARA PROTEÇÃO DE DADOS PESSOAIS	
INSTRUMENTOS OPERACIONAIS	**Meta 3: Elaborar Instrumentos operacionais para execução da LGPD**
1. Programa de Segurança de Dados Pessoais –	Tarefa 3.1: definir as medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito podem ser descritas em Instruções Normativas Específicas: - Proposta de gestão de dados pessoais - Plano de resposta a incidentes de segurança em dados pessoais
2. Cartilha de Boas Práticas e Governança	Tarefa 3.2: Desenvolver cartilha como link em página web ou aplicativo, com ferramentas para acessibilidade as informações
3. Inventário de Dados Pessoais	Tarefa 3.3: Elaborar meio de cadastro e/ou coleta eletrônica de informações a fim de gerar relatórios. Modelo ontológico e Modelo de dados
4. Inventário de Sistemas que tratam dados pessoais	Tarefa 3.4: Elaborar meio de cadastro e/ou coleta eletrônica de informações
5. Plano de Gestão de riscos de segurança e privacidade	Tarefa 3.5: Utilizar Modelo LGPD
6. Plano de Preservação de documentos digitais (nato digitais/digitalizados)	Tarefa 3.6: Elaborar com base na Política de Gestão e Preservação de Documentos Arquivísticos. Cadastro/coleta dos metadados de preservação
7. Guia para elaboração de termos de uso e políticas de privacidade para utilização dos serviços fornecidos pela universidade	Tarefa 3.7: Elaborar Guia como link em página web ou aplicativo, com ferramentas para acessibilidade às informações
8. Guia para anonimização de dados pessoais	Tarefa 3.8: Elaborar Guia como link em página web ou aplicativo, com ferramentas para acessibilidade às informações
9. Guia com os requisitos mínimos necessários de Segurança da Informação e Privacidade em contratações de Soluções de Tecnologia da Informação	Tarefa 3.9: Elaborar Guia como link em página web ou aplicativo, com ferramentas para acessibilidade às informações

10. Guia de Segurança em Aplicação *Web*	Tarefa 3.10: Elaborar Guia como link em página web ou aplicativo, com ferramentas para acessibilidade às informações
11. Guia de *Framework* de Segurança	Tarefa 3.11: Elaborar Guia como link em página web ou aplicativo, com ferramentas para acessibilidade às informações
12. Relatório de impacto à proteção de dados pessoais (RIPD)	Tarefa 3.12: Utilizar Modelo LGPD. Sugestão: Elaborar meio de geração eletrônica do relatório, baseado no cadastro de riscos dos dados pessoais. Definir periodicidade de publicização do RIPD (anual/semestral/mensal)

Fonte: elaboração própria

4.2 DIRETRIZES DE PROTEÇÃO DE DADOS PESSOAIS E PRIVACIDADE

A Universidade Federal do Espírito Santo (UFES), além da sua função última, tem a responsabilidade legal de elaborar a **Política de Segurança da Informação e Comunicações (POSIC)**[23].

A Política de Segurança da Informação e Comunicações (POSIC) é uma declaração formal acerca do compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda. Esta política deve direcionar a Universidade Federal do Espírito Santo (UFES) na gestão dos riscos e no tratamento dos incidentes de Segurança da Informação e Comunicações (SIC), por meio da adoção de procedimentos e mecanismos que visam à eliminação ou redução de ocorrência de modificações não autorizadas, garantindo confidencialidade, integridade e autenticidade, bem como a disponibilidade de recursos e sistemas críticos para assegurar a continuidade do funcionamento da UFES.

Esta Política deve sempre estar em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de Segurança da Informação e Comunicações (SIC), e aplica-se a todas as unidades e entidades vinculadas à Universidade Federal do Espírito Santo, bem como a todos os membros da comunidade universitária (incluindo alunos, docentes, servidores técnico-administrativos, estagiários, colaboradores terceirizados, dentre outros) e qualquer pessoa (agente público ou particular) que, oficialmente, execute atividade vinculada à atuação institucional da UFES.

Assim sendo, é necessário, de forma consistente e continuada, divulgar para a Comunidade Acadêmica as “boas práticas” que envolvem a segurança da informação e comunicações, orientando e aumentando o nível geral de conhecimento da matéria. Um dos maiores desafios na elaboração da POSIC é o mapeamento dos eventos de risco nestas áreas (Informação e Comunicações), para seu controle, e minimização de eventuais problemas, através da elaboração de um plano de gestão de riscos na organização, que doravante, incorporará os aspectos atinentes à LGPD.

[23] Disponível em: https://nti.ufes.br/sites/npd.ufes.br/files/field/anexo/posic_2019-2021.pdf Acesso em 29/05/2021.

No escopo da gestão de riscos é possível: identificar os riscos; definir a probabilidade de ocorrência; identificar a forma de avaliar o seu impacto e definir ações futuras para cada possível incidente. É importante notar que as fontes de riscos podem ser ações internas ou externas à organização. Com o Plano de Gestão de Riscos, tendo a função de avaliar todo cenário, fica melhor compreendido o nível potencial de controle e planejamento de ações em relação à ocorrência dos riscos e para a LGPD. O risco do projeto é um evento ou condição incerta que, se ocorrer, tem um efeito positivo ou negativo em um ou mais objetivos do projeto.

Os riscos são o reconhecimento de que eventos incertos podem ocorrer e, ao identificá-los, podemos antecipar e organizar as melhores estratégias para a sua gestão. Destarte, um risco não necessariamente afeta de modo negativo a instituição, pois, a partir de sua identificação, é possível que possa trazer benefícios (o que é reconhecido como risco positivo ou oportunidade, em diferenciação àqueles que imputam, de fato ameaças à Instituição, conhecidos como riscos negativos). Em geral, reconhece-se que o risco possui apenas uma dimensão negativa, que ameaça o funcionamento das organizações, mas os riscos positivos podem ser benéficos, como exemplo: o diagnóstico de insuficiência de ferramentas de anonimização de dados pessoais e o levantamento dos riscos a ele relacionados pode redundar em melhorias na gestão de contratos, trazendo boas soluções com preços competitivos.

Com o advento da Lei Geral de Proteção de Dados (LGPD), faz-se necessária a adequação da gestão de riscos, com foco na segurança e **privacidade** da informação. Além disso, há necessidade do melhor reconhecimento das informações da Instituição, através de seus processos, vinculando a eles as operações de tratamento preconizadas na Lei. Como sugere a LGPD, os agentes de tratamento devem adotar medidas de segurança e técnicas aptas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado (LGPD, art. 46).

É importante diferenciar as ações de risco vigentes e a necessidade de adequação, com viés de proteção dos dados pessoais (privacidade). Entendemos que a POSIC é um elemento importante de conscientização no uso adequado das tecnologias quando orienta, por exemplo, para a necessidade de uso do e-mail institucional para comunicação. Ou, também, quando indica maior cuidado com as senhas para uso pessoal e intransferível. Essas e outras ações estão determinadas na POSIC da UFES. Também, com a gestão de riscos, estão contempladas as ações preconizadas pela LGPD em relação ao armazenamento, preservação, uso e eliminação da informação. Faz-se necessário, contudo, avançar no processo de transparência, no sentido de que o titular dos dados seja conhecedor dos processos e tratamentos que os dados que a ele pertencem percorrerão no âmbito da Instituição.

Isto posto, entende-se que a continuidade da Gestão de Riscos e da Política de Segurança da Informação é extremamente importante, e que as adequações de ambas são cruciais para se atingir a boa abordagem da empregabilidade do conceito de **privacidade** dos dados pessoais desde a sua concepção (*Privacy by design*), colocando o desafio aos setores de desenvolvimento de soluções e ferramentas. Espera-se que, com as devidas adequações, a Instituição possa antecipar os eventos negativos, no que se refere à gestão dos dados pessoais, evitando as suas ocorrências. Estas deverão ser atualizadas para atender à gestão de dados pessoais, assim como observar as instruções normativas internas e os marcos legais e regulatórios previstos para além da LGPD.

4.3 AVALIAÇÃO DE RISCOS

Conforme nos ensina a Secretaria de Governo Digital, o Decreto nº 9.203, de 22 de novembro de 2017, dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Ele estabelece que **gestão de riscos** é o processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos (art. 2º, inciso IV). O decreto também informa que uma das diretrizes da governança pública é implementar controles internos fundamentados na gestão de risco, que privilegiará ações estratégicas de prevenção antes de processos sancionadores (art. 4º, inciso VI)[24]. É tarefa premente o estabelecimento, manutenção, monitoramento e aprimoramento do sistema de gestão de riscos e controles internos com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos que possam impactar a implementação da estratégia e a consecução dos objetivos da organização no cumprimento da sua missão institucional, observados os princípios indicados no decreto (art. 17).

Apresentada esta definição de gestão de riscos, lançamos mão, aqui, de dois documentos produzidos pela Ufes, a POSIC - Política de Segurança de Informação e Comunicações (2019-2021[25]), chancelado pelo Comitê de Governança Digital da Ufes, e o PDTIC – Plano Diretor de Tecnologia da Informação e Comunicação (2017-20[26]). Estes instrumentos apresentam a questão da gestão de riscos como central na estruturação das Tecnologias da Informação, identificando a adoção de abordagem sistemática do processo de Gestão de Risco da Segurança da Informação e Comunicações (GRSIC), conforme preconizado na Norma Complementar 04/IN01/DSIC/GSI/PR e na Norma ABNT NBR ISO/IEC 27005:2011, com o objetivo de manter os riscos em níveis aceitáveis. No caso da Ufes, o processo de GRSIC é definido pelas atividades de:

[24] Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/gestao-riscos. Acesso em 12/05/2021.
[25] Disponível em: https://nti.ufes.br/sites/npd.ufes.br/files/field/anexo/posic_2019-2021.pdf. Acesso em 12/05/2021.
[26] Disponível em: https://npd.ufes.br/sites/npd.ufes.br/files/pdtic-ufes-2017-2020.pdf . Acesso em 12/05/2021.

• Análise de contexto e identificação de requisitos de Segurança da Informação e Comunicações (SIC);

• Identificação da possibilidade de ocorrência de tais eventos e dos impactos associados;

• Levantamento dos ativos pertencentes aos grupos de risco;

• Definição do valor dos ativos;

• Classificação dos riscos segundo o grau de probabilidade, o impacto e as consequências para a segurança da informação;

• Definição da estratégia de aceitação dos riscos;

• Definição do plano de tratamento de riscos, que podem incluir, mas não estão restritos, a aquisição de hardware, aquisição de software, definição de processos, alocação de pessoal, estratégia de comunicação, sistema de documentação, contratação de serviços, entre outros;

• Implementação do plano de tratamento dos riscos;

• Monitoração e análise crítica;

• Melhoria do processo de GRSIC; e

• Comunicação do risco.

Tal como preconizado em nossa POSIC, o processo de GRSIC deve ser contínuo e deve utilizar indicadores que permitam a avaliação, auditoria e acompanhamento, e estar alinhado ao modelo denominado PDCA (*Plan-Do-Check-Act*), conforme definido na Norma Complementar nº 02/IN01/DSIC/GSIPR, visando fomentar a sua melhoria contínua. A sua implementação e operação deverá produzir subsídios para suportar a Segurança da Informação e Comunicações (SIC) e a Gestão de Continuidade de Negócios. A regulamentação da Gestão de Risco deverá ser feita por meio de Norma Complementar (POSIC/UFES, 19, 2021).

Já o PDTIC apresenta, em termos gerais, fatores de risco atrelados ao seu desenvolvimento, que em certo sentido, são também fatores correlacionados à adequação da instituição à LGPD. São eles:

- Falta de recursos para aquisição de equipamentos;
- Falta de recursos para aquisição de insumos;
- Falta de recursos para contratação de serviços de TIC;
- Falta de recursos para contratação de serviços de treinamento;
- Falta de recursos humanos com formação adequada (Inviabilidade de contratação);
- Dificuldades burocráticas para a efetivação das ações.

Em face dos fatores de risco, faz-se necessário um treinamento constante para os técnicos de TIC e demais servidores e usuários (previstas adiante), assim como o estabelecimento de um programa de divulgação e esclarecimento para os usuários finais acerca da LGPD.

Em relação à LGPD, tanto o Inventário de Dados Pessoais quanto o Relatório de Impacto de Proteção de Dados (RIPD) são instrumentos essenciais na mitigação dos riscos, contudo, é fundamental que o encarregado tenha **independência** para determinar a aplicação de recursos e as ações necessárias, bem como o pronto apoio das unidades administrativas no atendimento às solicitações de informações em relação às operações de tratamento de dados pessoais. O encarregado também deve ter amplo acesso à estrutura organizacional, investigar proativamente os níveis de conformidade e instruir os responsáveis pelos riscos – os comitês operadores de dados - a corrigir as lacunas eventualmente encontradas.

É válido destacar que o apoio da alta administração é essencial para o sucesso do trabalho a ser executado pelo encarregado, incluindo seu envolvimento nas decisões e recursos suficientes para pessoal, treinamento, entre outros, na medida de suas possibilidades. Os órgãos da Administração Pública também devem assegurar ao encarregado uma estrutura organizacional suficiente para governança e gestão da proteção de dados pessoais, demanda para a qual foram arquitetados os Comitês Operadores de Dados, conforme tópico 1.3. Nessa linha, o encarregado necessita também de autonomia e independência funcional para avaliação das atividades de tratamento de dados pessoais realizadas pelo órgão e um contínuo aperfeiçoamento por meio de treinamentos e capacitações realizadas com segurança da informação e proteção de dados pessoais.

4.3.1 Avaliação de riscos de segurança e privacidade

Em relação à LGPD, dois instrumentos relevantes foram disponibilizados pela Secretaria de Governo Digital (SGD). São eles: o Guia de Avaliação de Riscos de Segurança e Privacidade - LGPD[27] e o Guia de Boas Práticas - LGPD[28]. O primeiro nos fornece importantes referências e definições acerca das dimensões de estrutura, sistema e privacidade, abaixo sumarizadas:

- **Estrutura**: Nesta dimensão são avaliados controles que tratam de aspectos estruturais do sistema (processos e infraestrutura que o sustentam), características de ambiente que expandem a análise, mas também é indispensável para identificar o estado atual da segurança e privacidade na organização responsável pelo tratamento de dados pessoais;

[27] Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_avaliacao_riscos.pdf . Acesso em 22/05/2021
[28] Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf Acesso em 22/05/2021.

- **Sistema**: tem alicerce no processo de *Security-by-Design*, ou seja, os controles de segurança propostos visam incorporar a segurança da informação durante todo o ciclo de vida do sistema, e consequentemente auxiliam a redução da superfície de ataque para vulnerabilidades de sistema. A dimensão inclui temas como: desenvolvimento seguro, controles de acesso lógico, segurança web e outros. É importante reforçar que a instituição é livre para alterar, incluir ou excluir os controles, adequando este documento à realidade e à criticidade do sistema. Há sistemas críticos que o duplo fator de autenticação (ou o certificado digital) é de fundamental uso para elevar o nível de confiabilidade nas transações executadas no sistema, enquanto em outros casos com baixo risco (baixa probabilidade e baixo impacto) o seu uso pode ser dispensado. Portanto, identificar as lacunas e adaptar este documento à realidade do sistema é uma responsabilidade do controlador e deve sempre estar relacionada à gestão de riscos institucional;
- **Privacidade**: Os controles nesta dimensão estão relacionados ao alcance da conformidade legal com a privacidade de tratamento de dados pessoais. Os controles permitirão que o controlador analise o sistema que trata dados pessoais e verifique se os requisitos de adequação à privacidade estão sendo atendidos.

A partir destas dimensões, são apresentadas as respectivas descrições dos objetivos de controle, como também os riscos e seus escopos. São eles: acesso não autorizado, coleção excessiva, compartilhar ou distribuir dados pessoais com terceiros fora da administração pública federal sem o consentimento do titular dos dados pessoais, falha em considerar os direitos do titular dos dados pessoais (ex.: perda do direito de acesso), falha ou erro de processamento, informação insuficiente sobre a finalidade do tratamento, modificação não autorizada, perda, reidentificação de dados pseudonimizados, remoção não autorizada, retenção prolongada de dados pessoais sem necessidade, roubo, tratamento sem consentimento do titular dos dados pessoais e vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular. O Guia de avaliação de riscos à segurança e privacidade também apresenta uma tipologia de riscos (baixo, moderado e alto), dispostos numa matriz de risco composta por probabilidade x impacto.

A partir de uma série de ponderações presentes ao guia supracitado, o mesmo disponibiliza uma **ferramenta** para avaliação de riscos à segurança e à privacidade[29], constituída por um questionário que tem por objetivo realizar uma avaliação dos sistemas que tratam dados pessoais. É composto por 113 perguntas (controles) centradas nos eixos de segurança da informação e privacidade. Cada pergunta possui uma ou mais referências para maior detalhamento sobre o questionamento e teve como linha de base as Normas Complementares do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), o Guia de Boas Práticas da LGPD, a Metodologia de Gerenciamento de Integridade, Riscos e Controles Internos da Gestão do Ministério do Planejamento, Desenvolvimento e Gestão, as ISO 27001, 27002, 27005, 29100, 29134, 29151 e 31000, o NIST, OWASP, entre outras.

Contudo, conforme alertado pelo próprio guia, não é a ferramenta um questionário exaustivo e, dessa forma, ainda demandará uma análise crítica do responsável pelo sistema diante das peculiaridades que possa vir a ter. O questionário tem como propósito atuar no sistema que trata dados pessoais e por esse motivo está alinhado aos 14 riscos identificados no Guia de Boas Práticas da LGPD, cujo link fora acima apresentado.

Neste sentido, insta destacar que os instrumentos gerais já definidos pela instituição relacionados à avaliação de risco, à segurança e à privacidade dos dados, podem também ser direcionados à análise atinente à LGPD, visto que já foram elaborados à luz da metodologia de gestão de riscos da CGU[30]. Tais planilhas[31] seguem anexas a este plano, como instrumentos que podem vir a ser complementares à ferramenta disponibilizada pela Secretaria de Governo Digital por meio de seus guias anteriormente citados.

5 ADEQUAÇÃO DE CONTRATOS

Os contratos e convênios constituem temas sensíveis na adequação da Ufes à LGPD. Em face dessa constatação, fora previsto acima, no tópico 1.3, o estabelecimento de dois Comitês Operadores de Dados Pessoais específicos para, respectivamente, contratos e colaboradores institucionais externos (Pessoa Natural ou Jurídica). Tais comitês serão formados por representantes de unidades administrativas mais afeitas a estes instrumentos, cabendo-lhes as funções anteriormente descritas no sentido de garantir a conformidade dos processos de contratualização da Ufes aos ditames da LGPD. Abaixo seguem algumas adequações contratuais pertinentes aos modelos de contrato praticados pela DCOS/PROAD (Diretoria de Contratação de Obras e Serviços) e DPI/PROAD (Diretoria de Projetos Institucionais), ambas vinculadas à Pró-Reitoria de Administração:

a) Proposta de cláusula contratual para contratações de Obras e Serviços (DCOS):

[29] Ferramenta disponível em: https://pesquisa.sisp.gov.br/index.php/468289 Acesso em 30/05/2021.
[30] Disponível em: https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/institucionais/arquivos/cgu-metodologia-gestao-riscos-2018.pdf . Acesso em 30/05/2021.
[31] Anexo II, III e IV do presente plano.

1- Nos termos do inciso I do art. 7º da Lei nº 13.709 de 2018, os representantes da Licitante/Contratada autorizam a utilização de dados pessoais, pela Contratante, para os fins legais dispostos no referido diploma legal, permitindo sua divulgação em sítios próprios, bem como na confecção de documentos internos ou públicos.

1.1- Os representantes da Licitante/Contratada declaram estar cientes de que os dados pessoais de seus sócios, diretores, prepostos e afins, indicados para figurar nas etapas da contratação e execução contratual estão sujeitos à publicidade prevista na Lei de Licitações e legislação correlata.

1.2- Os dados de que trata o caput e o item anterior poderão ser tratados pela Contratante / UFES, sem a necessidade de anuência específica, para fins de cumprimento de formalidades legais.

b) Proposta de cláusula contratual para Projetos Institucionais (DPI):

1- Nos termos do inciso I do art. 7º da Lei nº 13.709 de 2018, os representantes da Contratada e participantes dos projetos autorizam a utilização de dados pessoais, pela Contratante, para os fins legais dispostos no referido diploma legal, permitindo sua divulgação em sítios próprios, bem como na confecção de documentos internos ou públicos.

1.1- Os representantes da Contratada e participantes dos projetos, declaram estar cientes de que os dados pessoais, como CPF e registros funcionais estão sujeitos à publicidade prevista na Lei 8.958 de 20/12/94, Decreto 7.423 de 31/12/10 e legislação correlata.

1.2- Os dados de que trata o caput e o item anterior poderão ser tratados pela Contratante / UFES, sem a necessidade de anuência específica, para fins de cumprimento de formalidades legais.

Para participantes de projetos institucionais, ainda é estabelecido termo de consentimento, conforme modelo no Anexo V deste plano.

Tais alterações vêm ao encontro das operações de tratamento preconizadas no artigo n. 05 da LGPD e deverão estar presentes nos termos de uso de dados pessoais e consentimento que serão elaborados pelos respectivos comitês, que deverão ser explícitos em relação à finalidade das alterações, sua adequação, sua pertinência e sua necessidade, sem, contudo, afetar os itens atinentes à transparência presentes na Lei 14.133, de 01 de abril de 2021[32]. Anexo a este plano seguirão alguns modelos de contrato e convênios, com vistas a subsidiar a confecção de futuros instrumentos em conformidade com a LGPD.

[32] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14133.htm. Acesso em 20/05/2021.

6 RELATÓRIO DE IMPACTO E PROTEÇÃO DE DADOS

O Relatório de Impacto à Proteção dos Dados Pessoais (RIPD) representa um instrumento importante de verificação e demonstração da conformidade do tratamento de dados pessoais realizado pela instituição e serve tanto para a análise quanto para a documentação do tratamento dos dados pessoais.

O RIPD visa descrever a avaliação dos riscos nas operações de tratamento de dados pessoais que são coletados, tratados, usados, compartilhados e quais medidas são adotadas para mitigação dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados.

Sua definição está formalizada no inciso XVII do art. 5º da LGPD, no entanto, o seu conteúdo mínimo é indicado pelo parágrafo único do art. 38, grifado abaixo.

> Art. 38. **A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais**, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
>
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, 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 controlador com relação a medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

Sendo assim, o RIPD é uma documentação que deve ser mantida pelo Controlador dos dados e pode ser solicitada a qualquer momento, sob determinação da ANPD. Sua elaboração deve contemplar as seguintes etapas:

1. Identificar os Agentes de Tratamento e o Encarregado;
2. Identificar a necessidade de elaborar o Relatório;
3. Descrever o tratamento;
4. Identificar partes interessadas consultadas;
5. Descrever necessidade e proporcionalidade;
6. Identificar e avaliar os riscos;
7. Identificar medidas para tratar os riscos;
8. Aprovar o Relatório;
9. Manter Revisão.

É importante destacar que o RIPD deve ser revisto e atualizado anualmente ou sempre que existir qualquer tipo de mudança que afete o tratamento dos dados pessoais realizados. Com essa boa prática a instituição demonstra que avalia continuamente os riscos de tratamento de dados pessoais que surgem em consequência do dinamismo das transformações tecnológicas. Sua elaboração está prevista em cronograma previsto ao final deste Plano.

7 RESPOSTA A INCIDENTES DE SEGURANÇA EM DADOS PESSOAIS

No âmbito da segurança e do sigilo de dados pessoais, a LGPD preceitua em seu Art. 48 que "o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares"

Em consonância, o Guia de Boas Práticas ainda sugere:

> Definir um plano de comunicação para incidentes de violação de dados. O objetivo é propiciar maior celeridade na solução de incidentes e padronização de atividades a serem executadas, assim como prever responsáveis pelo cumprimento das atividades.
>
> Documentar violações atestadas e incidentes ocorridos, a fim de analisar riscos de violação periodicamente.

Conforme abordado no item 4.1 deste plano, dentre as Práticas para Proteção de Dados Pessoais, deverá ser estabelecido um Programa de Segurança de Dados Pessoais contendo plano de resposta a incidentes de segurança em dados pessoais, conforme indicado no cronograma presente ao final deste Plano.

Ratifica-se, conforme as diretrizes gerais estabelecidas na POSIC-Ufes, mencionada anteriormente neste plano, que "a estrutura de suporte à Gestão de Segurança da Informação e Comunicações – GSIC será composta pelo Gestor de SIC, pelo Comitê de Segurança da Informação e Comunicações – CSIC e pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR".

As formas de tratamento de incidentes de segurança da informação seguirão conforme estabelecido no item 7.2, da POSIC-Ufes.

Destaca-se ainda a proposta de se abordar a temática de "resposta a incidentes de segurança em dados pessoais" em ações de capacitações, conforme apresentado no capítulo 8, a seguir.

8 AÇÕES DE CAPACITAÇÕES

8.1 PLANO DE CAPACITAÇÃO

Diante do contexto apresentado e no escopo da adequação da Ufes à LGPD, propõe-se a adoção de um plano de capacitação que tem por objetivo orientar os membros da comunidade universitária e usuários dos serviços prestados pela Ufes sobre a Lei Geral de Proteção de Dados Pessoais (LGDP) e o processo de adequação da universidade.

A proposta do plano de capacitação segue os direcionamentos conforme listados, a seguir:

8.2 METAS E RESULTADOS ESPERADOS

Apresentar o processo de adequação da Ufes, as estruturas, os documentos e procedimentos da LGPD, demonstrando os impactos na vida pessoal e profissional dos membros da comunidade universitária.

Espera-se que a comunidade universitária possa participar de todas as etapas dos processos de adequação para conhecer e utilizar adequadamente a LGPD em seu cotidiano.

Apresentar os seguintes temas relacionados a LGPD: Programa de Governança em Privacidade, Inventário de Dados Pessoais, Termos de Uso, Avaliação de Risco, Adequações de Contratos, Relatório de Impacto de proteção de dados, Respostas a Incidentes e Portal Gov.br.

Criar plataformas de agregação e disseminação de informações, documentos e materiais instrucionais à comunidade universitária e aos usuários dos serviços prestados pela Ufes.

8.3 PÚBLICO ALVO

Este plano tem como público alvo a comunidade universitária, servidores docentes e técnico-administrativos, estudantes, terceirizados, conveniados, e usuários dos serviços prestados pela instituição.

Os membros da comissão responsável pela gestão do processo e dos comitês operadores da LGPD na Ufes estarão submetidos a regras de capacitação específicas definidas internamente pelas instâncias colegiadas a que estão vinculados.

Os gestores da universidade, de todos os níveis, deverão participar das capacitações a fim de apoiar a implantação da nova cultura de proteção de dados pessoais nas unidades organizacionais.

8.4 MODALIDADES E CLASSIFICAÇÃO DAS AÇÕES

As ações de capacitação propostas neste plano podem ser classificadas em: Materiais informativos (cartilhas, folders, folhetos, vídeos); Guias e manuais; Cursos de curta duração; Seminários/Webinários e Sítio eletrônico ou Base de conhecimento.

8.5 EXECUÇÃO DAS AÇÕES

As ações de capacitação deste plano serão executadas por meio de materiais disponibilizados em sítio eletrônico e de plataformas de cursos a distância (AVA Progep), sistemas de reunião online (Google Meet ou Webconf RNP) e transmissão ao vivo. Serão realizadas de acordo com as etapas do processo de implantação da LGPD na Ufes, podendo ser iniciadas de imediato e encerradas após a implantação dos mecanismos previstos na lei. Cada ação de capacitação deve ter um projeto básico específico descrevendo seu planejamento.

Os cursos autoinstrucionais poderão ser realizados conforme a disponibilidade na plataforma, assim como vídeos hospedados em plataformas de streaming.

A realização dos seminários/webinários e a elaboração de materiais informativos (cartilhas, folders, folhetos, vídeos) deverão ser realizadas com suporte de especialistas da área.

As trilhas de aprendizagem e o sítio eletrônico ou base de conhecimento são ações de caráter transversal que permitem a agregação e disponibilização de materiais instrucionais e cursos de todas as etapas e de todas as modalidades, criando um centro de conteúdo que pode ser acessado pela comunidade interna e externa.

8.6 PLANEJAMENTO E ACOMPANHAMENTO DOS RESULTADOS

Uma comissão designada pelo Reitor será responsável pelo planejamento, implementação e acompanhamento das ações de desenvolvimento previstas no plano, com apoio das unidades organizacionais envolvidas. Os comitês operadores, além da comissão, também deverão acompanhar os resultados do processo a fim de identificar oportunidades de melhoria para o processo de implantação.

8.7 QUADRO DE ATIVIDADES PROGRAMADAS

Tema	Objetivo	Realização	Carga horária
Introdução à Lei Brasileira de Proteção de Dados Pessoais	Capacitar as pessoas para entenderem o funcionamento e diretrizes básicas expostas na nova lei geral de proteção de dados do Brasil	- Curso a distância (acesso em 19/05/2021)- https://www.escolavirtual.gov.br/curso/153	10h
Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais	Informar aos gestores públicos e servidores os pontos primordiais da legislação de proteção de dados	- Cartilha LGPD - CGE/PR (acesso em 19/05/2021) - https://www.cge.pr.gov.br/sites/default/arquivos_restritos/files/documento/2020-10/cartilha_LGPD.pdf - LGPD - Guia de Boas Práticas para Implementação na APF - https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaLGPD.pdf - Serpro e LGPD: segurança e inovação - https://www.serpro.gov.br/lgpd/	
Proteção de Dados Pessoais no Setor Público	Esclarecer aos participantes os diversos pontos apresentados na LGPD	- Curso a distância (acesso em 19/05/2021)- https://www.escolavirtual.gov.br/curso/290	15h
Governança de Dados	Conhecer os fundamentos relacionados à importância da governança de dados visando a disponibilização de informações corretas em tempo hábil para a tomada de decisões	- Curso a distância (acesso em 19/05/2021)- https://www.escolavirtual.gov.br/curso/270	30h
A LGPD e a proteção de dados pessoais no âmbito da Ufes	Apresentar o planejamento do processo de implantação da LGPD na Ufes	- Realização de Seminários/Webinários - Elaboração de materiais informativos	2h -
Programa de Governança em Privacidade	Apresentar os principais pontos da Lei Geral de Proteção de Dados, fornecendo os subsídios para a criação de um programa institucional de gerenciamento de privacidade.	- Realização de Seminários/Webinários - Elaboração de materiais informativos	2h -
Inventário de Dados Pessoais	Apresentar o inventário de todas as operações de tratamento de dados pessoais e suas avaliações sob a ótica dos princípios da LGPD.	- Realização de Seminários/Webinários - Elaboração de materiais informativos	2h -
Termos de Uso	Apresentar o processo de elaboração e aplicação dos Termos de Uso e Políticas de Privacidade vinculados à utilização de serviços públicos por meio de aplicações (sítios, sistemas ou aplicativos para	- Realização de Seminários/Webinários - Elaboração de materiais informativos	2h -

	dispositivos móveis) fornecidas por órgãos e entidades da administração pública.		
Avaliação de Riscos	Apresentar o processo de identificação e mensuração de riscos de segurança e privacidade, e de mitigação com a utilização dos controles mais indicados.	- Realização de Seminários/Webinários - Elaboração de materiais informativos	2h -
Adequações de Contratos	Apresentar o processo de adequação do processo de contratação para contemplar os requisitos mais importantes de segurança e privacidade dos dados	- Realização de Seminários/Webinários - Elaboração de materiais informativos	2h -
Relatório de Impacto de proteção de dados - RIPD	Apresentar o documento de comunicação e transparência que orienta a descrição dos processos de tratamento de dados pessoais que podem gerar riscos, bem como medidas, salvaguardas e mecanismos de mitigação.	- Realização de Seminários/Webinários - Elaboração de materiais informativos	2h -
Respostas a Incidentes	Apresentar o plano de Respostas a Incidentes de violação de dados para garantir maior celeridade na solução de incidentes e padronização de atividades a serem executadas, assim como prever responsáveis pelo cumprimento das atividades.	- Realização de Seminários/Webinários - Elaboração de materiais informativos	2h -
Portal Gov.br	Apresentar o processo de migração dos sites governamentais federais para o gov.br, abordando a base legal, a plataforma tecnológica disponibilizada e os critérios básicos para produção e publicação de conteúdo.	- Curso a distância (acesso em 19/05/2021) - https://www.escolavirtual.gov.br/curso/247 - Realização de Seminários/Webinários	15h 2h
Trilha de Aprendizagem sobre a LGPD	Reunir um conjunto de materiais instrucionais que facilite o acesso e contribua com o desenvolvimento do conhecimento sobre a LGPD e diversos aspectos relacionados.	- Criação da trilha (com possibilidade de contribuição pelos usuários).	-
Sítio eletrônico/Base de Conhecimento	Centralizar dados, informações-chave e documentos sobre a LGPD na Ufes, inclusive a trilha de aprendizagem	- Criação do site/base (sob a gestão da comissão)	-

9 CRONOGRAMA DE EXECUÇÃO

Ações	2021					2022/1	2022/2	2023/1
	Ago	Set	Out	Nov	Dez	Jan-Jun	Jul-Dez	Jan-Jun
Alinhamento de Expectativas com a Alta Gestão	X							
Consulta à Procuradoria acerca da conformidade jurídica do Plano de Adequação à LGPD	X							
Definição de Política para Proteção de Dados Pessoais (Resoluções CUn e Instruções Normativas - Item 4.1)						X		
Estabelecimento de Instrumentos operacionais (item 4.1)						X		
Adequações no SIE e elaboração de Inventário de Dados Pessoais (Item 2)	X	X	X	X	X	X		
Nomeação dos Comitês Operadores	X	X						
Capacitação dos Comitês Operadores	X	X	X	X	X			
Proceder primeiro diagnóstico após vigência do Plano (maturidade)	X							
Proceder segundo diagnóstico após vigência do Plano (maturidade)						X		
Proceder terceiro diagnóstico após vigência do Plano (maturidade)							X	
Proceder quarto diagnóstico após vigência do Plano (maturidade)								X
Adequação de contratos, convênios e termos de cooperação	X	X	X					
Elaboração de termos de Uso		X	X	X	X			
Adequações relacionadas à Tecnologia da Informação	X	X	X	X	X	X	X	
Elaborar Plano de comunicação para incidentes de violação de dados		X	X	X	X			
Plano de Comunicação (cultura de segurança dos dados)		X	X	X	X			
Capacitação da Comunidade Acadêmica		X	X	X	X			
Monitoramento de Riscos e elaboração de RIPD	X	X	X	X	X	X	X	X
Atualização da Carta de Serviços		X	X	X	X			
Alinhamento do Plano de Adequação à LGPD ao PDI 2021-30 (primeiro momento de revisão do PDI)								X

ANEXO I – LISTAGEM GERAL DO INVENTÁRIO DOS SERVIÇOS E PROCESSOS, TIPOS DE DADOS E TAXONOMIAS

UFES – Listagem geral do inventário dos serviços/processos de negócio que tratam dados pessoais								
	Nome	**Telefone**	**E-mail**	**Endereço**	**Cidade/UF**	**CEP**		
CONTROLADOR	Universidade Federal do Espírito Santo, por meio de seu reitor, Paulo Sérgio de Paula Vargas			Avenida Fernando Ferrari, 514 - Campus Goiabeiras, Bairro Goiabeiras	Vitória/ES	29.075-910		
ENCARREGADO	Ouvidoria da Ufes, por meio de seu Ouvidor, Renato Carlos Schwab Alves			Avenida Fernando Ferrari, 514 - Campus Goiabeiras, Bairro Goiabeiras	Vitória/ES	29.075-910		
SEQ	**Comitê Operador LGPD**	**Nome do serviço/processo de negócio**	**Nº Ref / ID**	**Data de Criação do Inventário**	**Data de Atualização do Inventário**	**Finalidade do tratamento dos dados pessoais**	**Dados Pessoais Sensíveis?**	**Dados Vulneráveis?**
1	Estudantes	Matrícula na graduação		07/01/21		Registro de matrícula e/ou vinculação discente a curso de graduação na Ufes	SIM	NÃO
2	Estudantes	Matrícula na pós-graduação stricto sensu		07/01/21		Registro de matrícula e/ou vinculação discente a curso de pós- graduação stricto sensu na Ufes	SIM	NÃO
3	Estudantes	Matrícula na graduação lato sensu		07/01/21		Registro de matrícula e/ou vinculação discente a curso de pós-graduação lato sensu na Ufes	SIM	NÃO
4	Público externo – pessoa natural	Agendamento de visita ao campus de Goiabeiras		07/01/21		Agendamento e contato com solicitante para visita com estudantes de ensino médio ao campus universitário de Goiabeiras	NÃO	NÃO
5	Estudantes	Cadastro e Recarga de cartão para acesso ao RU		07/01/21		Cadastro e emissão de cartão de acesso ao Restaurante Universitário do Campus Goiabeiras	NÃO	NÃO
6	Estudantes	Ingresso em cursos de Graduação – SISU		07/01/21		Inscrição na modalidade de ingresso SISU para Cursos de Graduação na Ufes	SIM	NÃO
7	Estudantes	Ingresso em cursos de Graduação – PSVS		07/01/21		Inscrição na modalidade de ingresso PSVS para Cursos de Graduação na Ufes	NÃO	NÃO

8	Estudantes	Ingresso em cursos de Graduação – ALUNO ESPECIAL	07/01/21	Inscrição na modalidade de ingresso ALUNO ESPECIAL para Cursos de Graduação na Ufes	NÃO	NÃO
9	Estudantes	Ingresso em cursos de Graduação – EAD	07/01/21	Inscrição na modalidade de ingresso EAD para Cursos de Graduação na Ufes	NÃO	NÃO
10	Estudantes	Emissão de diploma e 2ª via de diploma – Graduação e Pós-Graduação	07/01/21	Registrar e Validar diplomas de graduação e pós-graduação emitidos por Instituições privadas de Educação Superior	NÃO	NÃO
11	Estudantes	Cadastro em Bolsa de Extensão	07/01/21	Cadastrar alunos de graduação que realizam atividades de extensão universitária e podem concorrer a auxílio financeiro	SIM	NÃO
12	Estudantes	Cadastro em Bolsa de Pesquisa	07/01/21	Cadastrar alunos de graduação e pós-graduação que participam de projetos de pesquisa na Universidade e podem concorrer a auxílio financeiro	SIM	NÃO
13	Público externo – pessoa natural	Registro de diplomas de IES privadas	07/01/21	Registrar diploma expedido por IES privada para validade nacional como prova da formação recebida por seu titular	NÃO	NÃO
14	Colaboradores institucionais externos – pessoa natural ou jurídica	Atendimento aos veículos de comunicação	07/01/21	Agendar entrevistas e cadastrar contatos de fontes de informação	SIM	NÃO
15	Estudantes	Assistência e acompanhamento a pessoa com deficiência	07/01/21	Cadastrar alunos que necessitam de assistência e acompanhamento devido à deficiência	SIM	NÃO
16	Estudantes	Atendimento ginecológico para alunas assistidas	07/01/21	Agendar consulta e realizar atendimento com ginecologista para alunas cadastradas no Programa de Assistência Estudantil	SIM	NÃO
17	Estudantes	Atendimento no serviço social	07/01/21	Agendar atendimento com profissional do serviço social para atender demandas específicas de cunho social no âmbito acadêmico	SIM	NÃO

18	Estudantes	Atendimento odontológico para alunos assistidos	07/01/21	Agendar consulta/ atendimento odontológico para alunos da graduação que estejam cadastrados no Programa de Assistência Estudantil	SIM	NÃO
19	Estudantes e Servidores	Atendimento psicológico	07/01/21	Agendar consulta/atendimento com profissional da psicologia	SIM	NÃO
20	Público externo – pessoa natural	Auxílio à pesquisa documental na Ufes	07/01/21	Controle e mediação do acesso a documentos públicos de caráter histórico, administrativos e/ou acadêmicos, documentos públicos de caráter ostensivo e também documentos públicos em que o requerente seja parte ou interessado (documentos restritos). Medida de segurança	NÃO	NÃO
21	Estudantes	Auxilio para material de alto custo – Odontologia	07/01/21	Cadastrar interessado em auxílio financeiro para custear parte do material do curso de Odontologia	SIM	NÃO
22	Estudantes e Servidores	Bolsa de curso de língua estrangeira	07/01/21	Cadastro para concessão de bolsas de estudo em curso de língua estrangeira oferecido pelo Núcleo de Línguas da Universidade Federal do Espírito Santo (UFES)	NÃO	NÃO
23	Estudantes	Bolsa de Monitoria ou Apoio Administrativo - PaEPE	07/01/21	Cadastro para recebimento de auxílio financeiro em projetos especiais de apoio ao ensino, pesquisa e extensão (PaEPE)	SIM	NÃO
24	Público externo – pessoa natural	Cópia digital de documento arquivado na Ufes	07/01/21	Cadastro para mediação do acesso à informação e reprografia de documentos públicos de caráter ostensivo e também a cópia de inteiro teor de documentos públicos em que seja parte ou interessado. Medida de segurança	NÃO	NÃO
25	Estudantes	Cadastro na assistência estudantil - UFES (Proaes)	07/01/21	Cadastro no Programa de Assistência Estudantil para alunos com renda familiar per capita de até 1,5 salários mínimos para acesso aos auxílios estudantis e outros serviços	SIM	NÃO

26	Público externo – pessoa natural	Segurança e atendimento a emergências na Ufes	07/01/21	Registrar ocorrências de segurança, delitos, distúrbios, acidentes de trânsito e ocorrências similares nos campi Ufes	NÃO	NÃO
27	Público externo – pessoa natural	Visita técnica ao Arquivo Central da Ufes	07/01/21	Cadastro para mediação e controle do acesso de pessoas ao prédio da Diretoria de Documentação Institucional da Ufes. Medida de segurança	NÃO	NÃO
28	Estudantes e Servidores	Cadastro no Sistema de Registro Eletrônico de Ponto	07/01/21	Cadastro de servidores e estagiários no SREP para controle e monitoramento dos registros de frequência	SIM	NÃO
29	Servidores	Pagamento de folha de pessoal	07/01/21			NÃO
30	Estudantes	Pagamento de bolsistas	07/01/21			NÃO
31	Estudantes	Pagamento de estagiários	07/01/21			NÃO
32	Servidores	Abono de Permanência	07/01/21	Formulário de Requerimento contém dados pessoais do titular/servidor	SIM	NÃO
33	Servidores	Acesso ao SIAPE	07/01/21	Formulário de Requerimento para acesso ao SIAPE e Termo de Responsabilidade contém dados pessoais do titular/servidor		NÃO
34	Servidores	Acesso ao SIASS	07/01/21	Formulário de Solicitação de Habilitação no SIASS - Subsistema Integrado de Atenção à Saúde do Servidor Federal contém dados pessoais do titular/servidor		NÃO
35	Estudantes e Servidores	Acesso ao SIE/Protocolo Ufes	07/01/21	Termo de responsabilidade de acesso ao SIE – Sistema de Informação para o Ensino contém dados pessoais		NÃO
36	Servidores	Acesso ao SIGEPE	07/01/21	Ufes importa dados pessoais do Sistema SIGEPE		NÃO
37	Servidores	Acidente em Serviço	07/01/21	Formulários de registro de Acidente em Serviço contém dados pessoais do titular/servidor		NÃO
38	Servidores	Acumulação de Cargos, Empregos e Funções	07/01/21	Formulário contém dados de profissão e emprego		NÃO
39	Servidores	Adicional Noturno	07/01/21			NÃO

40	Servidores	Adicional por Serviço Extraordinário	07/01/21			NÃO
41	Servidores	Afastamento para participar de curso de formação	07/01/21			NÃO
42	Servidores	Afastamento para Mandato Eletivo	07/01/21	Formulário de Requerimento contém dados pessoais do titular/servidor		NÃO
43	Servidores	*Afastamento para Pós-Graduação Stricto Sensu – Servidores TAE*	07/01/21	Formulário de Afastamento para pós-graduação contém dados pessoais do titular/servidor		NÃO
44	Servidores	*Afastamento para pós-graduação Stricto Sensu – Servidores docentes*	07/01/21	Formulário de Afastamento para pós-graduação contém dados pessoais do titular/servidor	SIM	NÃO
45	Servidores	Ajuda de Custo – Mobília, Pecúnia ou Transporte	07/01/21	Requerimento e formalização processual contém dados pessoais sensíveis e dados de vulneráveis, além de cópia de documentos	SIM	SIM
46	Servidores	Ajuste de Exercício	07/01/21	Formulário de Requerimento contém dados pessoais do titular/servidor	SIM	NÃO
47	Servidores	Alteração de Dados Bancários	07/01/21	Formulário de Requerimento contém dados pessoais do titular/servidor		
48	Servidores	Alteração de Endereço de E-mail ou Telefone	07/01/21	Formulário de Requerimento contém dados pessoais do titular/servidor		
49	Servidores	Alteração de Jornada de Trabalho - médico	07/01/21			
50	Servidores	Alteração de Jornada de Trabalho	07/01/21			
51	Servidores	Alteração de Jornada de Trabalho - Docente	07/01/21	Atualização cadastral. Formulário de Requerimento contém dados pessoais do titular/servidor		
52	Servidores	Alteração de jornada de trabalho - TAE	07/01/21	Atualização cadastral. Formulário de Requerimento contém dados pessoais do titular/servidor		
53	Servidores	Alteração de nome ou estado civil	07/01/21	Atualização cadastral. Formulário de Requerimento contém dados pessoais do titular/servidor		

55	Servidores	Aposentadoria compulsória	07/01/21	Requerimento e formalização processual para aposentadoria do titular. Formulário contém dados pessoais		
56	Servidores	Aposentadoria por incapacidade	07/01/21			
57	Servidores	Aposentadoria voluntária	07/01/21			
58	Servidores	Aproveitamento de concurso	07/01/21			
59	Servidores	Assistência à Saúde Suplementar	07/01/21			
61	Servidores	Auxílio Alimentação	07/01/21			
62	Servidores	Auxílio Funeral	07/01/21			
63	Servidores	Auxílio Moradia	07/01/21			
64	Servidores	Auxílio Natalidade	07/01/21		SIM	SIM
65	Servidores	Auxílio Pré-Escolar	07/01/21		SIM	SIM
66	Servidores	Auxílio transporte	07/01/21			
67	Servidores	Avaliação de Desempenho	07/01/21			
68	Servidores	Averbação e Desaverbação de tempo de serviço/Contribuição	07/01/21			
69	Servidores	Cadastro de dependente	07/01/21			
70	Servidores	Cadastro de residente médico ou multiprofissional	07/01/21			
71	Servidores	Capacitações externas	07/01/21			
72	Servidores	Certidão de tempo de contribuição	07/01/21			
73	Servidores	Cessão, Requisição e Movimentação	07/01/21			
75	Servidores	Cessão, Requisição e Movimentação - Colaboração técnica (servidor da Ufes para outro órgão)	07/01/21	Declaração de cumprimento de jornada de trabalho possui dado pessoal		
76	Servidores	Cessão, Requisição e Movimentação - Colaboração técnica (servidor de outro órgão para a Ufes)	07/01/21	Declaração de cumprimento de jornada de trabalho possui dado pessoal		
77	Servidores	Concessão de carga horária para capacitação (técnico-administrativo)	07/01/21			
78	Servidores	Concurso público para professor efetivo	07/01/21			

79	Servidores	Conflito de interesses	07/01/21		
80	Servidores	Consignação em folha de pagamento	07/01/21		
81	Servidores	Contagem de tempo de serviço/Contribuição para aposentadoria	07/01/21		
82	Estudantes	Contratação de estagiário	07/01/21	SIM	NÃO
83	Servidores	Contratação de professor substituto	07/01/21		
84	Servidores	Contribuição para o Plano de Seguridade Social do Servidor - PSS	07/01/21		
85	Servidores	Declaração de bens e valores	07/01/21		
86	Servidores	Declaração de vínculos (Extra-SIAPE)	07/01/21		
87	Servidores	Declaração de que não se ausentou do país	07/01/21		
88	Servidores	Designação de Cargo de Direção, Função Gratificada e Função de Coordenador de Curso	07/01/21		
89	Servidores	Designação de companheiro(a) para fins de Pensão e Benefícios	07/01/21		
90	Servidores	Designação de Substituto Eventual/Vice-Diretor/Subchefe/Subcoordenador	07/01/21		
91	Servidores	Dimensionamento da Força de Trabalho dos servidores TAE	07/01/21		
92	Servidores	Estágio Probatório de Docente	07/01/21		
93	Servidores	Estágio Probatório de Servidor Técnico-Administrativo	07/01/21		
94	Servidores	Exoneração de cargo efetivo	07/01/21		
95	Servidores	Exoneração ou Dispensa de cargo de Direção, Função Gratificada ou Função de Coordenador de Curso	07/01/21		
96	Servidores	Férias Web	07/01/21		
97	Servidores	Exibir Férias Web	07/01/21		
98	Servidores	Flexibilização de Jornada	07/01/21		
99	Servidores	Frequência e Registro de Ponto	07/01/21		

100	Servidores	Gratificação natalina	07/01/21			
101	Servidores	Gratificação por encargo de curso e concurso	07/01/21			
102	Servidores	Horário especial para servidor estudante	07/01/21			
103	Servidores	Horário Especial para servidor portador de deficiência ou com Familiar portador de deficiência	07/01/21		SIM	SIM
104	Servidores	Identidade funcional	07/01/21			
105	Servidores	Incentivo à qualificação	07/01/21			
106	Servidores	Indenização de transporte	07/01/21			
107	Servidores	Insalubridade, periculosidade ou Raios-X	07/01/21			
109	Servidores	Interrupção de férias	07/01/21			
110	Servidores	Isenção de imposto de renda	07/01/21			
111	Servidores	Licença Gestante/Adotante/Maternidade	07/01/21			
112	Servidores	Licença para Acompanhar Cônjuge	07/01/21			
113	Servidores	Licença para Atividade Política	07/01/21			
114	Servidores	Licença para Capacitação	07/01/21			
115	Servidores	Licença para Tratamento de Saúde	07/01/21			
116	Servidores	Licença para Tratar de Interesses Particulares	07/01/21			
117	Servidores	Licença Paternidade	07/01/21			
118	Servidores	Licença por Motivo de Doença em Pessoa da Família	07/01/21			
119	Servidores	Licença Prêmio	07/01/21			
120	Servidores	Modelo de Procuração - Pessoa Física	07/01/21			
121	Servidores	Modelo de Projeto Básico de Ação de Capacitação	07/01/21			
122	Servidores	Nome Social	07/01/21			
123	Servidores	Nomeação para Cargo Efetivo	07/01/21			
124	Servidores	Exibir Nomeação para Cargo Efetivo	07/01/21			
125	Servidores	Pensão Alimentícia	07/01/21			

126	Servidores	Pensão por morte	07/01/21
127	Servidores	Perfil Profissiográfico Previdenciário - PPP (Anexo VI da IN 53-2011-PRES-INSS)	07/01/21
128	Servidores	Posse e efetivo exercício em cargo público	07/01/21
129	Servidores	Processo Seletivo para contratação de Estagiário	07/01/21
130	Servidores	Processo Seletivo para contratação de Professor Substituto	07/01/21
131	Servidores	Progressão por Capacitação Profissional (PCCTAE)	07/01/21
132	Servidores	Progressão por Mérito Profissional (PCCTAE)	07/01/21
133	Servidores	Progressão, Promoção e Aceleração da Promoção Docente	07/01/21
134	Servidores	Readaptação	07/01/21
135	Servidores	Recondução	07/01/21
136	Servidores	Redistribuição	07/01/21
137	Servidores	Exibir Redistribuição	07/01/21
138	Servidores	Registro de capacitação	07/01/21
139	Servidores	Reintegração	07/01/21
140	Servidores	Remoção	07/01/21
141	Servidores	Requerimento Geral (PDF) (Utilizar nos casos em que não houver formulário padrão)	07/01/21
142	Servidores	Requerimento Geral (DOCX)	07/01/21
143	Servidores	Retribuição por Titulação Docente	07/01/21
144	Servidores	Reversão	07/01/21
145	Servidores	Revisão do Plano de Desenvolvimento de Pessoas	07/01/21
146	Servidores	Solicitação de Reserva de Espaço Físico do DDP	07/01/21

147	Servidores	Substituição de Cargo de Direção, Função Gratificada ou Função de Coordenador de Curso	07/01/21			
148	Servidores	Vacância de cargo efetivo	07/01/21			
149	Estudantes	Requerimento – Aluno Especial	07/01/21			
150	Estudantes	Requerimento – Aproveitamento de estudos/ Dispensa de disciplinas/ Eletiva para Optativa	07/01/21			
151	Estudantes	Cadastro de bolsista para iniciação científica	07/01/21			
152	Estudantes	Reconhecimento de Diplomas de Pós-Graduação	07/01/21			
153	Estudantes	Carteira de estudante de Pós-Graduação	07/01/21	Emissão da carteira de estudante de pós-graduação através do preenchimento do formulário de solicitação	SIM	NÃO
154	Servidores	Agendamento de webconferência para defesa de Teses e Dissertações	07/01/21			
155	Estudantes e Servidores	Carta de Apoio Institucional (convênios e acordos de cooperação os projetos)	07/01/21			
156	Servidores	Portal de Periódicos da CAPES - acesso remoto via CAFe e via SAR (Compartilhamos dados pessoais)	07/01/21			
157	Colaboradores institucionais externos – pessoa natural ou jurídica	Bolsas CAPES Professores Visitantes	07/01/21	Cadastro no Programa Professor Visitante Estrangeiro (PVE) que apoia visitas de média ou longa duração, de professores do exterior convidados por cursos de doutorado de Instituições de Ensino Superior (IES) brasileiras. Coleta dados pessoais para concessão de bolsa; Passagem aérea; Auxílio instalação	SIM	NÃO

158	Colaboradores institucionais externos – pessoa natural ou jurídica	Bolsas CAPES Pós-Docs	07/01/21	Cadastro no Programa Cooperação Internacional da CAPES para pesquisadores de universidades estrangeiras realizarem pós-doutorado no Brasil. Coleta dados para concessão de bolsas e benefícios da Capes	SIM	NÃO
159	Servidores	Afastamento para Eventos e Outras Atividades de Curta Duração no Exterior	07/01/21	Cadastro em formulário próprio de solicitação para afastamentos do país para participação em eventos, e para visitas técnicas de curta duração (até 30 dias)	SIM	NÃO
160	Estudantes	Bolsas DCR - FAPES/CNPq de Pós-Doutorado	07/01/21	Requerer bolsas e auxílios do DCR – FAPES/CNPq para Pós-Doutorado	SIM	NÃO
161	Estudantes	Programa PRODOUTORAL da CAPES	07/01/21	Cadastro no Programa Prodoutoral. Coleta de dados pessoais para requerer bolsa e auxílio moradia. Compartilha dados pessoais com a Capes	SIM	NÃO
162	Estudantes e Servidores	Plataforma Stela Esperta – Ufes	07/01/21	Importa dados pessoais e acadêmicos da Plataforma Sucupira	SIM	NÃO
163	Público externo – pessoa natural	Propriedade Intelectual – Requerimento de Patente	07/01/21	Preencher requerimento de Proteção, documento que solicita à Diretoria de Inovação Tecnológica (DIT) o depósito do pedido de patente do titular dos dados pessoais e o Formulário de Descrição da Invenção. Compartilha dados pessoais com o Instituto Nacional da Propriedade Industrial (INPI)	SIM	NÃO
164	Público externo – pessoa natural	Propriedade Intelectual – Pedido de registro de Programa de Computador	07/01/21	Preencher o Memorando de Requerimento de Proteção, documento que solicita à Diretoria de Inovação Tecnológica (DIT) o pedido de registro de programa de computador e o Formulário de Pedido de Registro de Programa de Computador. Compartilha dados pessoais com o Instituto Nacional da Propriedade Industrial (INPI)	SIM	NÃO

165	Público externo – pessoa natural	Propriedade Intelectual – Pedido de registro de Marca	07/01/21	Preencher o Memorando de Requerimento de Proteção, documento que solicita à Diretoria de Inovação Tecnológica (DIT) o pedido de registro e o Formulário do Pedido de registro de marca	SIM	NÃO
166	Público externo – pessoa natural	Propriedade Intelectual – Pedido de registro de Cultivares	07/01/21	Preencher o Requerimento de Proteção, documento que solicita à Diretoria de Inovação Tecnológica (DIT). Compartilha dados pessoais com o Serviço Nacional de Proteção de Cultivares (SNPC)	SIM	NÃO
167	Público externo – pessoa natural	Propriedade Intelectual – Pedido de registro de Indicação Geográfica - cidades ou regiões que ganham notoriedade por causa de seus produtos ou serviços	07/01/21	Preencher o Requerimento de Registro de Limitação Geográfica junto à Diretoria de Inovação Tecnológica (DIT), indicando delimitação de área de produção, restringindo seu uso aos produtos da região a fim de manter os padrões locais e impedir que outras pessoas usem o nome da região com produtos de baixa qualidade	SIM	NÃO
168	Público externo – pessoa natural	Propriedade Intelectual – Pedido de registro de Desenho Industrial	07/01/21	Preencher requerimento de registro de Desenho Industrial para evitar cópias e proteger um invento da utilização por terceiros	SIM	NÃO
169	Público externo – pessoa natural	Propriedade Intelectual – Pedido de registro de Topografia de Circuitos Integrados	07/01/21	Preencher requerimento junto à Diretoria de Inovação Tecnológica (DIT) para solicitar o pedido de registro de topografia de circuitos integrados	SIM	NÃO
170	Estudantes	Programa Institucional de Iniciação em Desenvolvimento Tecnológico e Inovação (PIBITI)	07/01/21	Termo de Compromisso, Termo de Responsabilidade e Sigilo e Plano de Trabalho do Bolsista do PIBITI contém dados pessoais	SIM	NÃO

TIPOS DE DADOS					
Comitê LGPD por categoria de dados pessoais	**Tipo de dado pessoal**	**Tipo de Dado Pessoal Sensível**	**Vulnerabilidade de dados do titular**	**Categoria de Dados Coletados**	**Hipótese Legal**
1 – Estudantes	Nome Completo	1.Origem racial ou étnica	1 – Crianças e adolescentes	1 – Dados de identificação pessoal	1 – Mediante consentimento do titular
2 – Servidores	CPF	2. Convicção religiosa	2 – Outro grupo vulnerável	2 – Dados financeiros	2 – Para cumprimento de obrigação legal ou regulatória
3 – Contratos	Telefone de contato	3. Opinião política		3 – Características pessoais	3 – Para execução de políticas públicas
4 – Público externo – pessoa natural	E-mail de contato	4. Filiação a sindicato		4 – Hábitos pessoais	4 – Para realização de estudos e pesquisas
5 – Colaboradores institucionais externos – pessoa natural ou jurídica	Profissão	5. Filiação a organização de caráter religioso		5 – Características psicológicas	5 – Para execução ou preparação de contrato
	Endereço residencial / comercial	6. Filiação ou crença filosófica		6 – Composição familiar	6 – Para exercício de direitos em processo judicial, administrativo ou arbitral
	Data de nascimento	7. Filiação ou preferências políticas		7 – Interesses de lazer	7 – Para proteção da vida ou da incolumidade física do titular ou de terceiro
	Número Identidade – RG	8. Dado referente à saúde		8 – Associações	8 – Para tutela da saúde de titular
	Título de Eleitor	9. Dado referente à vida sexual		9 – Processo judicial ou administrativo ou criminal	9 – Para atender interesses legítimos do controlador ou de terceiros
	Título de reservista	10. Dado biométrico – características biológicas mensuráveis para reconhecimento automatizado		10 – Hábitos de consumo	10 – Para proteção do crédito
	Gênero	11. Dado biométrico - características comportamentais mensuráveis para reconhecimento automatizado		11 – Dados residenciais	11 – Para garantia da prevenção à fraude e à segurança do titular
	Nacionalidade	12. Dado genético – características hereditárias		12 – Educação e treinamento	

	Assinatura	13. Dado genético - características obtidas por análise de ácidos nucleicos	13 – Profissão e emprego
	Exames médicos	14. Dado genético – características obtidas por outras análises científicas	14 – Registros – gravações de vídeo
	Extratos financeiros		15 – Outros
	Estado civil		
	Dados bancários		
	Extratos previdenciários		
	Declarações individuais		
	Documento de incapacidade civil		
	Documento sobre deficiência		
	Fotografias / Imagens		
	Grau de escolaridade		
	Idade		
	Filmagens		
	Carteira de habilitação		
	Passaporte		
	Localização via GPS		
	Endereço IP		

TAXONOMIAS			
Atributos biográficos	**Atributos biométricos**	**Atributos genéticos**	**Dados cadastrais**
Nome civil	Características biológicas mensuráveis para reconhecimento automatizado	Características hereditárias	CPF
Nome social	Características comportamentais mensuráveis para reconhecimento automatizado	Características obtidas por análise de ácidos nucleicos	CNPJ
Data de nascimento		Características obtidas por outras análises científicas	NIS
Filiação			PIS
Naturalidade			PASEP
Nacionalidade			Título de Eleitor
Sexo			
Estado civil			
Grupo familiar			
Endereço			
Vínculos empregatícios			
Convicção religiosa			
Opinião política			
Filiação a organização filosófica			
Filiação a organização política			
Filiação a sindicato			

ANEXO II – MAPA DE RISCO

PLANILHA DE GESTÃO DE RISCO DISPONIBILIZADA PELA CGU

Preenchimento da aba: Mapa de Risco

Macroprocesso / Processo	Identificação de Eventos de Riscos			Avaliação do Riscos				Resposta a Risco						
				Risco Inerente	Identificação dos Controles Existentes				Controles Propostos / Ações Propostas					
	Eventos de Risco	Causas	Efeitos / Consequências	Descrição	Descrição do Controle Atual	Avaliação quanto ao Desenho do Controle	Avaliação quanto a Operação do Controle	Possíveis Respostas	Tipo	Objetivo	Descrição	Data do Início	Data da Conclusão	Status

ANEXO III – CÁLCULO DO RISCO INERENTE

PLANILHA DE GESTÃO DE RISCO DISPONIBILIZADA PELA CGU

Preenchimento da aba: Cálculo do Risco Inerente

Macroprocesso / Processo	Eventos de Riscos	Impacto							Probabilidade					Nível de Risco	
		Esforço de Gestão	Regulação	Reputação	Negócios/ Serviços à Sociedade	Intervenção Hierárquica	Orçamentário discricionário	Média	Muito alta (>90%)	Alta (>=50% <= 90%)	Média (>=30% <= 50%)	Baixa (>=10% <= 30%)	Muito baixa (< 10%)	Risco	Descrição
		15%	17%	12%	18%	13%	25%	100%							

Na aba Impacto encontraremos a tabela1, que auxilia a calcular o peso do impacto do risco

Estratégico-Operacional					Econômico-Financeiro	Peso
Esforço de Gestão	Regulação	Reputação	Negócios/Serviços à Sociedade	Intervenção Hierárquica	Orçamentário discricionário	
15%	17%	12%	18%	13%	25%	100%
Evento com potencial para levar o negócio ou serviço ao colapso	Determina interrupção das atividades	Com destaque na mídia nacional e internacional, podendo atingir os objetivos estratégicos e a missão	Prejudica o alcance da missão da Ufes	Exigiria a intervenção do Reitor	> = 25%	5
Evento crítico, mas que com a devida gestão pode ser suportado	Determina ações de caráter pecuniários (multas)	Com algum destaque na mídia nacional, provocando exposição significativa	Prejudica o alcance da missão da Unidade	Exigiria a intervenção do Pró-Reitor/Superintendente	> = 10% < 25%	4
Evento significativo que pode ser gerenciado em circunstâncias normais	Determina ações de caráter corretivo	Pode chegar à mídia provocando a exposição por um curto período de tempo	Prejudica o alcance dos objetivos estratégicos	Exigiria a intervenção do Diretor	> = 3% < 10%	3
Evento cujas consequências podem ser absorvidas, mas carecem de esforço da gestão para minimizar o impacto	Determina ações de caráter orientativo	Tende a limitar-se às partes envolvidas	Prejudica o alcance das metas do processo	Exigiria a intervenção do Coordenador	> = 1% < 3%	2
Evento cujo impacto pode ser absorvido por meio de atividades normais	Pouco ou nenhum impacto	Impacto apenas interno / sem impacto	Pouco ou nenhum impacto nas metas	Seria alcançada no funcionamento normal da atividade	< 1%	1

Na aba Probabilidade temos a tabela 2, que auxilia a calcular a probabilidade do risco

Aspectos Avaliativos	Frequência Observada/Esperada	Peso
Evento esperado que ocorra na maioria das circunstâncias	Muito alta (>90%)	5
Evento provavelmente ocorra na maioria das circunstâncias	Alta (>=50% <= 90%)	4
Evento deve ocorrer em algum momento	Média (>=30% <= 50%)	3
Evento pode ocorrer em algum momento	Baixa (>=10% <= 30%)	2
Evento pode ocorrer apenas em circunstâncias excepcionais	Muito baixa (< 10%)	1

ANEXO IV – PLANO DE AÇÃO

PLANILHA DE GESTÃO DE RISCO DISPONIBILIZADA PELA CGU

Preenchimento da aba: Plano de Ação

				O que?			Onde?	Quem?	Como?		Quando?		
Macroprocesso / Processo	Evento de Risco	Resposta a Risco	Categoria do Risco	Controle Proposto / Ação Proposta									
				Descrição	Tipo	Objetivo	Área Responsável pela Implementação	Responsável Implementação	Como será Implementado	Intervenientes	Data do Início	Data da Conclusão	Status

Na aba Resposta ao risco, temos a tabela 3, que auxilia a preencher a resposta ao risco

Nível de Risco	Descrição do Nível de Risco	Parâmetro de Análise para Adoção de Resposta	Tipo de Resposta	Ação de Controle	Pontuação
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 efeitos	13 a 25
Risco Alto	Indica que o risco residual 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	7 a 12
Risco Moderado	Indica que o risco residual 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).	4 a 6
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 a 3

ANEXO V – TERMO DE CONSENTIMENTO PARA PARTICIPANTES DE PROJETOS INSTITUCIONAIS

Departamento de Contratos e Convênios
UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO
POP DECCON 01101.1 – Verificar a instrução processual

ANEXO VIII – TERMO DE CONSENTIMENTO PARA TRATAMENTO DE DADOS PESSOAIS

Art. 7º, Inciso I, Lei 13.709/18

Através do presente instrumento, eu_____, inscrito (a) no CPF sob n°_____, venho por meio deste, autorizar que Universidade Federal do Espírito Santo, disponha dos meus dados pessoais, de acordo com inciso I do artigo 7° da Lei n° 13.709/2018, em razão da minha participação no projeto_____, permitindo sua divulgação em sítios próprios nos termos da publicidade exigida pela Lei 8.958 de 20/12/94, Decreto 7.423 de 31/12/10 e legislação correlata.

Vitória/ES, 8 de julho de 2021.

_____

NOME COMPLETO
CPF Nº XXX.XXX.XXX-XX