MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL FLUMINENSE

PROGRAMA DE GOVERNANÇA EM PROTEÇÃO DE DADOS PESSOAIS E PRIVACIDADE
UNIVERSIDADE FEDERAL FLUMINENSE (UFF)

Niterói
2024

SUMÁRIO

1. INTRODUÇÃO
2. FINALIDADES E OBJETIVOS
3. ETAPAS DE INICIAÇÃO E PLANEJAMENTO
    1. Alinhamento com a alta administração, Nomeação do Encarregado, Comitê de Governança Digital, Comitê de Governança de Dados e Privacidade (CGDP) e Comitê de Segurança da Informação:
    2. Definição do índice de maturidade sobre os temas LGPD, proteção de dados e privacidade, segurança da informação:
    3. Plano de Capacitação:
    4. Plano de Comunicação:
    5. Política de Segurança da Informação:
    6. Política de Privacidade e Proteção de Dados Pessoais:
    7. Inventário de dados pessoais:
    8. Política de Gestão de Riscos e Prevenção de Incidentes:
    9. Definição de critérios de aferição do uso dos princípios “privacidade desde a concepção” e “privacidade por padrão”:
4. RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD):
5. MONITORAMENTO E ADEQUAÇÃO CONTÍNUA À LGPD E ÀS REGULAMENTAÇÕES DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD):

REFERÊNCIAS

1. INTRODUÇÃO

O Programa de Proteção de Dados Pessoais e Privacidade tem por objetivo o alinhamento de toda a instituição de modo a atuar em conformidade com as normativas vigentes e adoção de boas práticas.

A Lei Geral de Proteção de Dados Pessoais (LGPD - Lei 13.709 de 14 de agosto de 2018) versa 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 Programa de Privacidade e Segurança da Informação (PPSI) (PPSI - PORTARIA SGD/MGI nº 852, de 28 de março de 2023) tem como objetivo elevar a maturidade e resiliência dos órgãos e entidades em termos de privacidade e segurança da informação, no âmbito do SISP (Sistema de Administração dos Recursos de Tecnologia da Informação da Administração Pública Federal da qual a UFF faz parte. Nas disposições preliminares, são conceituados os termos proteção e privacidade de dados entendidos como ações que visam proteger os direitos e liberdades fundamentais das pessoas naturais, entre eles a privacidade em meios digitais e privacidade como direito à inviolabilidade da vida privada, da honra e da imagem das pessoas. (Constituição Federal, art 5º, incisos X e LXXIX).

A política de privacidade e proteção de dados pessoais na UFF (Portaria UFF nº 68.760 de 27 de dezembro de 2024, publicada no Boletim de Serviço - ANO LVIII – N.° 159 27/12/2024 SEÇÃO IV P.161) estabelece diretrizes e princípios que norteiam o tratamento de dados pessoais, no âmbito da Universidade Federal Fluminense (UFF) e em conformidade com a Lei Geral de Proteção de Dados Pessoais, bem como estabelecer critérios e procedimentos gerais a serem observados por servidores técnico-administrativos, docentes, alunos, estagiários, colaboradores em geral e demais cidadãos interessados, com objetivo de atingir níveis adequados de proteção aos dados pessoais e oferecer garantias aos titulares de dados pessoais quanto à confidencialidade e à privacidade, conforme anexo 1.

O Manual de Boas Práticas de Privacidade e Segurança da Informação na Universidade Federal Fluminense foi elaborado com o objetivo de difundir boas práticas de privacidade e segurança da informação, de modo a garantir a proteção adequada dos dados pessoais coletados, com vistas a promover a adoção das boas práticas, por meio de disponibilização de recomendações e procedimentos relacionados à temática de Privacidade e Segurança da Informação, conforme anexo 2.

Este Programa irá orientar as ações a serem desenvolvidas na UFF para a adequação da instituição à LGPD. O bom desempenho do programa será obtido com um planejamento estratégico com definição de plano de ação com etapas, conforme anexo 3, que apresenta o Plano de Ação do CGDP. O plano de ação do Comitê de Governança de Dados e Privacidade foi aprovado pelo Comitê de Governança, Integridade, Riscos e Controles (CGIRC) e está na página da LGPD da UFF.

2. FINALIDADES E OBJETIVOS

A Universidade Federal Fluminense apresenta seu Programa de Governança em Proteção de Dados Pessoais e Privacidade com a finalidade de:

- nortear a instituição para atuar em conformidade com as normativas e regulamentos sobre proteção de dados pessoais e privacidade;
- estabelecer políticas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade e proteção de dados pessoais;

- manter relação de confiança com o titular de dados, por meio de atuação transparente;
- estar integrado à estrutura geral de governança da instituição; e
- aplicar mecanismos de supervisão internos.

3. ETAPAS DE INICIAÇÃO E PLANEJAMENTO

3.1. Alinhamento com a alta administração, Nomeação do Encarregado, Comitê de Governança Digital, Comitê de Governança de Dados e Privacidade (CGDP) e Comitê de Segurança da Informação (CSI):

O Programa de Governança em Proteção de Dados Pessoais e Privacidade está elaborado em consonância e alinhado com a alta administração da Universidade Federal Fluminense, cuja efetividade das ações na instituição e operacionalização das mesmas, envolvem as decisões do controlador com a contribuição dos Comitês constituídos para apoiar, mitigar e balizar as atividades nas unidades organizacionais da UFF. Essas atividades devem estar de acordo com o que preconiza a Lei Geral de Proteção de Dados Pessoais, cuja eficiência está relacionada ao empenho de todas as instâncias da Instituição para cumprimento da finalidade de proteção dos dados pessoais e privacidade na execução das políticas públicas.

O controlador instituiu, por meio de portarias, Comitês para proteção de dados pessoais, segurança da informação e gestão de riscos, objetivando a adequação à Lei Geral de Proteção de Dados e Pessoais.

A Instituição nomeou o Encarregado pelo Tratamento de Dados Pessoais, consoante o disposto no art. 1º da Instrução Normativa SGD/ME no 117, de 19 de novembro de 2020, e em cumprimento ao art. 23, inciso III, e art. 41 da Lei 13.709, de 14 de agosto de 2018.

O Encarregado é integrante do Comitê de Governança Digital e coordena o Comitê de Governança de Dados Pessoais e Privacidade (CGDP), possuindo acesso direto à alta administração para alinhamento de etapas, procedimentos e recomendações para adequação à LGPD na Universidade Federal Fluminense, conforme estabelece a Portaria UFF 68.735 de 10 de outubro de 2024, publicada no Boletim de Serviço - ANO LVIII – N.° 128 11/10/2024 SEÇÃO IV P.130, que pode ser observado no anexo 4.

O Comitê de Governança Digital tem por objetivo deliberar sobre os assuntos relativos à implementação das ações de governo digital e ao uso de recursos de tecnologia da informação e comunicação. O comitê é composto pela Chefia de Gabinete, que o preside, por representantes da Pró-Reitoria de Pesquisa, Pós-Graduação e Inovação (PROPPI), Pró-Reitoria de Graduação (PROGRAD), Pró-Reitoria de Extensão (PROEX) e Pró-Reitoria de Assuntos Estudantis (PROAES), por representantes da Superintendência de Tecnologia da Informação (STI) e da Superintendência de Comunicação Social (SCS) e pelo encarregado do tratamento de dados pessoais, conforme estabelece a PORTARIA UFF Nº 68.595 de 22 de setembro de 2023, publicada no Boletim de Serviço - ANO LVII – N.° 180 22/09/2023 SEÇÃO IV P.045, que pode ser vista no anexo 5.

O Comitê de Governança de Dados e Privacidade (CGDP) foi instituído com o objetivo de definir o direcionamento, o monitoramento, a supervisão e a avaliação das práticas de gestão para garantir a proteção de dados e da privacidade no âmbito da Universidade Federal Fluminense, conforme disposto na Lei Geral de Proteção de Dados (LGPD) e suas normativas. O comitê CGDP é composto pelo encarregado pelo tratamento de dados pessoais na UFF, pelo Presidente do Comitê de Governança Digital, pelo Coordenador da Comitê de Segurança da Informação, pelo Presidente da Comissão de Dados Abertos e pelo Coordenador do Subcomitê de Gestão de Riscos.

O Comitê CGDP possui função técnica, tendo por escopo promover as boas práticas de gestão de dados e privacidade na UFF, potencializando discussões estratégicas, por meio de recomendações fundamentadas, auxiliando no desempenho das funções legais e regulamentares dos órgãos administrativos, conforme consta na PORTARIA UFF Nº 68.476 de 12 de janeiro de 2023, publicada no Boletim de Serviço - ANO LVI – N.° 12 17/01/2023 SEÇÃO IV P.083, que pode ser observada no anexo 6.

Possui a atribuição de propor ao Comitê de Governança, Integridade, Riscos e Controles (CGIRC) a elaboração da Política de Privacidade e de Proteção de Dados Pessoais na UFF. Possui função independente, mas também atua em conjunto com o Comitê de Segurança da Informação (CSI) no atendimento e no cumprimento das etapas e ciclos de Apoio e ao Diagnóstico para implementação do *Framework* Privacidade e Segurança da Informação, instituído pelo Secretaria de Governo Digital (SGD) direcionado às unidades de Tecnologia da Informação e Comunicação dos órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP).

O CGDP elabora planos de ação que são submetidos à aprovação do CGIRC, órgão colegiado de natureza deliberativa e de caráter permanente da Universidade para tratar de temas de gestão transversais à atividade das unidades da UFF como o planejamento estratégico, integridade, sistemas de monitoramento de desempenho, políticas de governança, sistemas de gestão de riscos e de controles internos.

O Comitê de Segurança da Informação (CSI) é responsável por conduzir o alinhamento das ações de segurança da informação para o alcance dos objetivos estratégicos da instituição em conformidade com a legislação vigente, devendo atuar, para alinhamento da UFF à LGPD, na definição, normatização e monitoramento interno, de temas como estratégias de backup e recuperação de incidentes de segurança, políticas de autenticação e controle de acesso. Possui atribuições dentre outras a proposição de alterações na política de segurança da informação interna e de normas internas relativas à segurança da informação, conforme consta na PORTARIA UFF Nº 68.509 de 22 de março de 2023, publicada no Boletim de Serviço - ANO LVII – N.° 55 22/03/2023 SEÇÃO IV P.105, disposta no anexo 7.

O CSI é composto pelo Gestor de Segurança da Informação, que o coordena, por representante do Gabinete do Reitor, por dois especialistas em segurança em tecnologia da informação do corpo docente da universidade, pelo Superintendente da Superintendência de Documentação, pelo Superintendente da Superintendência de Tecnologia da Informação da instituição; por dois representantes das áreas de infraestrutura e de sistemas da Superintendência de Tecnologia da Informação da instituição, por dois representantes da área de Governança de TI da Superintendência de Tecnologia da Informação e por dois representantes das unidades fora de sede da instituição.

3.2. Definição do índice de maturidade sobre os temas LGPD, proteção de dados e privacidade, segurança da informação:

O índice de maturidade é medido por meio da aplicação de formulário baseado no modelo de maturidade preconizado pela Controladoria Geral da União (CGU), como procedimento de monitoramento interno da adequação da UFF à LGPD.

O Comitê de Governança de Dados e Privacidade (CGDP) elabora o formulário de definição do índice de maturidade da UFF sobre LGPD. A aplicação do questionário tem como público direto, todos os servidores da UFF, para análise da maturidade da instituição sobre o conhecimento e aplicação da legislação e suas normativas no tratamento de dados pessoais nos serviços públicos executados nas diferentes unidades organizacionais da UFF. Conforme pode ser observado no Plano de Ação (anexo 3), o formulário (anexo 8) foi aplicado no segundo semestre de 2023.

3.3. Plano de Capacitação:

A Escola de Governança em Gestão Pública da UFF (EGGP) desenvolve as atividades de capacitação previstas no Plano de Ação do CGDP para os servidores da UFF, conforme apresentam os anexos 9 e 10. O objetivo é capacitar os servidores da Instituição sobre a relevância dos temas proteção de dados, segurança da informação, gestão de riscos e o uso consciente e responsável nos sistemas internos UFF, como, por exemplo, o Sistema Eletrônico de Informação (SEI). O plano de capacitação em proteção de dados pessoais e o plano de capacitação em segurança da informação estão na página LGPD da UFF.

3.4. Plano de Comunicação:

A Superintendência de Comunicação Social (SCS) desenvolve as atividades de divulgação e comunicação previstas no Plano de Ação do CGDP para os servidores da UFF. O objetivo é apresentar à comunidade acadêmica e demais interessados as principais ações de comunicação previstas para tratar da temática de proteção de dados pessoais no âmbito universitário. Ações de conscientização são adotadas buscando o atingimento dos públicos diretamente envolvidos, como técnicos administrativos e docentes, conforme pode ser observado no anexo 11 e no Plano de Comunicação.

3.5. Política de Segurança da Informação:

O Comitê de Segurança da Informação elabora a política de segurança da informação (PSI) da UFF e está alinhada ao Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC). A PSI deve ser amplamente comunicada ao corpo de servidores, alunos, colaboradores e entidades externas que fazem uso dos recursos de tecnologia da informação da UFF. O objetivo é estabelecer mecanismos e controles para garantir a efetiva proteção dos dados, informações e conhecimentos gerados, redução dos riscos de ocorrência de perdas, alterações e acessos indevidos, preservando a produção intelectual, disponibilidade, integridade, confiabilidade e autenticidade das informações, na UFF. A política de segurança da Informação e as normativas complementares da Superintendência de Tecnologia da Informação estabelecem controles adequados para cumprir os requisitos de segurança da informação necessários à proteção da privacidade e de dados pessoais tratados na UFF, conforme pode ser observado na Política de Segurança da Informação, que consta no anexo 12.

3.6. Política de Privacidade e Proteção de Dados Pessoais:

A política de privacidade e proteção de dados pessoais é elaborada pelo Comitê de Governança de Dados e Privacidade visando estabelecer diretrizes e princípios que devem nortear o tratamento de dados pessoais, no âmbito da Universidade Federal Fluminense (UFF) e em conformidade com a Lei Geral de Proteção de Dados Pessoais. Estabelece, também, critérios e procedimentos gerais a serem observados por servidores técnico-administrativos, docentes, alunos, estagiários, colaboradores em geral e demais cidadãos interessados com objetivo de alcançar níveis adequados de proteção aos dados pessoais e oferecer garantias aos titulares de dados pessoais quanto à confidencialidade e à privacidade, conforme consta na

Portaria UFF nº 68.760 de 27 de dezembro de 2024, publicada no Boletim de Serviço - ANO LVIII – N.° 159 27/12/2024 SEÇÃO IV P.161, e no anexo 1.

3.7. Inventário de dados pessoais:

O Inventário de Dados Pessoais representa o documento primordial para documentar o tratamento de dados pessoais realizados pela instituição em alinhamento à Lei Geral de Proteção de Dados Pessoais (LGPD).

Definido o modelo a ser aplicado na Instituição, todas Pró-Reitorias e Superintendências que realizam tratamento de dados pessoais, para execução dos serviços públicos oferecidos pela UFF, serão responsáveis pelo preenchimento e atualização do inventário anualmente.

3.8. Política de Gestão de Riscos e Prevenção de Incidentes:

A política de gestão de riscos na Universidade Federal Fluminense denominada PGRISCOS-UFF, tem por objetivo estabelecer os princípios, as diretrizes e as responsabilidades sobre o gerenciamento de riscos da UFF, contribuindo para o alcance dos objetivos estratégicos da instituição. A PGRISCOS-UFF segue as recomendações das normas vigentes, conforme pode ser observado na RESOLUÇÃO CUV/UFF No 161 DE 07 DE DEZEMBRO DE 2022, publicada no Boletim de Serviço- ANO LVII – N.° 02 03/01/2023 SEÇÃO III P.040.

No que tange à gestão de riscos, recomenda-se que unidades da UFF revisem e adequem seus processos de trabalho, avaliando as possibilidades e os riscos de vazamento de dados que podem ocorrer nas áreas que realizam tratamento de dados pessoais, em conformidade com a LGPD, adotando medidas de prevenção e mitigação dos riscos.

O tratamento de incidentes de segurança da informação, que envolvam o tratamento de dados pessoais, garantindo sua detecção, contenção, eliminação e recuperação, deve ser realizado no prazo estabelecido pela legislação vigente, conforme observado no anexo 13.

3.9. Definição de critérios de aferição do uso dos princípios “privacidade desde a concepção” e “privacidade por padrão”:

Privacidade desde a concepção (privacy by design) significa que a privacidade e a proteção de dados devem ser consideradas desde a concepção e durante todo o ciclo de vida, do sistema, serviço, ou processo de trabalho.

Privacidade por padrão (privacy by default) representa que a instituição adota medidas, utiliza ferramentas para preservar a privacidade como padrão, isto é, a configuração padrão já confere a maior expectativa de privacidade possível ao titular de dados pessoais.

Esse conceito significa que, se um serviço for implantado, quando estiver disponível ao público, as configurações mais seguras de privacidade deverão ser aplicadas por padrão.

4. RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD):

O relatório de impacto (RIPD) é a documentação que contém a descrição do tratamento de dados pessoais que podem gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais e às liberdades civis e aos direitos fundamentais do titular de dados, previstos na Lei Geral de Proteção de Dados Pessoais (LGPD).

O RIPD deve ser elaborado a partir dos resultados obtidos no Inventário de dados da instituição, quando poderão ser identificados os riscos potenciais dos tratamentos realizados com dados pessoais na UFF, conforme consta no Plano de Ação, que pode ser observado no anexo 3.

5. MONITORAMENTO E ADEQUAÇÃO CONTÍNUA À LGPD E ÀS REGULAMENTAÇÕES DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD):

O monitoramento da adequação das instituições à LGPD é feito pela CGU periodicamente por meio da avaliação do índice de maturidade. Na UFF, a avaliação é realizada pelo Comitê de Governança de Dados e Privacidade, sob a coordenação do Encarregado pelo Tratamento de Dados Pessoais, em períodos definidos no Plano de Ação, que pode ser observado no anexo 3, ou quando houver alteração nos processos internos ou na legislação.

REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27001 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão da segurança da informação. Rio de Janeiro, ABNT, 2013.

ABNT. Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro, ABNT, 2013.

ABNT. Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27701 – Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes. Rio de Janeiro, ABNT, 2019.

ABNT. Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27005:2023 Segurança da informação, segurança cibernética e proteção à privacidade — Orientações para gestão de riscos de segurança da informação.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados (LGPD)**. Diário Oficial da União: seção 1, Brasília, DF, ano 155, n. 157, p. 59-64, 15 ago. 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>.

BRASIL. Senado Federal. **Plano de Proteção de Dados Pessoais do Senado Federal.** Disponível em: <https://www12.senado.leg.br/institucional/protecao-dados/plano-de-protecao>.

BRASIL. Escola Nacional de Administração Pública. **Programa de Governança em Privacidade.** Disponível em:

<https://repositorio.enap.gov.br/bitstream/1/6479/2/Programa%20de%20Governan%C3%A7a%20_em%20Privacidade%20da%20Enap_PGP-Enap.pdf>.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Guia Orientativo - Tratamento de dados pessoais pelo Poder Público. Brasília, jun./2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-pode r-publico-anpd-versao-final.pdf

BRASIL. Portaria SGD/MGI nº 852, de 28 de março de 2023. Dispõe sobre o Programa de Privacidade e Segurança da Informação (PPSI). Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908

Anexos:

1) Política de privacidade e proteção de dados pessoais na UFF
2) Manual de Boas Práticas de Privacidade e Segurança da Informação na Universidade Federal Fluminense
3) Plano de Ação do CGDP
4) Portaria UFF 68.735 de 10 de outubro de 2024, publicada no Boletim de Serviço - ANO LVIII – N.° 128 11/10/2024 SEÇÃO IV P.130 (Encarregada de Dados Pessoais)
5) PORTARIA UFF Nº 68.595 de 22 de setembro de 2023, publicada no Boletim de Serviço - ANO LVII – N.° 180 22/09/2023 SEÇÃO IV P.045 (Comitê de Governança Digital)
6) PORTARIA UFF Nº 68.476 de 12 de janeiro de 2023, publicada no Boletim de Serviço - ANO LVI – N.° 12 17/01/2023 SEÇÃO IV P.083 (Comitê de Governança de Dados e Privacidade)
7) PORTARIA UFF Nº 68.509 de 22 de março de 2023, publicada no Boletim de Serviço - ANO LVII – N.° 55 22/03/2023 SEÇÃO IV P.105 (Comitê de Segurança da Informação)
8) Formulário aplicado para mensurar o índice de maturidade sobre LGPD
9) Plano de capacitação em proteção de dados pessoais
10) Plano de capacitação em segurança da informação
11) Plano de Comunicação
12) Política de Segurança da Informação
13) Política de Gestão de Riscos

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL FLUMINENSE

PORTARIA UFF Nº 68.760 de 27 de dezembro de 2024

Institui a Política de Privacidade e Proteção de Dados Pessoais da Universidade Federal Fluminense (UFF).

O VICE-REITOR NO EXERCÍCIO DA REITORIA DA UNIVERSIDADE FEDERAL FLUMINENSE, no uso de suas atribuições legais, estatutárias e regimentais,

CONSIDERANDO a Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso às informações;;

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

CONSIDERANDO o Decreto nº 7.724, de 16 de maio de 2012, que regulamenta da Lei nº 12.527, de 2011;

CONSIDERANDO as normativas internas da UFF que versam sobre o tema;

CONSIDERANDO a aprovação da Política de Privacidade e Proteção de Dados Pessoais da Universidade Federal Fluminense (UFF), em 25/11/2024, conforme o processo SEI nº 23069.152958/2024-71,

RESOLVE:

Art. 1º Instituir a Política de Privacidade e Proteção de Dados Pessoais da Universidade Federal Fluminense (UFF) em anexo.

Classif. documental	002

Art. 2° Esta Portaria entra em vigor na data de sua publicação no Boletim de Serviço desta Universidade.

FABIO BARBOZA PASSOS
Vice-Reitor no Exercício da Reitoria

ANEXO

Política de Privacidade e Proteção de Dados Pessoais da Universidade Federal Fluminense

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º A presente política estabelece diretrizes e princípios que devem nortear o tratamento de dados pessoais, no âmbito da Universidade Federal Fluminense (UFF) e em conformidade com a Lei Geral de Proteção de Dados Pessoais, bem como estabelecer critérios e procedimentos gerais a serem observados por servidores técnico-administrativos, docentes, alunos, estagiários, colaboradores em geral e demais cidadãos interessados com objetivo de níveis adequados de proteção aos dados pessoais e oferecer garantias aos titulares de dados pessoais quanto à confidencialidade e à privacidade.

Art. 2º Para os efeitos desta política, considera-se:

I - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento sobre qualquer assunto, acadêmico ou não, contidos em qualquer meio, suporte ou formato;

II - dados processados: dados submetidos a qualquer operação ou tratamento por meio de processamento eletrônico ou por meio automatizado com o emprego de tecnologia da informação;

III - documento: unidade de registro de informações, qualquer que seja o suporte ou formato;

IV - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

V - 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;

VI - dado anonimizado: dado relativo ao titular, que pode ter sido alterado ou parcialmente oculto, de modo que não permita a identificação da pessoa natural, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

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

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

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

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

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

XII - agentes de tratamento: o controlador e o operador;

XIII - 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;

XIV - 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;

XV - pseudonimização: tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro;

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

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

XVIII – eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados digital ou arquivo físico, com emprego de procedimento adequado para essa ação.

Art. 3º Consideram-se os seguintes princípios no tratamento de dados pessoais:

I - boa-fé: convicção de agir com correção e em conformidade com o Direito;

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

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

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

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

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

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

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

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

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

CAPÍTULO II
DO TRATAMENTO DE DADOS PESSOAIS

Art. 4º O tratamento de dados pessoais sob responsabilidade das Pró-Reitorias, Superintendências, Unidades Acadêmicas ou outras unidades da UFF é permitido, sem necessidade de consentimento pelo titular, nas seguintes hipóteses:

I- mediante a correta divulgação ao titular das finalidades determinadas, na coleta e posterior tratamento dos dados pessoais;

II - quando necessários para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - quando necessários para planejamento, execução ou avaliação de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres e demais ações específicas;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

Incluir definição de órgãos de pesquisa

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo administrativo;

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; e

IX - quando necessário para atender aos interesses legítimos do controlador, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

§1º. É vedado o tratamento de dados pessoais mediante vício de consentimento.

§2º. Quando a UFF necessitar comunicar ou compartilhar dados pessoais com outros controladores, ou para outras finalidades que não aquela que suscitou a disponibilização dos dados pelo titular, deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta política.

§3º. A solicitação de consentimento para tratamento de dados deve ser clara, devendo descrever o objetivo e destacar as outras solicitações, conforme Art. 8º da Lei nº 13.709, de 2018. (LGDP).

Art. 5º O tratamento dos dados pessoais deverá ser realizado durante todo o ciclo de vida destes na UFF, em acordo com a legislação, no que diz respeito ao acesso, coleta, avaliação, classificação, armazenamento, controle, extração, comunicação, distribuição, difusão, eliminação, modificação, processamento, produção, recepção, reprodução, transferência, transmissão e utilização.

Art. 6º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados e, mediante solicitação, estas deverão ser disponibilizadas de forma clara, adequada, acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I - finalidade específica do tratamento;

II - forma e duração do tratamento;

III - identificação do controlador;

IV - informações de contato do controlador;

V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

VI - responsabilidades dos agentes que realizarão o tratamento; e

VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 da Lei nº 13.709, de 2018. (LGPD)

Seção I
Do Tratamento de Dados Pessoais Sensíveis

Art. 7º O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) para o exercício regular de direitos em processo administrativo;

e) para a proteção da vida ou da incolumidade física do titular ou de terceiro;

f) para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da

LGPD e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Seção II
Da anonimização de dados pessoais

Art. 8º Os dados anonimizados não serão considerados dados pessoais, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

CAPÍTULO III
Do funcionamento

Art. 9º No âmbito da UFF, o Controlador é representado pelo Reitor, e o Encarregado de Dados Pessoais é designado por meio de Portaria do Reitor.

Art. 10 A Governança de Dados e Privacidade é atribuição do Comitê de Governança de Dados e Privacidade - CGDP instituído por meio de Portaria, coordenado pelo Encarregado e vinculado ao Controlador.

Art. 11 O Comitê de Governança de Dados e Privacidade tem composição multidisciplinar, com abrangência transversal à Universidade Federal Fluminense para tratar de assuntos relativos à proteção de dados, de segurança da informação, integridade, acesso às informações e gestão de riscos, referentes ao tratamento de dados pessoais.

Parágrafo único. O Comitê de Governança de Dados e Privacidade é composto por representantes do Comitê de Governança Digital, Comissão de Segurança da Informação, Comissão de Dados Abertos, Subcomitê de Gestão de Riscos e pelo Encarregado pelo Tratamento de Dados Pessoais na UFF.

Art. 12 O Comitê de Governança de Dados e Privacidade (CGDP) tem por escopo promover as boas práticas de gestão de dados e privacidade na UFF, promovendo discussões estratégicas e emitindo recomendações em conformidade com a Autoridade Nacional de Proteção de Dados (ANPD) e a Controladoria Geral da União (CGU) consoante ao disposto na Lei Geral de Proteção de Dados Pessoais.

Art. 13 Cada unidade organizacional, será convocada por meio de suas chefias de unidades, para colaborarem no que for solicitado pelo Comitê de Governança de Dados e Privacidade – CGDP, no desenvolvimento das atividades previstas nos planos de ação estabelecidos para adequação e/ou revisões nos fluxos de processos na UFF, em atendimento aos preceitos legais sobre o tratamento de dados pessoais, cabendo ao Encarregado de Dados Pessoais, propor o planejamento das atividades ao Reitor, na figura de controlador, zelar pelo desenvolvimento das ações necessárias ao atendimento à legislação vigente.

Art. 14 As informações solicitadas pelo Encarregado, em cumprimento de suas funções gerenciais sobre o tratamento dos dados pessoais, devem ser encaminhadas dentro dos prazos previstos, para que se possa cumprir as obrigações estabelecidas na legislação, as normativas e as orientações expedidas pelos órgãos de controle.

Seção III
Do Controlador de Dados Pessoais

Art. 15 O controlador é o agente responsável por tomar as principais decisões referentes aos tratamentos de dados pessoais e por definir a finalidade dos tratamentos.

Art. 16 Compete ao Controlador:

I - instituir estruturas (Uorgs, Comissões, Comitês) que tratem de Segurança da Informação, Proteção de Dados e Privacidade, definindo as respectivas atribuições e competências com base da Lei Geral de Proteção de Dados;

II - designar o Encarregado pelas informações relativas aos dados pessoais;

III - fornecer as instruções para a política de governança dos dados pessoais e respectivos programas;

IV - verificar a observância das normativas sobre a matéria na UFF;

V - comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular do dado, a ocorrência de incidentes de segurança com os dados pessoais, que possam causar danos ou riscos relevantes ao titular;

VI - incentivar a disseminação da cultura da privacidade de dados pessoais nas unidades da UFF;

VII - determinar, junto ao Encarregado de Dados Pessoais, a permanente atualização das normativas internas relativas à LGPD, bem como suas ações e programas.

Seção IV
Do Encarregado pelos Dados Pessoais

Art. 17 O Encarregado é o agente responsável por garantir a conformidade da instituição no tocante à LGPD.

Parágrafo único. As informações sobre contato do Encarregado deverão ser divulgadas publicamente no sítio eletrônico da UFF.

Art. 18 Compete ao Encarregado:

I - realizar a interlocução entre a instituição/controlador, os servidores, os contratados, os titulares dos dados, e a Autoridade Nacional de Proteção de Dados (ANPD);

II - prestar esclarecimentos, realizar comunicações, orientar servidores, contratados e demais envolvidos sobre as práticas adotadas para garantir a proteção dos dados pessoais;

III - prestar esclarecimentos e adotar providências sobre reclamações e comunicações dos titulares apresentadas na plataforma oficial de Ouvidoria e Acesso à Informação, conforme legislação em vigor;

IV - receber comunicações da ANPD e adotar providências.

Seção V
Da custódia dos dados durante o tratamento

Art. 19 Compete, aos servidores responsáveis pelo tratamento de dados nos procedimentos acadêmicos e/ou administrativos pertinentes aos serviços da UFF, independente do setor - pró reitorias, superintendências, unidades acadêmicas, serviços especializados:

I - documentar as operações que lhe cabem realizar durante o processo de tratamento de dados pessoais;

II - proteger a privacidade dos dados pessoais de acordo com o amparo legal vigente;

III - descrever os tipos de dados coletados;

IV - utilizar metodologia de coleta dos dados pessoais que considere a minimização necessária para alcançar a finalidade do processo;

V - capacitar-se para exercer as atividades que envolvam dados pessoais com eficiência, ética, critério e responsabilidade.

Art. 20 No período de tratamento de dados, os servidores que estiverem realizando o tratamento, serão responsáveis pela segurança das informações e das ações de acesso e de mitigação de riscos relacionadas a elas.

§ 1º Quando o servidor fizer uso de ferramentas, sistemas ou estrutura disponibilizada pela UFF, para tratamento dos dados, a responsabilidade é solidária junto à Superintendência de Tecnologia da Informação (STI), que deve manter rotinas técnicas de minimização de riscos de segurança da informação, com base na Política de Segurança da Informação da instituição, aprovada pelo Comitê de Governança, Integridade, Riscos e Controle (CGIRC).

§ 2º As alterações nas permissões de acesso aos dados, devem ser registradas pelos setores responsáveis, com a finalidade de rastreamento e monitoramento no caso de vazamentos de dados e dos procedimentos para minimização de riscos associados.

§ 3º Se identificada alguma inconsistência ou irregularidade nos dados acessados face a permissão de acesso declarada ao servidor, este deve notificar a sua chefia imediata e/ou ao setor responsável pelos dados, para que o problema seja identificado e adotadas as providências cabíveis.

Seção VI
Da proteção dos dados pessoais

Art. 21 A proteção dos dados pessoais deve estar em consonância com a Lei Geral de Dados Pessoais e outras legislações e normativas dos órgãos de controle e da UFF sobre o tema.

Art. 22 Os setores que produzem documentação deverão utilizar medidas de segurança administrativas, técnicas e físicas apropriadas e suficientes para proteger, a confidencialidade e integridade dos dados pessoais contidos no suporte (meio físico ou digital), incluindo a proteção contra acesso não autorizado.

Art. 23 A proteção dos dados pessoais deve ser observada pelas áreas publicadoras de conteúdo nos sistemas da UFF, obedecendo aos princípios da necessidade e da finalidade.

Art. 24 Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento de dados pessoais, obrigam-se a garantir a proteção e segurança da informação sobre dados pessoais prevista nesta política, mesmo após o término do tratamento dos mesmos.

Art. 25 Os servidores devem estar cientes sobre sua responsabilidade e alinhados com as normas vigentes sobre o tema, no oferecimento dos serviços prestados e, para tal, devem participar das iniciativas de capacitação da instituição.

Seção VII
Do incidente de segurança com dados pessoais

Art. 26 Incidente de segurança com dados pessoais é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração, vazamento ou, ainda, qualquer forma de tratamento de dados inadequada ou ilícita, que possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

Art. 27 Identificado o incidente que coloque em risco a segurança de dados pessoais, devem ser realizados procedimentos específicos:

a) Avaliação interna do incidente com o objetivo de obter informações iniciais sobre impacto do evento; natureza, categoria e quantidade de titulares de dados pessoais afetados; categoria e quantidade de dados afetados, consequências do incidente para os titulares e a entidade, criticidade e probabilidade.

b) Caberá à Equipe de Tratamento e Resposta à Incidentes (ETIR), na UFF, identificar se o incidente tem causa ou origem cibernética, tais como, mas não se limitando a: ataques cibernéticos, falhas nos sistemas ou na estrutura da STI/UFF.

c) Outras formas de violação de dados serão comunicadas ao encarregado, que fará a comunicação ao controlador, à ANPD e ao titular de dados pessoais, conforme recomenda a legislação.

d) Emissão de relatório final com todas as informações coletadas, as ações realizadas para o tratamento efetivo do evento, as considerações necessárias para promover a melhoria contínua no atendimento de incidentes e para atualizar o Relatório de Impacto à Proteção de Dados Pessoais.

CAPÍTULO IV
Do canal de atendimento às demandas de Proteção de Dados na UFF

Art. 28 Os titulares dos dados pessoais podem abrir demanda junto a plataforma de Ouvidoria e acesso à informação, disponibilizada pela Controladoria Geral da União para apresentar reclamações ou solicitar informações sobre o tratamento de seus dados pessoais pela UFF.

DAS DISPOSIÇÕES FINAIS

Art. 29 Os casos omissos a esta Política serão resolvidos pelo Comitê de Governança, Integridade, Riscos e Controle (CGIRC) da UFF.

Universidade Federal Fluminense

MANUAL DE BOAS PRÁTICAS DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO NA UNIVERSIDADE FEDERAL FLUMINENSE

Sumário

INTRODUÇÃO 3

IMPLANTAÇÃO DO PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI) NA UFF 4

SEGURANÇA DA INFORMAÇÃO E SEUS PRINCÍPIOS 5

GESTÃO DA PRIVACIDADE 6

DAS BOAS PRÁTICAS DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO NA UFF 7

LINKS ÚTEIS 17

Introdução

Este manual foi elaborado com o objetivo de difundir boas práticas de privacidade e segurança da informação, de modo a garantir a proteção adequada dos dados pessoais coletados, com vistas a promover a adoção das mesmas por meio de disponibilização de recomendações e procedimentos relacionados à temática de Privacidade e Segurança da Informação.

Ações de sensibilização, conscientização e capacitação dos recursos humanos nos temas relacionados à privacidade e à segurança da informação, estas previstas no Plano de Capacitação (elaborado pela Escola de Governança em Gestão Pública) e Plano de Comunicação da UFF (elaborado pela Superintendência de Comunicação Social) presentes na página do Comitê de Governança de Dados e Privacidade.

Implantação do Programa de Privacidade e Segurança da Informação na UFF

A Privacidade e Segurança da Informação no Governo Digital tem como ponto de partida o Programa de Privacidade e Segurança da Informação (PPSI) instituído pela PORTARIA SGD/MGI Nº 852, DE 28 DE MARÇO DE 2023 tem como objetivo elevar a maturidade e a resiliência dos órgãos e entidades, em termos de privacidade e segurança da informação, no âmbito do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP).

A Universidade Federal Fluminense é integrante do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP e para a implantação e adequação da instituição ao Programa de Privacidade e Segurança da Informação na instituição.

O conjunto de ações para atendimento da temática privacidade e segurança da informação estão sendo desenvolvidas pelos Comitês de Segurança da Informação (CSI) e de Governança de Dados e Privacidade (CGDP), de sob a supervisão da alta gestão da UFF

Segurança da Informação e seus Princípios

A segurança da informação envolve uma série de boas práticas e estratégias com foco em garantir a integridade de dados contra ataques cibernéticos e várias outras ameaças e riscos que podem prejudicar a instituição.

Princípios da Segurança da Informação:

- **Confidencialidade:** informação conhecida apenas por quem necessita conhecê-la, ou seja, pessoas autorizadas;
- **Integridade:** informação mantida íntegra, inalterada, garantindo a preservação dos dados;
- **Disponibilidade:** os serviços devem estar acessíveis e disponíveis para os usuários que têm autorização para acessá-los;
- **Autenticidade:** os dados são legítimos, verdadeiros, sem intervenções de pessoas não autorizadas;
- **Conformidade:** todos os procedimentos voltados à segurança da informação precisam estar em conformidade com a lei. Os dados protegidos devem atender a Lei Geral de Proteção de Dados Pessoais, garantindo que a instituição atue dentro do que prevê a legislação vigente;

Gestão da Privacidade

A gestão de privacidade busca atuar sobre como a informação é coletada, distribuída e utilizada dentro de uma organização.

Quando a instituição possui uma estrutura de segurança da informação bem implantada, há a aproximação do atingimento da conformidade com as questões de privacidade de proteção de dados exigidos nas regulamentações.

A UFF adota o princípio da privacidade por padrão, que tem como caraterística fundamental oferecer o grau máximo de privacidade, garantindo que os dados pessoais sejam protegidos automaticamente em qualquer sistema.

O objetivo é o atingir ao que preconiza outro princípio que é a do segurança de ponta a ponta, significando que a proteção se estende ao ciclo de total de vida dos dados, isto é, os dados coletados são protegidos durante todo seu ciclo de vida e abrangendo coleta, uso, acesso, armazenamento e descarte. Este princípio parte do pressuposto de que, sem segurança adequada, não existe privacidade.

Das Boas Práticas de Privacidade e de Segurança da Informação

Recomendações para o uso consciente de sistemas

Os colaboradores e usuários dos sistemas devem fazer o uso consciente dos mesmos. Algumas ações, ainda que não intencionais, podem gerar incidentes de segurança.

O nível de conscientização e treinamento dos colaboradores pode minimizar os riscos a incidentes de segurança.

- Ao terminar o seu trabalho, faça log off, ou seja, feche os e-mails, sistemas e contas abertas para que não haja uso indevido por outra pessoa.

SEI (Sistema Eletrônico de Informações)

Ao inserir um documento em um processo no sistema, seja ele um documento interno ou externo, é fundamental que o usuário se atente ao nível de acesso indicado no material de apoio para aquele documento.

- É importante verificar se aquele documento contém informações pessoais como número de CPF, identidade, entre outros, o que faz com que esse documento deva ser classificado como Restrito.
- Mas atenção! Estamos nos referindo a documentos. Os processos, de forma geral, são classificados como públicos.

Na geração de processos ou documentos, atente-se à adequada configuração do nível de acesso (público, restrito ou sigiloso). Quando houver o tratamento de dados ou informações pessoais o nível de acesso deve ser restrito sob a hipótese legal de "Informação Pessoal (Art. 31 da Lei no 12.527/2011)".

Quando for necessário criar processos ou documentos públicos, ou disponibilizá-los a usuários externos, recomenda-se que o servidor proceda com a descaracterização dos dados pessoais existentes, promovendo o equilíbrio entre a transparência e a proteção dos dados pessoais.

Envio de email pelo SEI

Ao enviar um e-mail pelo SEI é fundamental verificar se o documento contém informações pessoais, como número de CPF, identidade, entre outros, o que faz com que esse e-mail deva ser classificado como “Restrito”.

Para isso, depois de enviar o e-mail, basta:

- Clicar no documento que aparecerá na árvore do processo;
- Clicar no botão “Consultar/Alterar documento”;
- Marcar a opção “Restrito”, a Hipótese Legal "Informação pessoal (Art. 31 da Lei nº 12.527/2011) e clicar em "Confirmar dados".

Ver também em pílulas do SEI.

Cadastro em sites, aplicativos e dispositivos móveis

- Ao fazer cadastros em sites e aplicativos, só forneça dados que sejam obrigatórios
- Nos dispositivos móveis, só leia códigos QR se tiver certeza de que a fonte é confiável
- Ao instalar e usar um aplicativo, autorize apenas acessos essenciais a seu funcionamento e operação
- Ative a autenticação de duas etapas em todas as plataformas que você usa que tenham essa função;

Controle de acesso

Os controles de acesso lógico são implantados com o objetivo de garantir que:

- apenas usuários autorizados tenham acesso aos recursos;
- os usuários tenham acesso apenas aos recursos realmente necessários para a execução de suas tarefas;
- o acesso a recursos críticos deve ser bem monitorado e restrito a poucas pessoas;

Uso de senhas

- Vale lembrar também que utilizar a mesma senha para vários sistemas não é uma boa prática, pois a primeira atitude de um invasor, quando descobre a senha de um usuário em um sistema vulnerável, é tentar a mesma senha em outros sistemas a que o usuário tenha acesso.
- não compartilhar senhas;
- evitar registrar as senhas em papel;
- selecionar senhas de boa qualidade, evitando o uso de senhas muito curtas ou muito longas, que os obriguem a escrevê-las em um pedaço de papel para não serem esquecidas
- Se você realmente não conseguir memorizar sua senha e tiver que escrevê-la em algum pedaço de papel, tenha pelo menos o cuidado de não identificá-la como sendo uma senha.
- Nunca deixe uma senha visível, afixada em papel no próprio computador, em cima da mesa ou no seu local de trabalho.
- Nunca guarde a senha junto com a sua identificação de usuário e nunca a envie por e-mail ou armazene em arquivos do computador.
- Crie senhas fortes, difíceis de adivinhar, e não as repita

Criação de senhas

Como escolher uma boa senha?

- Geralmente são consideradas boas senhas aquelas que incluem, na composição, letras (maiúsculas e minúsculas), números e símbolos embaralhados, totalizando mais de oito caracteres.

- Também é conveniente escolher senhas que possam ser digitadas rapidamente, dificultando que outras pessoas, a certa distância ou por cima dos ombros, possam identificar a sequência de caracteres.
- É também recomendável não utilizar a mesma senha para vários sistemas. Se um deles não for devidamente protegido, a senha poderá ser descoberta e utilizada nos sistemas que, a priori, estariam seguros.

Senhas que devem ser evitadas

Os usuários devem evitar senhas compostas de elementos facilmente identificáveis por possíveis invasores, como por exemplo:

- nome do usuário;
- identificador do usuário (ID), mesmo que os caracteres estejam embaralhados;
- nome de membros de sua família ou de amigos íntimos;
- nomes de pessoas ou lugares em geral;
- nome do sistema operacional ou da máquina que está sendo utilizada;
- nomes próprios;
- datas;
- números de telefone, de cartão de crédito, de carteira de identidade ou de outros documentos pessoais;
- placas ou marcas de carro;
- palavras que constam de dicionários em qualquer idioma;
- letras ou números repetidos;

- letras seguidas do teclado do computador (ASDFG, YUIOP);
- objetos ou locais que podem ser vistos a partir da mesa do usuário (nome de um livro na estante, nome de uma loja vista pela janela);
- qualquer senha com menos de 8 caracteres.

Emails

Evite o compartilhamento de dados pessoais.

- Ao encaminhar e-mails a mais de um destinatário, principalmente de fora da instituição, incluir todos em cópia oculta para que não haja o compartilhamento do endereço eletrônico.
- Encaminhar e-mails apenas para áreas ou servidores que precisam receber a informação.
- Ao encaminhar e-mails recebidos, atentar-se para apagar do corpo do e-mail referências a dados pessoais de remetentes e destinatários anteriores.
- A exigência de cópia de documentos por e-mails e outros meios eletrônicos deve estar relacionada à finalidade da coleta dos dados pessoais e o armazenamento, se necessário, deve ser realizado de forma a impedir o acesso de pessoas não autorizadas;

Uso de emails institucionais

- A recomendação é que as comunicações internas da UFF devem ser feitas por e-mails da instituição,isto é, e-mails com o perfil para uso institucional.

- Caso algum servidor/setor/unidade ainda não possua e-mail de perfil institucional ou problemas para uso do mesmo, isto pode ser regularizado junto à STI, entrando em contato com https://app.uff.br/atendimento informando o vínculo com a Universidade e demanda pretendida.
- O uso da informação institucional pressupõe condutas adequadas com o perfil de acesso e responsabilização por uso inadequado.
- Quando utilizamos e-mails não institucionais, ou de e-mails que não constam de nossos contatos de e-mail, surge um alerta para cuidado com o compartilhamento das informações confidenciais, este e-mail não faz parte da sua organização nem dos seus contatos.
- Outra recomendação é que nas assinaturas dos e-mails devem vir com a UORG na qual o servidor está lotado e assinadas pelo remetente da mensagem e não somente a indicação do setor.

Como evitar exposição de dados

1 - Uso de impressoras e scanners, salvamento de documentos em pastas:

- Não deixe documentos que contenham dados pessoais nas máquinas de xerox nem em cima das mesas;
- Faça revisão periódica dos arquivos que estão no computador para eliminar documentos que foram digitalizados e já atingiram a sua finalidade.

- Ao escanear um documento para uma pasta pública, lembre-se de copiá-lo para sua pasta privativa e apagá-lo da pasta pública o mais rapidamente possível.
- Ao imprimir documentos que contenham dados pessoais, certifique-se que somente as pessoas autorizadas tenham acesso, não deixando cópias disponíveis, evitando exposição de dados.

2 - Uso de mídias e armazenamento:

- Guarde as mídias em local seguro
- Documentos com dados pessoais procure salvá-los protegidos com senha
- Salve as informações em sistemas UFF ou geridos pela UFF
- Evite o salvamento no seu PC a informação que contenha dados pessoais.
- Os sistemas uff foram construídos para serem seguros por obedecer parâmetros de integridade, confidencialidade e segurança da informação.

3 - Compartilhamento de informações

- Verificar se a informação, o documento, print de tela, etc. ao ser compartilhado em e-mail ou sistemas, contém dados pessoais. Caso haja dado que não possa ser compartilhado, este deve ser protegido/tarjado para divulgação de terceiros.

4 - Áreas publicadoras

- As áreas publicadoras de conteúdo da UFF devem observar a proteção dos dados pessoais dos titulares.
- Observar se na publicação nas páginas UFF, conforme orienta o Manual de boas práticas do site institucional da Superintendência de Comunicação Social da UFF: que não sejam divulgadas informações pessoais de servidores ou estudantes e esteja atento às diretrizes da Lei Geral de Proteção de Dados (LGPD).
- A recomendação se estende para redes sociais, como consta no Manual de boas Práticas e Mídias Sociais da Superintendência de Comunicação Social da UFF: nunca compartilhe dados pessoais ou confidenciais de usuários e de integrantes da comunidade acadêmica, atuando em conformidade com a Lei Geral de Proteção de Dados (LGPD).

5 - Correspondências

- As embalagens e envelopes das correspondências podem vir com dados pessoais expostos do remetente ou recebedor.
- Atentar também para os códigos de barra e/ou QR Codes colados que permitem acessar dados pessoais.
- O uso do endereço de trabalho é indevido correspondência que não forem de cunho institucional.

- Ao inutilizar as correspondências, embalagens e envelopes de correspondências, certifique-se de que o dado pessoal foi protegido, como marcação com canetas permanentes que ocultem/encubram os dados, uso de fragmentadoras de papel.
- No mesmo sentido a eliminação de cartões, crachás e dispositivos que não tenham mais o uso dentro da instituição.

6 - Eliminação de cópias

- Na produção de documentos, relatórios, apostilas, observar se ao eliminar cópias tiradas a mais, estas contem dados pessoais, motivo pelo qual devem ser eliminadas adequadamente.

Obs: Estas cópias não se confundem com a eliminação de documentos oficiais que possuem gestão documental com procedimentos já estabelecidos pela UFF.

Acesso a contas e sistemas em equipamento fora da UFF

- Evite, sempre, usar contas da UFF em qualquer micro disponibilizado publicamente.

- Evite o uso de wi-fi público, para acessar sistemas da UFF

- Em particular, em micros fora da UFF, nunca use a opção de gravar senhas em micros utilizados por outras pessoas, além de você: se algum outro usuário do micro clicar em um link que baixe um vírus, pode ocorrer que todas as contas e senhas armazenadas neste micro sejam capturadas pelo agressor, e poderão ser usadas por ele, ou disponibilizadas publicamente.

- PORTARIA UFF Nº 68.760 de 27 de dezembro de 2024 Institui a Política de Privacidade e Proteção de Dados Pessoais da Universidade Federal Fluminense (UFF).

https://boletimdeservico.uff.br/wp-content/uploads/sites/620/2024/12/159-24.pdf

Links úteis

- https://www.uff.br/sobre/comites-e-comissoes/
  Aba Comitê de Governança de Dados e Privacidade
- https://www.uff.br/sobre/comites-e-comissoes/
  Aba Comitê de Segurança da Informação
- https://www.uff.br/lgpd/
- https://www.uff.br/wp-content/uploads/2024/05/plano_de_capacitacao_em_protecao_de_dados_pessoais_1.pdf
- https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias-e-modelos
- https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf
- https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/cartilha_ppsi.pdf
- https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/modelo_ppdp.pdf
- https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca

Links úteis

- CARTILHA DE BOAS PRÁTICAS LGPD - TRATAMENTO DE DADOS PESSOAIS (SETIC – Superintendência Estadual de Tecnologia da Informação ou Comunicação) _ RONDÔNIA

- Brasil. Tribunal de Contas da União. Cinco controles de segurança cibernética para ontem / Tribunal de Contas da União. – Brasília : TCU, 2022. 36 p. : il. color.

- Brasil. Tribunal de Contas da União. Boas práticas em segurança da informação / Tribunal de Contas da União. – 4. ed. – Brasília : TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012

PLANO DE AÇÃO

CGDP

2023/2024

OBJETIVOS/ MARCOS	ATIVIDADES	QUEM	COMO	PRAZO
1. Divulgação de informações sobre a LGPD, com vista ao reforço da cultura organizacional da UFF para a LGPD	Divulgar informes sobre a LGPD na UFF	Encarregado, SCS , PROGEPE/ EGGP	Definição de planejamento anual : 1. das ações da CGDP e seus parceiros para adequação dos serviços da UFF à legislação; 2. dos programas de formação / treinamento /atualização disponíveis aos servidores da UFF que lidam com dados pessoais .	A partir de março 2023 (ação contínua)

OBJETIVOS/ MARCOS	ATIVIDADES	QUEM	COMO	PRAZO
2. Inventário de dados pessoais	a. Atualizar o diagnóstico atual da cultura organizacional da UFF, com vistas a adequação da UFF à LGPD, com base na aplicação de questionários para áreas de serviços da UFF.	Encarregado e SCS	Aplicação de questionário a todos os servidores da UFF, para análise da maturidade da instiituição sobre o conhecimento e aplicação da legislação e suas normativas no tratamento de dados pessoais nos serviços públicos executados nos diversos setores administrativos.	03/ 2023 até 05/2023
	b. Estabelecer modelo/gabarito de coleta sistemática dos dados para elaboração do Inventário de Dados na UFF	CGDP e convidados STI	Estudo do modelo disponibilizado pela CGU em guia específico, para adaptação aos serviços oferecidos pela UFF. O modelo será enviado a cada área de gestão para elaboração do Inventário de Dados da área.	03/2023 até 04/2023
	c. Aplicar o modelo/gabarito nas áreas de gestão administrativa que coletam dados pessoais para oferta de serviços	CGDP, PróReitorias, Superintendências, e outras	1.Estabelecer responsável pelo preenchimento do gabarito do Inventário de Dados em cada área; 2. Realização de treinamento com esses responsáveis; 3. Preenchimento do gabarito para todos os serviços das áreas que coletam e tratam dados pessoais , com base na carta de serviços da UFF.	05/2023 até 10/2023

3. Relatório de Impacto à Proteção dos Dados Pessoais- RIPD	a. Descrição dos tipos de dados coletados constantes do Inventário de dados da UFF e das metodologias utilizadas para as coletas	CGDP e PLAD /PROPLAN	Mapeamento sistemático, com base no inventário de dados, dos riscos prováveis em virtude dos formatos de coleta e tratamento dos dados pessoais na execução dos serviços na UFF.	10/2023 até 04/2024
	b. Analisar/ranquear os riscos que apresentam maior probabilidade nos processos de tratamento de dados pessoais, juntamente com o impacto que causam para a conformidade com a LGPD		Avaliação dos riscos-chave envolvidos nos tratamentos de dados pessoais, com potencial de comprometer a segurança dos sistemas de dados na UFF e causar situações de não -conformidade com a legislação, em limites ináceitáveis.	
	c. Anaĺise das medidas, salvaguardas e mecanismos de mitigação de riscos já adotados		Verificação da existência e adequação dos processos de controles internos na gestão de riscos, para gerenciamento dos limites de exposição em cada órgão/unidade/área	
	d. Proposição de ações específicas que deverão ser implementadas para mitigar os riscos de maior impacto para a conformidade com a LGPD		Emissão de recomendações às diversas áreas sobre seus processos de tratamento com a finalidade de mitigar os riscos observados.	
	e. Apresentar ao CGIRC/UFF, o RIPD, para aprovação e posterior publicação em Portaria .		Definição do relatório de Impacto à Proteção de Dados da UFF, em atendimento à exigência da LGPD.	

4. Levantamento e adequação de contratos praticados na UFF	Identificação dos contratos que coletam, transferem e processam dados pessoais, com base no inventário de dados pessoais da UFF e sua atualização de acordo com a LGPD.	CGDP, Pró Reitorias, Superintendências, e GABR	Mapeamento dos contratos que coletam, transferem e processam dados pessoais, com base no inventário de dados pessoais da UFF	10/2023 até 12/2024
			Adequação dos diversos termos de contratos, para definir Instrução Normativa com modelos para a UFF.	01/2024 até 03/2024

5. Implementação da “Politica de Governança de Privacidade - PGP” da UFF

a. Atualizar / definir as políticas e práticas de privacidade de dados	CGDP e PLAD/PROPLAN	Revisão/atualização do Plano de Gestão de Riscos, com vistas a verificar a previsão de conceitos, metodologias e ferramentas que estejam compatíveis com o previsto na LGPD.	05/2023 até 08/2023
b.Atualizar /definir a Política de Segurança de Dados / Informação	CGDP e Comitê de Segurança da Informação - CSI	Revisão/atualização da Política de Segurança da Informação , com vistas a verificar sua compatibilidade com as normas previstas na LGPD.	

5. Implementação da “Politica de Governança de Privacidade - PGP” da UFF

c. Estabelecer o Plano de Capacitação e Comunicações	CGDP, PROGEPE e SCS	Definição de um planejamento para capacitação dos servidores sobre os cuidados com a coleta e tratamento de dados pessoais, com vistas às exigências da LGPD	03/2023 até 06/2023
d.Estabelecer IN para os termos de uso de dados pessoais	CGDP e convidados	Definição de documento normalizador/ orientador sobre o tratamento, compartilhamento, divulgação, guarda e descarte de documentos com dados pessoais.	
e. Definir IN para produção de serviços baseados em cultura de segurança e proteção de dados (Privacy by Design)		Definição de documento normalizador/ orientador sobre o mapeamento de serviços a serem implantados nas áreas, com prévia adoção de metodos que garantam atendimento dos princípios da LGPD.	
f. Estabelecer os termos da Politica de Governança em Privacidade da UFF		Definição da PGP/UFF , aprovado pelo CGIRC/UFF e publicado em Portaria do Reitor	Até 06/2024

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL FLUMINENSE

PORTARIA UFF Nº 68.735 de 10 de outubro de 2024

Designa Encarregada pelo Tratamento dos Dados Pessoais e substituto na Universidade Federal Fluminense.

O VICE-REITOR NO EXERCÍCIO DA REITORIA da UNIVERSIDADE FEDERAL FLUMINENSE, no uso de suas atribuições legais, estatutárias e regimentais,

CONSIDERANDO o disposto no Art. 1º da Instrução Normativa SGD/ME nº 117, de 19 de novembro de 2020, e em cumprimento ao Art. 23, inciso III, e Art. 41 da Lei 13.709, de 14 de agosto de 2018 e a Resolução CD/ANP nº 18, de 16 de julho de 2024.

RESOLVE:

Art. 1º Designar a servidora CARLA SIQUEIRA DA SILVA, Assistente em Administração, SIAPE 1098886, lotada na Ouvidoria - OUV/GAR como Encarregada pelo Tratamento dos Dados Pessoais na Universidade Federal Fluminense.

Art. 2º O servidor MARCOS TADEU VON LUTZOW VIDAL, Professor do Magistério Superior - Assistente, SIAPE 310513, lotado no TET - DEPARTAMENTO DE ENGENHARIA DE TELECOMUNICAÇÕES atuará como substituto da Encarregada em suas ausências, impedimentos e vacância.

Art. 3º A Encarregada pelo Tratamento de Dados Pessoais é a 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), dentre outras atribuições, é o responsável por orientar a respeito das práticas a serem tomadas em relação à proteção de dados pessoais, nos termos do Art. 41, Parágrafo 2º, da LGPD.

Classif. documental	011.1

Art. 4º A Encarregada atua também na Coordenação do Comitê de Governança de Dados e Privacidade (CGDP) instituído por PORTARIA UFF nº 68.476 de 12 de janeiro de 2023, que tem com o objetivo de definir o direcionamento, o monitoramento, a supervisão e a avaliação das práticas da gestão, para garantir a proteção de dados e da privacidade no âmbito da Universidade Federal Fluminense, conforme disposto na Lei Geral de Proteção de Dados - LGPD e suas normativas.

Art. 5º A presente designação não corresponde à Função Gratificada ou Cargo de Direção.

Art. 6º A presente Portaria entra em vigor a partir da data da sua publicação no Boletim de Serviço desta Universidade, revogando a PORTARIA UFF nº 68.506 de 20 de março de 2023.

FABIO BARBOZA PASSOS
Vice-Reitor no Exercício da Reitoria

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL FLUMINENSE

PORTARIA UFF Nº 68.595 de 22 de setembro de 2023

Retifica a PORTARIA UFF N° 68.593 de 21 de setembro de 2023, que altera a composição do Comitê de Governança Digital.

O VICE-REITOR NO EXERCÍCIO DA REITORIA DA UNIVERSIDADE FEDERAL FLUMINENSE, no uso de suas atribuições legais, estatutárias e regimentais,

CONSIDERANDO a necessidade de estabelecer políticas e diretrizes na área de Tecnologia da Informação e Comunicação (TIC) da Universidade Federal Fluminense,

RESOLVE:

Art 1º Retifica a Portaria UFF N° 68.593 de 21 de setembro de 2023, publicada no BS/UFF Nº 179, de 21/09/2023. Seção IV, págs. 086 a 087, que altera a composição do Comitê de Governança Digital, para deliberar sobre os assuntos relativos à implementação das ações de governo digital e ao uso de recursos de tecnologia da informação e comunicação.

Art.2º **Designar** para compor este Comitê os seguintes servidores:

- **Laura Antunes Maciel**, SIAPE Nº 1351804, Chefe de Gabinete;

- **José Walkimar de Mesquita Carneiro**, SIAPE Nº 311512, Pró-Reitoria de Graduação;

- **Mônica Maria Guimarães Savedra**, SIAPE Nº 1714538, Pró-Reitoria de Pesquisa, Pós-Graduação e Inovação;

- **Leila Gatti Sobreiro**, SIAPE Nº 1081962, Pró-Reitoria de Extensão;

- **Alessandra Siqueira Barreto**, SIAPE Nº 1463418, Pró-Reitoria de Assuntos Estudantis;

- **Ricardo Campanha Carrano**, SIAPE Nº 1768285, Superintendência de Tecnologia da Informação;

- **Thaiane Moreira de Oliveira**, SIAPE Nº 102427, Superintendência de Comunicação Social; e

- **Carla Siqueira da Silva**, SIAPE Nº 1098886, Encarregado do Tratamento de Dados Pessoais.

Art.3º Estas designações não correspondem à função gratificada.

Art. 4º Os demais itens da Portaria UFF N° 68.294 de 9 de julho de 2021, permanecem inalterados.

Esta Portaria entra em vigor na data de sua publicação no Boletim de Serviço desta Universidade.

FABIO BARBOZA PASSOS
Vice-Reitor no Exercício da Reitoria

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL FLUMINENSE

PORTARIA UFF Nº 68.476 de 12 de janeiro de 2023

Institui o Comitê de Governança de Dados e Privacidade-CGDP, na Universidade Federal Fluminense.

O REITOR da Universidade Federal Fluminense, no uso das suas atribuições legais, estatutárias e regimentais,

RESOLVE:

Art. 1º - Instituir, Comitê de Governança de Dados e Privacidade-CGDP, da UFF, com o objetivo de definir o direcionamento, o monitoramento, a supervisão e a avaliação das práticas da gestão, para garantir a proteção de dados e da privacidade no âmbito da Universidade Federal Fluminense, conforme disposto na Lei Geral de Proteção de Dados - LGPD e suas normativas.

Parágrafo único - O Comitê possui função técnica, tendo por escopo promover as boas práticas de gestão de dados e privacidade na UFF, potencializando as suas discussões estratégicas, por meio de recomendações fundamentadas, auxiliando no desempenho das funções legais e regulamentares dos órgaos administrativos.

Art. 2º - O Comitê de Governança de Dados e Privacidade terá a seguinte composição mínima:

I - o Encarregado da LGPD;

II - o Presidente do Comitê de Governança Digital;

III - o Coordenador da Comissão de Segurança da Informação;

IV - o Presidente da Comissão de Dados Abertos;

V - o Coordenador do Subcomitê de Gestão de Riscos.

§ 1º O Comitê será coordenado pelo Encarregado da LGPD.

§ 2º O Coordenador será substituído, em suas faltas e impedimentos, por um Vice-Coordenador, definido entre os componentes do Comitê.

§ 3º Os componentes do Comitê irão atuar em regime de cooperação, e vão definir, as respectivas diretrizes e competências para realização das atividades dentro dos objetivos estabelecidos nesta Portaria.

Art. 3º - O Comitê de Governança de Dados e Privacidade, possui as seguintes atribuições:

I - estabelecer de diretrizes, a partir das quais os desenvolvedores de tecnologia da informação, os administradores dos sistemas de informação, cada qual dentro de seu escopo de competência, realizem o monitoramento de dados pessoais e de fluxos das respectivas operações de tratamento e utilização;

II - definir do modelo de Inventário de Dados Pessoais da UFF, que será realizado por cada área de gestão;

III - orientar a análise de riscos e a elaboração do Relatório de Impacto à Proteção de Dados;

IV - propor ao CGIRC a elaboração das Politicas de Privacidade e de Proteção de Dados;

V - elaborar as bases para o tratamento e proteção de dados nos contratos, convênios e instrumentos congêneres, sites, aplicativos, dentre outros;

VI - análise de outros temas afetos ao acesso e à proteção de dados e privacidade.

Art. 4º - O Comitê é diretamente subordinado ao Reitor sem prejuízo de sua independência funcional.

Paragrafo Único - Compete ao Gabinete do Reitor, dar suporte administrativo operacional ao Comitê, no exercício de suas atribuições definidas nesta Portaria.

Art. 5º - São competências do Coordenador da CGDP;

I - Convocar as reuniões do Comitê;

II - Convidar, em nome do CGDP, eventuais participantes e/ ou convocar reuniões extraordinárias;

III - propor ao Reitor , como Controlador, ações para a melhoria da Governança de Dados e Privacidade, definidas pelo CGDP;

IV - propor ao Reitor, como Controlador, as adequações e revisões necessárias nos fluxos e processos da UFF, abragendo o mapeamento dos dados sobre o caminho que este percorre desde o momento em que é coletado até o término do tratamento, para o atendimento à legislação e recomendações dos órgãos de controle;

V - planejar a comunicação e iniciativas de capacitação e educação continuada sobre a LGPD para a comunidade interna e externa à UFF;

VI - monitorar a conformidade da aplicação daas políticas previstas no Art. 3º inc. IV.

§ 1º As atas das reuniões serão elaboradas por um servidor designado para esse fim.

§ 2º As atas aprovadas serão assinadas pelos membros do Comitê presentes na reunião e arquivadas em meio eletrônico.

§ 3º As ações do Comitê serão decididas por consenso na reunião.

Art. 6º - Mediante requisição do Encarregado LGPD, os dirigentes da UFF deverão encaminhar, no prazo assinalado, as informações eventualmente necessárias para atender as solicitações da ANPD.

Art. 7º - Compete aos Pró-Reitores e Superintendentes:

I - observar as recomendações e atender às requisições encaminhadas pelo Encarregado;

II - encaminhar ao Encarregado, no prazo assinalado:

a) informações solicitadas pela ANPD, nos termos do art. 29 da Lei Federal nº 13.709, 14 de agosto de 2018;

b) relatórios de diagnósticos e de impacto à proteção de dados pessoais, ou informações necessárias à sua elaboração;

III - assegurar que o Encarregado seja informado, de forma adequada e tempestiva, sobre:

a) existência de sistemas locais próprios, tratamento e o uso compartilhado de dados pessoais necessários à execução de políticas públicas previstas em normas legais e regulamentares ou respaldadas em contratos, convênios ou instrumentos congêneres;

b) a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares de dados pessoais.

Art. 8º - Esta Portaria entrará em vigor na data de sua publicação no Boletim de Serviço desta Universidade, revogadas as disposições em contrário.

ANTONIO CLAUDIO LUCAS DA NOBREGA
Reitor

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL FLUMINENSE
CONSELHO UNIVERSITÁRIO

RESOLUÇÃO CUV/UFF Nº 308, DE 06 DE MARÇO DE 2024

Dispõe sobre a Política de Segurança da Informação (PSI) da Universidade Federal Fluminense (UFF).

O CONSELHO UNIVERSITÁRIO DA UNIVERSIDADE FEDERAL FLUMINENSE, no uso de suas atribuições estatutárias e regimentais, e o que mais consta do Processo nº 23069.178579/2023-21,

R E S O L V E :

Art. 1º - **Aprovar** a Política de Segurança da Informação (PSI) da Universidade Federal Fluminense (UFF).

Art. 2º - A presente Resolução entrará em vigor na data da sua aprovação.

* * * *

Sala das Sessões, 06 de março de 2024.

FABIO BARBOZA PASSOS
Presidente
# # # # # #

Anexo I

Política de Segurança da Informação (PSI) da Universidade Federal Fluminense.

Capítulo I Disposições Preliminares

Art.1º A Política de Segurança da Informação (PSI) tem como objetivo estabelecer mecanismos e controles para garantir a efetiva proteção dos dados, informações e conhecimentos gerados, redução dos riscos de ocorrência de perdas, alterações e acessos indevidos, preservando a produção intelectual, disponibilidade, integridade, confiabilidade e autenticidade das informações, na UFF.

Art. 2º A administração e gestão da segurança da informação em ambiente computacional da UFF ficarão a cargo da Superintendência de Tecnologia da Informação – STI da UFF.

Art. 3º A Superintendência de Tecnologia da Informação (STI) será a responsável pelas normas e procedimentos institucionais que se façam necessários para a garantia da Segurança e mitigação de riscos ao ambiente de Tecnologia da Informação – TI da UFF.

Art. 4º Esta PSI se aplica a toda a comunidade acadêmica da UFF e seus órgãos, nos diversos níveis hierárquicos e vínculos – membros, servidores e demais agentes públicos ou particulares que, oficialmente,executem atividades vinculadas à atuação institucional da UFF – que, a qualquer momento, tenham necessidade de utilizar os recursos de TI.

Art. 5º A Superintendência de Tecnologia da Informação (STI) e o Comitê de Segurança da Informação (CSI), deverão manter uma lista de responsabilidades pelas aprovações dos variados tipos de liberações deacesso.

Art. 6º A Superintendência de Tecnologia da Informação será responsável pela edição e aplicação dos planos de gerenciamento e resposta a incidentes de segurança da informação em ambientes computacionais da UFF, devendo os mesmos ser suportados por política, norma ou procedimento específicos para tal.

Parágrafo único. Todos os servidores e demais colaboradores que tratem de gerenciamento de sistemas, acesso à informação e atividades relacionadas à segurança da informação são co-responsáveis pela execução dos planos, políticas e procedimentos de segurança da informação, bem como por mitigar incidentes de segurança da informação e agir com celeridade para notificação e resolução dos mesmos.

Art. 7º Os servidores deverão ser capacitados para o desenvolvimento de competências em privacidade e segurança da informação, com a devida comunicação aos níveis estratégico, tático e operacional da UFF.

Capítulo II
Das Definições e Categorizações

Art. 8º As redes, compostas pelos seus ambientes, salas de equipamentos, e demais ativos, serão categorizadas conforme sua criticidade quanto à segurança da informação, para que sejam aplicadas as políticas descritas conforme a criticidade. Os níveis sugeridos são

1. Redes em ambientes públicos (alunos, salas de aula, espaços comuns, espaços de convivência, etc.)
2. Redes em ambientes com dados sensíveis (laboratório com pesquisas sensíveis, setores administrativos,secretarias acadêmicas, etc.)
3. Redes em ambientes com controle compartilhado (por projeto acadêmico ou institucional)
4. Redes em ambientes dos sistemas críticos (núcleo de servidores e virtualização)

Art. 9º Para efeito desta política, considera-se:

Ambiente computacional da UFF: inclui todos os recursos computacionais da UFF e recursos computacionais de usuários que, de alguma maneira, estejam utilizando a infraestrutura da rede da UFF;

Ambiente de Produção: ambiente que possui os dados reais dos sistemas, aqueles que os usuários utilizam para as funções diárias e cujas informações possuem valores legais e são aproveitadas pela instituição; porpossuir dados reais, é considerado ambiente extremamente crítico para a segurança das informações da instituição e, por isso, seu acesso deve ser limitado e somente liberado a quem realmente possui necessidadede utilizá-lo em tarefas do dia-a-dia e de alimentação de dados e informações para o sistema.

Ambiente de Homologação: ambiente no qual são feitos os testes em sistemas por um grupo restrito de usuários com acesso para validação de funções de um novo sistema ou de novas funções para um sistema preexistente; possui cópias desatualizadas dos dados de produção; por possuir dados reais, mesmo que desatualizados, existe razoável criticidade quanto ao comprometimento da segurança das informações institucionais.

Ambiente de Desenvolvimento: é o ambiente no qual os desenvolvedores de sistemas possuem acesso para criar um novo sistema ou novas funções para um sistema preexistente; obrigatoriamente possui esquemas reais (tabelas, campos em tabelas, com formatos e valores), porém, preenchidos com dados falsos; não compromete a segurança das informações da instituição.

Área Normativa: área da instituição que é responsável pelas informações contidas em um sistema; o usuárionormativo deve obrigatoriamente pertencer à área normativa.

Comunidade acadêmica: nesta política, considera-se como o conjunto de pessoas formado pelos alunos, ex-alunos, professores, técnico-administrativos e demais funcionários a serviço da instituição, bem como usuários dos serviços administrativos e acadêmicos da universidade e/ou dos recursos de informação e ambiente computacional.

Continuidade de negócios: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, a fim de manter suas operações em um nível aceitável, previamente definido. (PORTARIA GSI/PR nº 93/2021)

Incidente de segurança da informação: um ou múltiplos eventos de segurança da informação relacionados e identificados que podem prejudicar os ativos da organização ou comprometer suas operações. [FONTE:ISO/IEC 27035-1:2016, 3.4]

Perfil de acesso: conjunto de regras e privilégios de computação que liberam apenas determinadas operações em um sistema; é o perfil de acesso que determina as permissões de um usuário, ou seja, o que ele pode ou não fazer em um sistema.

Recursos computacionais da UFF: todos os ativos, incluindo sistemas, serviços e infraestrutura de TI,

independentemente de terem sido adquiridos pela instituição; uma vez integrantes de algum ambiente computacional, estão sujeitos a esta PSI.

Segurança da Informação: preservação da confidencialidade, integridade e disponibilidade da informação.[FONTE: ISO 27000:2020]

Sistema de informação: conjunto de aplicações, serviços, ativos (3.1.2) de tecnologia da informação ou outros componentes de manuseio de informações. [FONTE: ISO/IEC 27000:2018, 3.35]

Usuário: qualquer pessoa, com ou sem conhecimento especializado, que utilize os recursos computacionais e/ou o ambiente computacional da UFF.

Usuário Normativo: usuário de área, ou seja, não é necessariamente um analista de TI, que possui conhecimento profundo da área operacional e recebe conhecimento acerca dos perfis de usuário de um determinado sistema; é ele o responsável por aprovar a liberação de acesso de um determinado perfil de acesso a um determinado usuário; ou seja, é ele o responsável por afirmar que as funções de um determinadousuário são compatíveis com o perfil a ser liberado para o mesmo.

Capítulo III
Das Diretrizes Gerais

Art. 10º A segurança da informação é responsabilidade de qualquer usuário, não apenas da área de TI; destaforma, deverá refletir em hábitos, atitudes, responsabilidade e cuidados constantes no momento do uso, solicitação de aprovação de recursos etc.

Art. 11º O CSI irá propor projetos e ações para orientar e conscientizar os usuários quanto aos preceitos desegurança da informação a serem observados por todos, inclusive nas divisões, órgãos e campi da UFF quepossuem ambiente de TI distinto, com maior ou menor integração com o restante da instituição.

Art. 12º A utilização de informações e recursos computacionais deve ser sempre compatível com a ética, confidencialidade, legalidade e finalidade das atividades desempenhadas pelo usuário.

Art. 13º A utilização de recursos (ativos) disponibilizados pela instituição, ou integrados ao ambiente computacional, deve ser feita segundo os padrões e procedimentos definidos pela STI, através dos canais oficiais da STI, visando manter a disponibilidade e o desempenho das aplicações.

Art. 14º A utilização indevida dos recursos computacionais ou violação desta PSI será investigada e analisada pelas áreas competentes quanto a sua criticidade, e poderá provocar a suspensão temporária dos acessos, e deverá ser notificada à STI e à chefia imediata ou instância superior.

Art. 15º A UFF deverá manter um Plano de Gestão de Riscos com base na legislação vigente, que contemplea privacidade e a segurança da informação, as ameaças mais prováveis e suas ocorrências, a classificação dos riscos e medidas para tratamento.

Art. 16º A STI deverá manter um Plano de Contingência que permita operar os sistemas e recursos de forma que garanta um nível mínimo de disponibilidade de operação e deverá passar por revisões conforme necessidades técnicas.

Art. 17º A informação, documentação e produção técnica e acadêmica desenvolvidas e/ou inseridas nos

sistemas em uso na UFF são para uso exclusivo da Universidade para administração, gestão, prestação de serviços, ensino, pesquisa e extensão, sendo propriedade intelectual da Universidade e compartilhadas apenas com o Governo Federal, nos termos da lei.

Art. 18º A documentação dos sistemas de informação e projetos desenvolvidos devem ser disponibilizadasem meios de informação não perecíveis a longo prazo, no mínimo enquanto os sistemas estiverem em operação.

Art. 19º Os sistemas de informação e automação desenvolvidos, implementados ou integrados por terceiros deverão contemplar em seus contratos as cláusulas de proteção de dados e segurança da informação previstas em lei.

Art. 20º Todos os gestores de unidades deverão manter à disposição de suas equipes planos de contingênciaatualizados para os casos de queda de energia, inconformidades de acesso, de interrupção dos sistemas de informação e serviços de forma a não vulnerabilizar a segurança da informação.

Art. 21º Compete à alta administração, aos órgãos, departamentos, Comitês e Comissões delegadas monitorar o desempenho e avaliar a concepção, a implementação e os resultados da sua política de segurança da informação e das normas internas de segurança da informação;

Capítulo IV
Do acesso, classificação e tratamento das informações e proteção de dados

Art. 22º O acesso às informações institucionais deverá ser garantido ao usuário solicitante, nos termos da Lei geral de acesso à informação, desde que não infrinja o direito à privacidade, segurança pública, segurança institucional e legislações vigentes, sem que haja concessão de acesso aos sistemas em que a informação solicitada está registrada ou aos bancos de dados institucionais e desde que seja solicitado oficialmente, de acordo com os procedimentos para a prestação deste serviço e na forma da lei.

Art. 23º As informações classificadas como Reservada; Secreta e Ultrassecreta cumprirão os prazos de restrição de acesso previsto em lei, bem como aquelas as sigilosas por força de lei ou de contrato, as que requerem alto grau de controle e proteção contra acessos não autorizados, em segredo de justiça e hipótesesde segredo industrial decorrentes da exploração direta de atividade econômica pelo Estado ou por pessoa física ou entidade privada que tenha qualquer vínculo com o poder público.

PARÁGRAFO ÚNICO. É responsabilidade do produtor da informação, documento ou sistema providenciar a classificação das informações sensíveis e sigilosas e outras providências para garantir a restrição do acesso.

Art. 24º Todo e qualquer dado pessoal terá garantia de proteção e acesso restrito nos termos da lei, sendo acessível exclusivamente para as finalidades administrativas e acadêmicas da UFF.

Capítulo V
Da gestão da Segurança das Informações e suas responsabilidades

Art. 25º A responsabilidade pela gestão da segurança da informação é atribuída aos agentes envolvidos noprocesso de criação, salvaguarda, transporte e destruição da informação, sendo assim caracterizados:

I) Normativos: responsáveis pela classificação da informação, pela definição de perfil do usuário e o tipo de acesso às informações;

II) Usuários: todos aqueles que utilizam os recursos de tecnologia da informação, sendo, portanto, responsáveis pelo conhecimento e aplicação desta PSI;

III) Custodiante: responsável pela guarda da informação com segurança; na UFF e nos seus campi, esse agente é a Superintendência de Tecnologia da Informação, que terá a incumbência de implementar e controlar as autorizações de acesso à rede, correio/e-mail, internet, sistemas, servidores etc.; monitorar o uso adequado dos recursos liberados, bem como implementar e operacionalizar os mecanismos de segurança da informação.

Art. 26º Os usuários normativos de sistemas que não sejam da competência e expertise da atuação da STI,serão designados pela chefia de primeiro nível das áreas usuárias ou Comissões e Comitês instituídos pelo reitor e áreas legalmente responsáveis pelo sistema.

Art. 27º Os gestores das unidades organizacionais da UFF são usuários normativos das informações pertencentes ao domínio de sua autoridade, e podem delegar as funções de concessão de direitos de acesso/homologação de alterações nos sistemas; para tanto, devem formalizar estas delegações junto à Superintendência de Tecnologia da Informação.

Art. 28º É responsabilidade da área produtora da informação o monitoramento de obsolescência e providências para mudança de suporte, garantia de acesso, salvaguarda e preservação da informação, até orecolhimento para o arquivo permanente.

Capítulo VI
Das Vedações E Responsabilidades

Art.29º É vedada aos usuários a saída ou entrada de recursos computacionais institucionais de um setor sem prévia autorização do gestor responsável de cada unidade envolvida; apenas a STI possui autorização paramovimentação livre dos recursos computacionais institucionais.

Art. 30º É vedado o pernoite de recursos computacionais institucionais em veículos oficiais fora dos *campi* da Universidade ou em veículos privados de qualquer natureza, exceto quando autorizado por gestor competente.

Art. 31º É vedada a retirada de recursos computacionais de armazenamento de dados ou a mobilização dosmesmos sem autorização prévia dos gestores da STI responsáveis pela área.

Art.32º É responsabilidade do portador dos recursos computacionais autorizado a movimentá-los a garantia de proteção contra roubos, furtos e acesso indevido às informações e senhas porventura disponíveis no dispositivo.

Capítulo VII Ambientes Públicos

Art. 33º É permitido exclusivamente o uso de softwares licenciados nos equipamentos, dispositivos ou sistemas que estejam conectados e/ou em uso para quaisquer funcionalidades a serviço da instituição.

Art. 34º Equipamentos e sistemas com senha padrão, que vem junto com o produto, deve ser obrigatoriamente modificada pelo usuário antes da disponibilização do equipamento, sistema e/ou ambiente.

Art. 35º Todas as senhas são pessoais e intransferíveis.

Art. 36º A Superintendência de Tecnologia da Informação definirá e adotará um padrão de identificação de usuários que permitirá associar, de maneira única, cada direito de acesso à pessoa que o detém e concederá direitos de acesso compatíveis com as funções desempenhadas pelos usuários, através de perfis de acesso diferenciados; tais perfis objetivam restringir os dados e operações disponíveis, e sua definição será realizada em conjunto com Usuários Normativos.

Art. 37º A aquisição e instalação de equipamentos de rede devem obrigatoriamente atender às especificações técnicas definidas e publicadas pela STI.
Parágrafo único: Quando o equipamento pretendido não estiver previsto ou com suas especificações técnicas definidas pela STI, uma consulta formal prévia deve ser efetuada.

Art. 38º Equipamentos que necessitem ser conectados na rede UFF, exceto computadores, impressoras, scanners e similares, deverão ser registrados na STI, em especial switches e roteadores. A ausência do registro poderá culminar no bloqueio automático do acesso à rede pelo equipamento, sem aviso prévio.

Capítulo VII Ambientes Sensíveis

Art. 39º Todas as regras anteriores se aplicam a este ambiente.

Art. 40º É proibida a desinstalação, sem autorização formal dos órgãos responsáveis, de softwares ou hardwares que estejam sendo utilizadas para realizar controle físico e lógico dos recursos disponíveis; caso isso ocorra, o fato será comunicado, imediatamente, à chefia imediata do usuário ou ao Coordenador de curso do aluno e à STI, que irá apurar as causas, corrigirá o problema e providenciará a reinstalação.

Art. 41º A aquisição e instalação de softwares devem ser obrigatoriamente autorizadas pela STI.

Capítulo IX Ambientes compartilhados

Art. 42º Todas as regras anteriores se aplicam a este ambiente.

Art. 43º A STI, em parceria com o gestor do ambiente compartilhado, irá restringir as pessoas que poderãoser administradoras das respectivas estações de trabalho.

Capítulo X
Da Segurança Física de Ambientes Computacionais de Nível Crítico de TI

Art. 44º Todas as regras anteriores se aplicam a este ambiente.

Art. 45º Toda movimentação de equipamentos que compõem a estrutura de ambientes computacionais de nível crítico da UFF deve ser devidamente autorizada pela STI.

Art. 46º A UFF manterá dispositivos de proteção contra problemas de segurança física (condições ambientais adversas, desastres naturais, incêndios etc.) e lógica (vírus, acesso não autorizado, invasões etc.)compatíveis com os requisitos definidos nesta política; cabe à STI a definição de tais dispositivos de proteção, considerando características regionais, a criticidade das informações e os recursos tecnológicos envolvidos; nenhum fluxo de informações poderá existir sem que passe pelas camadas de proteção lógica.

Art. 47º Será utilizado hardware que disponha de recursos de redundância de processador, disco, energia etc., bem como equipamentos de prevenção e combate a incêndios (SPCI), além de controle da energia elétrica (rede estabilizada), temperatura e umidade.

Art. 48º O acesso físico aos Ambientes Computacionais de Nível Crítico de TI será restrito a pessoas oficialmente autorizadas.

Capítulo XI
Da Segurança Lógica de Ambientes Críticos de TI

Art. 49º Cabe à Superintendência de Tecnologia da Informação garantir que todos os ambientes lógicos (sistemas operacionais, SGDBs e sistemas de informação) tenham o seu acesso restrito por senhas, estandoem conformidade com as diretrizes descritas nesta Política.

Art. 50º Todo programa ou transação desenvolvido ou adquirido para execução em ambientes computacionais de nível crítico da UFF deve, obrigatoriamente, conter as verificações de autorização de execução em perfeita sintonia com o ambiente tecnológico em que será processado; não haverá exceção à verificação de autorização para execução de qualquer programa ou transação; em princípio, tudo que não for explicitamente permitido, está negado.

Art. 51º Todo novo programa ou transação adquirido para execução em ambientes computacionais de nível crítico da UFF deverá ser submetido à análise da Superintendência de Tecnologia da Informação com a finalidade de verificar sua conformidade.

Art. 52º Nenhuma senha será gravada no código-fonte de programas em texto plano, ou em arquivos ou tabelas destinadas a outros fins, devendo o tratamento desse tipo de informação seguir norma específica daSuperintendência de Tecnologia da Informação.

Art. 53º O acesso – mesmo que de simples consulta – aos arquivos ou tabelas de senha não será permitido,em nenhuma circunstância, a nenhum colaborador; tal restrição será provida por mecanismos de segurançalógica ou criptografia.

Art. 54º Toda conta de acesso a ambientes computacionais de nível crítico sem uso há mais de 60 dias até o limite de 180 dias poderá ser desabilitada pela Superintendência de Tecnologia da Informação, sem prévia autorização do proprietário ou da gerência para isso, de modo a liberar recursos físicos e/ou licenças de softwares alocados.

Art. 55º Somente será permitido o uso de recursos homologados e autorizados pela STI, desde que sejam identificados individualmente, inventariados, com documentação atualizada e atendendo a legislação pertinente em vigor.

Art. 56º A homologação de recursos computacionais em ambientes de nível crítico será de única e exclusivacompetência da STI, sendo regida por normas e procedimentos específicos de Homologação de Software eHomologação de Hardware.

Art. 57º É recomendada a existência de planos de segurança e de infraestrutura para implantação de sistemas de informação.

Art. 58º Não serão implementados sistemas de informação em ambientes computacionais de nível crítico quando trouxerem fragilidades que comprometam a segurança do ambiente UFF.

Art. 59º As senhas de acesso aos sistemas são de uso pessoal e intransferível;

Art. 60º Qualquer tentativa de acesso a sistemas cujo acesso lhe é negado, serão notificadas à chefia imediata do usuário.

Art. 61º É dever de todos zelar pelo sigilo de suas senhas de autenticação, bem como escolher senhas fortesdificultando serem descobertas facilmente por outra pessoa.

Art. 62º A conta de acesso e a senha de acesso para cada pessoa será única, individual e intransferível, sendo reconhecidas como equivalentes à sua assinatura e representam o nível de delegação concedida parao desempenho de suas funções.

Art. 63º Os acessos externos a recursos de ambiente de nível crítico da instituição somente serão concedidos mediante autorização prévia dos gestores responsáveis da STI, segundo instruções detalhadas caso a casoe realizados por intermédio de soluções técnicas institucionais.

Art. 64º O acesso à internet é permitido por intermédio de sistema de segurança institucional; é proibido o acesso direto à internet por intermédio de provedores externos estando conectado à rede UFF.

Art. 65º A Superintendência de Tecnologia da Informação deve assegurar que nenhum colaborador ou prestador de serviço obtenha direitos de acesso a recursos em ambientes de nível crítico, incompatíveis com a sua função, onde cada usuário terá uma única conta de acesso por aplicação, com permissões necessáriasapenas à execução de suas atividades.

Art. 66º Os colaboradores externos à UFF, mesmo não existindo vínculo direto, também poderão ser cadastrados nos sistemas, associados a um servidor responsável e também controlados por data de vigênciade acordo com a permanência na função.

Capítulo X
Da Segregação de Ambientes de desenvolvimento e suas Funções

Art. 67º A STI deve assegurar que todos os sistemas de informação da Instituição sejam aderentes às diretrizes a seguir:

I) Segregação de ambientes lógicos, com acessos únicos e isolados, de maneira que o ambiente de produçãofique apartado dos demais.

II) Os ambientes de teste, de homologação, de desenvolvimento e outros com funções similares, devem terseus códigos e dados (banco de dados) com acesso exclusivo dos usuários envolvidos com atividades de desenvolvimento e suporte a sistemas;

III) Estes usuários poderão realizar operações de consulta nos ambientes de produção, conforme necessidade e a critério da STI.

IV) O acesso às bases de dados dos ambientes de produção será feito, unicamente, através dos sistemas deinformação, estando completamente vetado qualquer tipo de acesso direto; os casos extremos de necessidade de liberação serão aprovados pela STI em conjunto com o usuário com nível gerencial da áreasolicitante.

V) Todo objeto, tais como programas, telas, funções etc., que for transferido para o ambiente de produção, deverá ser originado do ambiente de desenvolvimento ou de homologação, mantendo nesses ambientes o arquivo fonte original.

VI) Deve existir nos ambientes de produção, sempre que tecnologicamente possível, um controle automático das versões dos programas-fonte; este controle possibilitará a recuperação de versões anteriores,assim como a identificação do responsável pela sua implantação; o acesso aos programas-fonte, principalmente para inclusão, exclusão e alteração nos seus códigos, será restrito, através de perfis de acessoespecíficos e registrado em trilhas de auditoria.

Capítulo XI
Da política de backup e continuidade de negócios

Art. 68º A política de cópia de segurança e restauração de dados e sistemas será definida pela Superintendência de Tecnologia da Informação em documento específico, disponibilizado ao público apósaprovação oficial, bem como as normativas e regulamentações das atividades relacionadas;

Art. 69º As áreas normativas dos sistemas manterão cópias de segurança dos dados e sistemas de acordo com a política específica por tema acordada sobre backup.

Art. 70º Os backups de dados e sistemas devem ser realizados com nível de segurança física e lógica compatíveis com a criticidade e importância do conteúdo, atendendo aos requisitos legais

Art. 71º A STI é responsável por regulamentar os procedimentos para cópia de segurança e restauração dedados e sistemas e outros procedimentos de backup de dados nas redes em ambientes dos sistemas críticos.

Art. 72º Nos demais ambientes, a área normativa deverá providenciar responsáveis para a execução, acompanhamento e manutenção dos procedimentos de backup e restauração de dados e sistemas, de acordocom o art. 68°.

Art.73º A alta disponibilidade de acesso deve ser promovida por redundância adicional para conectividadede rede, obtida por meio de múltiplas rotas, passando por diferentes meios físicos.

Capítulo XII
Das Auditorias e Trilhas de Auditoria

Art. 74º Os órgãos oficiais de controle interno e externo poderão ter acesso a qualquer informação que esteja armazenada em ambiente lógico (Sistemas Operacionais, SGDBs e Sistemas de Informações)

Art. 75º Havendo evidência de qualquer atividade que possa comprometer a segurança do ambiente de TI, a UFF poderá auditar e monitorar as atividades de qualquer usuário, além de inspecionar seus arquivos e registros de acesso, sempre que julgar e comprovar necessidade.

Art. 76º A STI deve providenciar os recursos tecnológicos de seus sistemas e exigir recursos para que os sistemas de terceiros mantenham trilhas de auditoria sempre disponíveis para uso, bem como definir o tempo de retenção e as informações que deverão sistematicamente e automaticamente compor os

arquivosconhecidos como trilhas de auditoria.

Art. 77º As trilhas de auditoria de um determinado sistema devem ser de fácil acesso e, sempre que possível,centralizadas.

Art. 78º As trilhas de auditoria devem ser obrigatórias e registrar automaticamente todas as operações críticas efetuadas, sendo constituídas de, pelo menos, os seguintes campos:

I) Identificador do usuário (nominal, não podendo ser somente IP ou MAC Address),
II) Data da operação,
III) Horário da operação,
IV) Operação realizada,
V) Quando pertinente, quais dados foram modificados.

Art. 79º As trilhas de auditoria devem estar disponíveis para consulta por um prazo mínimo estipulado na legislação vigente.

Art. 80º As trilhas de auditoria não podem ser, em hipótese alguma, alteradas manualmente; as únicas inclusões de dados admissíveis serão as oriundas das rotinas automáticas de registro.

Capítulo XIII Referências Normativas

Art. 81º Esta PSI está alinhada aos instrumentos normativos apresentados a seguir:

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:2022.** Segurança da informação, segurança cibernética e proteção à privacidade. Sistemas de gestão da segurança da informação. Requisitos. ABNT: Rio de Janeiro, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:2022.** Segurança da informação, segurança cibernética e proteção à privacidade. Controles de segurança da informação. ABNT:Rio de Janeiro, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27005:2023**. Segurança da informação, segurança cibernética e proteção à privacidade. Orientações para gestão de riscos de segurançada informação. ABNT: Rio de Janeiro, 2023.

BRASIL. Casa Civil. Instituto Nacional de Tecnologia da Informação. **Instrução Normativa n. 07**, de 29de maio de 2020. Altera o tempo de armazenamento dos logs, trilhas de auditorias e imagens. Disponível em: https://www.gov.br/iti/pt-br/assuntos/legislacao/instrucoes-normativas/sei_iti_-_0427993_-_instrucao_normativa_07_2020.pdf Acesso em: 28 jun. 2023.

BRASIL. **Decreto n. 9.637**, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm Acesso em: 26 jun. 2023. BRASIL. **Decreto 7.845,** de 14 de novembro de 2012. Regulamenta procedimentos para credenciamentode segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleode Segurança e Credenciamento.

BRASIL. **Lei n. 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponívelem: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 31 maio 2023.

BRASIL. **Lei 9.609,** de 19 de fevereiro de 1998. Dispõe sobre a propriedade intelectual de programa de computador, sua comercialização no país e dá providências.

BRASIL. Gabinete de Segurança Institucional. **Instrução Normativa GSI/PR n. 01** de 27 de maio de 2020. Dispõe sobre a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

BRASIL. Gabinete de Segurança Institucional. **Portaria GSI/PR n. 93**, de 18 de outubro de 2021. Aprovao glossário de segurança da informação. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370> Acesso em: 13 set. 2023

BRASIL. Gabinete de Segurança Institucional. **Portaria GSI/PR n. 120**, de 21 de dezembro de 2022. Aprova o Plano de Gestão de Incidentes Cibernéticos para a administração pública federal. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-120-de-21-de-dezembro-de-2022-452767918 Acesso em: 13 set. 2023

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos/Secretaria de Governo Digital. **Portaria SGD/MGI nº 852**, de 28 de março de 2023. Dispõe sobre o Programa de Privacidade e Segurança da Informação (PPSI). Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023- 473750908 Acesso em: 29 jun. 2023.

BRASIL. Programa do Governo Eletrônico Brasileiro. **Padrões de Interoperabilidade do Governo Eletrônico**: e-Ping, versão 2018. Disponível em: https://eping.governoeletronico.gov.br/ Acesso em: 05 jul. 2023.

BRASIL. Secretaria de Logística e Tecnologia da Informação. **Portaria Normativa SLTI/MP n. 05**, de 14 de julho de 2005. Institucionaliza os Padrões de Interoperabilidade do Governo Eletrônico – e-Ping.

[NBR] BRITISH STANDARD. **ISO/IEC 27000:2020**. Information technology – Security techniques – Information security management systems – Overview and vocabulary. Brussels: BS, 2020.

CGDP - LGPD - Tratamento de dados na UFF

Formulário de levantamento sobre o tratamento de dados na UFF.

O Comitê de Governança de Dados e Privacidade, instituído pela Portaria 68.476, de 12 de janeiro de 2023, com objetivo de promover as boas práticas de gestão de dados e privacidade na UFF, aplica um novo formulário para identificar o índice de maturidade da instituição sobre o tratamento de dados pessoais na Universidade.

A Universidade Federal Fluminense já havia aplicado um formulário anterior elaborado pelo GT LGPD constituído para estabelecer, no âmbito da Universidade, os procedimentos para cumprimento da Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709, de 14 de agosto de 2018, alterada pela Lei nº 13.853, de 8 de julho de 2019, que agora passou por revisão e novos enfoques.

O objetivo da aplicação do formulário é auxiliar o direcionamento, o monitoramento, a supervisão e as práticas de gestão, mapeando o nível de maturidade no tratamento de dados por setores da UFF, identificando elementos da coleta, da trajetória e das formas de tratamento dos mesmos no âmbito dos serviços prestados pela Universidade, passando pelos tipos de dados, documentos e registros mantidos pela instituição.

Os dados pessoais dos respondentes não serão divulgados. Os resultados do levantamento serão utilizados exclusivamente para fins de cumprimento da Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709, de 14 de agosto de 2018, alterada pela Lei nº 13.853, de 8 de julho de 2019.

Este formulário aceitará respostas até o dia 14 de julho de 2023.

Agradecemos desde já a sua colaboração.

* Indica uma pergunta obrigatória

1. 1. e-mail *

IDENTIFICAÇÃO DO SETOR E DO RESPONDENTE

2. 2. Selecione o tipo de órgão a que se vincula o setor *

Marcar apenas uma oval.

- ◯ Unidade Acadêmica
- ◯ Pró-Reitoria
- ◯ Superintendência
- ◯ Gabinete do Reitor

3. 3. Nome do órgão máximo a que seu setor está vinculado *

_____

4. 4. Nome do setor *

_____

5. 5. Sigla do setor *

_____

6. 6. E-mail institucional do setor *

_____

7. 7. Nome do responsável pelo setor *

_____

8. 8. E-mail institucional do responsável pelo setor *

_____

9. 9. Nome do respondente *

_____

10. 10. E-mail institucional do respondente *

_____

11. Você conhece a Lei Geral de Proteção de Dados (LGPD)

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.

11. Marcar apenas uma opção

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

12. Você tem conhecimento de que a UFF possui uma página sobre a Lei Geral de Proteção de Dados (LGPD)?

https://www.uff.br/?q=lgpd

12. Marcar apenas uma opção

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

13. Você tomou conhecimento das campanhas institucionais sobre a Lei Geral de Proteção de Dados (LGPD) realizadas na Universidade Federal Fluminense (página da UFF, Comunica UFF, Minuto de Gestão de Pessoas) com as matérias enviadas por e-mail id.uff dos servidores?

13. Marcar apenas uma opção

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

14. Considera que as campanhas institucionais sobre a Lei Geral de Proteção de Dados (LGPD) realizadas pela Universidade Federal Fluminense tenham atingido o objetivo de esclarecer, dar recomendações e incentivar a capacitação do servidores da Universidade sobre o tema?

14. Marcar apenas uma opção

Marcar apenas uma oval.

- Sim
- Não

15. Você já fez algum dos cursos indicados pela Equipe de Capacitação da Escola de Governança em Gestão Pública como treinamento ou capacitação sobre Lei Geral de Proteção de Dados (LGPD)?

15. Marcar apenas uma opção

Marcar apenas uma oval.

- Sim
- Não

16. Você já realizou algum curso de capacitação sobre a Lei Geral de Proteção de Dados (LGPD)?

16. Marcar apenas uma opção

Marcar apenas uma oval.

- Sim
- Não

17. Você sabe quem é considerado pela legislação (Lei Geral de Proteção de Dados - LGPD) como titular de dados pessoais?

17. Marcar apenas uma opção

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

A LGPD NO DESEMPENHO DE SUAS ATIVIDADES NO SETOR DE TRABALHO

18. 18. Selecione os PRINCIPAIS setores/ segmentos com os quais o setor se relaciona *

Marque todas que se aplicam.

- ☐ Pró-Reitorias e Superintendências da UFF
- ☐ Coordenações de Cursos de Graduação
- ☐ Coordenações de Curso de Pós-Graduação
- ☐ Departamentos de Ensino
- ☐ Direções de Unidades Acadêmicas
- ☐ Estudantes dos Cursos de Graduação
- ☐ Estudantes dos Cursos de Pós-Graduação
- ☐ Docentes da UFF em geral
- ☐ Técnicos da UFF em geral
- ☐ Público externo à UFF
- ☐ Outras IES
- ☐ Outras Instituições

TRATAMENTO DE DADOS PESSOAIS PELO SETOR

Para fins deste levantamento e da aplicação da LGPD, considera-se tratamento de dados qualquer operação realizada com dados pessoais, tais como: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle de informação, modificação, comunicação, transferência, difusão ou extração.

DADOS PESSOAIS:
São quaisquer informações relacionadas a pessoa natural identificada ou identificável. São exemplos de dados pessoais: nome, endereço, e-mail, CPF, dados de localização (função de dados de localização em telefones ou GPS), endereço de IP (protocolo de internet, testemunhos de conexão (cookies), etc.

DADOS SENSÍVEIS:
São aqueles que, se expostos ou compartilhados, podem causar impacto para vida pessoal e/ou profissional.
São exemplos de dados sensíveis: dados pessoais sobre origem racial, convicção religiosa, opinião política, filiação a sindicato ou 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.

19. 19. Você aplica os entendimentos e diretrizes presentes na LGPD em seu ambiente de trabalho? *

Marcar apenas uma oval.

- Sim
- Não
- Não sei

20. O setor realiza coleta de dados pessoais e/ou dados sensíveis em qualquer etapa da sua atividade no trabalho?

20. Marcar apenas uma opção

Marcar apenas uma oval.

- Sim
- Não
- Não sei

21. Selecione os conjuntos de dados coletados ou tratados pelo setor

Observar as definições contidas na introdução da ação

21. Marcar todas as opções que se aplicam:

Marque todas que se aplicam.

- [ ] Dados pessoais de estudantes de graduação
- [ ] Dados pessoais de pessoal técnico-administrativo de graduação
- [ ] Dados pessoais de pessoal docente
- [ ] Dados sensíveis de estudantes de graduação
- [ ] Dados sensíveis de pessoal técnico-administrativo
- [ ] Dados sensíveis de pessoal docente
- [ ] Dados pessoais de pessoas externas à UFF partícipes de contratos ou termos de convênio ou acordos de cooperação com a UFF
- [ ] Dados sensíveis de pessoas externas à UFF partícipes de contratos ou termos de convênio ou acordos de cooperação com a UFF

22. Quais são os dados pessoais coletados ou tratados no seu setor?

22. Marcar todas as opções que se aplicam:

Marque todas que se aplicam.

- [ ] Nome
- [ ] Documento de identificação - RG, CNH, CPF
- [ ] Telefone
- [ ] Endereço residencial
- [ ] Data e local de nascimento
- [ ] Retrato em fotografia
- [ ] Prontuário médico
- [ ] Cartão bancário - dados bancários
- [ ] Não sei
- [ ] Não se aplica

23. Quais são os dados sensíveis coletados ou tratados no seu setor?

23. Marcar todas as opções que se aplicam:

Marque todas que se aplicam.

- [ ] Origem racial ou étnica
- [ ] Convicção Religiosa
- [ ] Filiação Sindical
- [ ] Orientação sexual
- [ ] Dado genético ou biométrico
- [ ] Dado referente à saúde
- [ ] Não sei/ Não se aplica

24. O setor realiza coleta ou tratamento de outros dados não descritos nas duas perguntas imediatamente anteriores? Se sim, descreva os outros dados.

24. *

25. Qual é o PRINCIPAL meio de manutenção dos dados nos serviços prestados no seu setor?

25. Marcar apenas uma opção

Marque todas que se aplicam.

- [ ] Digital
- [ ] Papel

26. Os dados pessoais e sensíveis coletados ou tratados são mantidos em sistema institucional? Selecione os Sistemas e Bases de dados institucionais utilizados pelo setor.

Consulta em http://www.noticias.uff.br/bs/2019/02/032-19.pdf , páginas 65 e 66

26. Marcar todas as opções que se aplicam *

Marque todas que se aplicam.

- [ ] e-mail institucional - UFFMAIL e seus recursos
- [ ] Sistema Acadêmico - IdUFF
- [ ] Sistema Acadêmico - Administração Acadêmica
- [ ] Sistema Acadêmico - Inscrição
- [ ] Sistema Acadêmico - Quadro de horários
- [ ] Sistema Acadêmico - ENADE
- [ ] Sistema Acadêmico - Lançamento de notas
- [ ] Diploma Privado
- [ ] Monitoria
- [ ] Pergamum
- [ ] Sigadoc
- [ ] Periódicos
- [ ] RAD
- [ ] PIBIC
- [ ] Dspace - RIUFF
- [ ] CPD
- [ ] CPPD
- [ ] Bolsas - Assistência Estudantil
- [ ] SIA - Chefias
- [ ] SISAP
- [ ] Sispos - Gestão acadêmica
- [ ] Sispos - Alunos
- [ ] Sispos- Candidatura
- [ ] SisPPge
- [ ] SISPRO
- [ ] SISPTA
- [ ] SIA Compras
- [ ] SACI - Carteirinha
- [ ] SAI - Avaliação Institucional
- [ ] SCAB - Sistema de Controle de Bibliotecas
- [ ] SDCA - Controle de Acesso
- [ ] Sistema de processos - controle de processos administrativos
- [ ] Avaliação de desempenho
- [ ] Cálculo horas - cálculo de horas adicional e extra
- [ ] Capacitação
- [ ] Contracheque
- [ ] ex- servidor
- [ ] Ficha financeira
- [ ] Cadastro de pessoas?fita espelho UFF - Produção
- [ ] Frequência

- [ ] Incentivo a qualificação
- [ ] Perícia médica
- [ ] Consulta a contracheque SEI
- [ ] CKAN - Dados Abertos
- [ ] SEI
- [ ] SIORG
- [ ] Não sei/ Não se aplica
- [ ] Outro: _____

27. 27. O setor faz uso de outro sistema, base de dados ou plataforma não relacionada anteriormente? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não se aplica

28. 28. Caso tenha respondido SIM na pergunta anterior, informe a origem do sistema de dados ou plataforma utilizada e o link de acesso. Caso tenha respondido NÃO, escreva "não se aplica". *

_____

29. 29. Caso seja sistema, base de dados ou plataforma adquiridos por recurso próprio do setor, disponibilizar o link de aceso ao contrato e termo de uso. Caso não, escreva "não se aplica". *

_____

_____

_____

_____

_____

30. Na sua opinião é desnecessária a coleta de algum dado no seu setor?

30. Marcar apenas uma opção *

Marcar apenas uma oval.

- Sim
- Não
- Não sei

31. Quando há coleta de dados pessoais, você observa se há necessidade de coleta de todos os dados elencados no formulário de solicitação de sua unidade de trabalho para atendimento de uma solicitação?

31. Marcar apenas uma opção

Marcar apenas uma oval.

- Sim
- Não
- Não sei

32. Você tem conhecimento de que na coleta de dados deve ser solicitado somente o necessário para atingimento da finalidade?

32. Marcar apenas uma opção

Marcar apenas uma oval.

- Sim
- Não
- Não sei

33. Qual é o tipo de tratamento de dados é realizado pelo setor?

33. Marcar todas opções que se aplicam

Marque todas que se aplicam.

- [ ] Coleta: recolhimento de dados com finalidades específicas
- [ ] Produção: criação de bens e de serviços a partir do tratamento de dados
- [ ] Recepção: ato de receber os dados ao final da transmissão
- [ ] Classificação: maneira de ordenar os dados conforme algum critério estabelecido
- [ ] Utilização: ato ou efeito do aproveitamento dos dados
- [ ] Acesso: possibilidade de comunicar-se com um dispositivo, meio de armazenamento, unidade de rede, memória, registro, arquivo, etc., visando receber, fornecer, ou eliminar dados
- [ ] Reprodução: cópia de dado preexistente obtido por meio de qualquer processo
- [ ] Transmissão: movimentação de dados entre dois pontos por meio dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelértricos, pneumáticos, etc,s
- [ ] Distribuição: ato ou efeito de dispor de dados de acordo com algum critérios estabelecido
- [ ] Processamento: ato ou efeito de processar dados
- [ ] Arquivamento: ato ou efeito de manter registrado um dado, que já tenha perdido a validade ou sua vigência
- [ ] Armazenamento: ação ou resultado de manter ou conservar em repositório um dado vigente
- [ ] Comunicação: transmitir informações pertinentes a políticas de ação sobre os dados
- [ ] Eliminação: exclusão de dados ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado
- [ ] Avaliação: ato ou efeito de calcular valor sobre um ou mais dados
- [ ] Modificação: ato ou efeito de alteração de dado
- [ ] Transferência: mudança de dados de um área de armazenamento para outra, ou para terceiro
- [ ] Difusão: ato ou efeito de divulgação, propagação, multiplicação dos dados
- [ ] Extração: ato de copiar ou retirar dados do repositório em que se encontrava
- [ ] Não sei/Não se aplica

34. 34. Qual a finalidade principal do tratamento? *

35. Algum dado pessoal ou sensível é compartilhado?

35. Marcar apenas a opção

Marcar apenas uma oval.

- ◯ Não é compartilhado
- ◯ É compartilhado com outro setor da mesma unidade
- ◯ É compartilhado com outra unidade da UFF
- ◯ É compartilhado com qualquer terceiro que solicite
- ◯ É compartilhado com o público
- ◯ Outro: _____

36. O setor compartilha ou publica em página da internet de livre acesso dados pessoais fora do contexto das atividades do setor enquanto executor de política pública?

Por compartilhamento, entende-se: conceder acesso a banco de dados, enviar e-mails com dados pessoais para qualquer pessoa, tramitar documentos, físicos ou deixá-los acessíveis sem procedimentos de segurança

36. Marcar apenas uma opção *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não se aplica

37. 37. Caso tenha respondido SIM à pergunta anterior, descreva as situações em que isso ocorre e/ou a previsão legal para a sua ocorrência. *

_____

38. 38. Ainda em caso de resposta positiva àquela pergunta, informe se é solicitado ao TITULAR do DADO o consentimento explícito. *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não se aplica

39. São coletados dados pessoais de criança ou adolescente em qualquer etapa da sua atividade no trabalho?

39. Marcar apenas uma opção *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não se aplica

40. Os dados pessoais coletados da criança ou adolescente são autorizados pelos pais ou responsáveis?

40. Marcar apenas uma opção *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não se aplica

41. São coletados dados sensíveis da criança ou adolescente em qualquer etapa de sua atividade no trabalho?

41. Marcar apenas uma opção *

Marcar apenas uma oval.

- Sim
- Não
- Não se aplica

42. Os dados sensíveis coletados da criança ou adolescente são autorizados pelos pais ou responsáveis?

42. Marcar apenas uma opção *

Marcar apenas uma oval.

- Sim
- Não
- Não se aplica

TIPOS E CONJUNTOS DE DOCUMENTOS, DADOS E REGISTROS - administrativos, acadêmicos, científicos e de extensão

43. Selecione os conjuntos de TIPOS DE DOCUMENTOS ou REGISTROS ADMINISTRATIVOS tratados pelo setor em formato físico ou digital

43. Marcar todas as opções que se aplicam *

Marque todas que se aplicam.

- [ ] Apostila
- [ ] Ata
- [ ] Atestado
- [ ] Carta
- [ ] Certidão
- [ ] Convênio
- [ ] Decisão
- [ ] Declaração
- [ ] Determinação de Serviço
- [ ] Edital
- [ ] e-mail
- [ ] Fax
- [ ] Guia de remessa ou encaminhamento de correspondências, documentos, processos
- [ ] Instrução Normativa/Instrução de Serviço/Norma de Serviço
- [ ] Ofício/Memorando
- [ ] Parecer
- [ ] Portaria
- [ ] Portaria de Pessoal
- [ ] Processo
- [ ] Programas e Projetos
- [ ] Protocolo de Intenções
- [ ] Regimento
- [ ] Regulamento
- [ ] Relatório
- [ ] Requerimento
- [ ] Resolução
- [ ] Não aplica
- [ ] Outro: _____

44 - Selecione os conjuntos de DOCUMENTOS, DADOS ou REGISTROS ACADÊMICOS tratados pelo setor em formato físico ou digital

44. Marcar todas as opções que se aplicam *

Marque todas que se aplicam.

- [ ] Funcionamento dos cursos - Projeto pedagógico dos cursos
- [ ] Funcionamento dos cursos - Criação de cursos, Conversão de cursos.
- [ ] Funcionamento dos cursos - Autorização. Reconhecimento. Renovação de reconhecimento.
- [ ] Funcionamento dos cursos - Desativação de cursos. Extinção de cursos.
- [ ] Organização curricular - Estrutura do currículo (grade ou matriz curricular)
- [ ] Organização curricular - Reformulação curricular
- [ ] Organização curricular - Disciplinas: programas didáticos (conteúdos programáticos)
- [ ] Organização curricular - Oferta de disciplinas (quadro de horários, distribuição de carga horária docente)
- [ ] Organização curricular - Atividades complementares
- [ ] Planejamento de atividade - Calendário Acadêmico
- [ ] Colação de grau - Termo ou ata de colação de grau
- [ ] Ingresso - Processo de seleção principal
- [ ] Ingresso - Reingresso. Admissão de graduado. Portador de diploma. Obtenção de novo título
- [ ] Ingresso - Transferência voluntária ou facultativa
- [ ] Ingresso - Transferência ex officio
- [ ] Ingresso - Reopção de curso. Mudança de curso. Transferência interna.
- [ ] Ingresso - outras formas
- [ ] Registros Acadêmicos - Matrícula
- [ ] Registros Acadêmicos - Inscrição em disciplinas
- [ ] Registros Acadêmicos - Dispensa de disciplinas. Aproveitamento de estudos.
- [ ] Registros Acadêmicos - Trancamento
- [ ] Registros Acadêmicos - Desligamento
- [ ] Documentação Acadêmica - Histórico escolar (rendimento acadêmico, nota, frequência)
- [ ] Documentação Acadêmica - Emissão de diploma (expedição, registro, apostila)
- [ ] Documentação Acadêmica - Emissão de diploma (revalidação e reconhecimento)
- [ ] Documentação Acadêmica - Emissão de diploma (verificação de autencidade)
- [ ] Documentação Acadêmica - Assentamentos individuais (documentos pessoais e acadêmicos)
- [ ] Monitorias - Programas e Projetos
- [ ] Monitorias - Processo de seleção
- [ ] Monitorias - Indicação, aceite e substituição de monitor e orientador.
- [ ] Monitorias - Avaliação (relatórios e certificados)
- [ ] Estágios não obrigatórios - Acompanhamento e avaliação. Termos de compromisso e desligamento
- [ ] Estágios obrigatórios - Acompanhamento e avaliação. Termos de compromisso e desligamento

- [ ] ENADE - regularidade, lista de inscritos, lista de dispensados.
- [ ] Iniciação à docência - seleção
- [ ] Iniciação à docência - Indicação, aceite e substituição de monitor e orientador.
- [ ] Iniciação à docência - Avaliação (relatórios e declarações)
- [ ] Frequência de monitores, estagiários e bolsistas.
- [ ] Mobilidade acadêmica. Mobilidade nacional (documentos dos beneficiados).
- [ ] Mobilidade acadêmica. Mobilidade internacional (documentos dos beneficiados).
- [ ] Regime disciplinar dos alunos: penalidades (advertência ou repreensão).
- [ ] Declarações
- [ ] Certidões
- [ ] Não se aplica

45. Selecione os conjuntos de DOCUMENTOS, DADOS ou REGISTROS CIENTÍFICOS tratados pelo setor em formato físico ou digital

45. Marcar todas as opções que se aplicam *

Marque todas que se aplicam.

- [ ] Registro de projetos de pesquisa
- [ ] Registro de componentes de projeto de pesquisa
- [ ] Registro de participação em projeto de pesquisa
- [ ] Registro de resultado de projeto de pesquisa
- [ ] Registro de colaboração em projeto de pesquisa
- [ ] Registro de produção intelectual e publicações científicas
- [ ] Registro de eventos científicos
- [ ] Não se aplica

46. Selecione os conjuntos de DOCUMENTOS, DADOS ou REGISTROS DE EXTENSÃO tratados pelo setor em formato físico ou digital

46. Marcar todas as opções que se aplicam *

Marque todas que se aplicam.

- [ ] Registro de projetos de extensão
- [ ] Registro de componentes de projeto de extensão
- [ ] Registro de participação em projeto de extensão
- [ ] Registro de resultado de projeto de extensão
- [ ] Registro de colaboração em projeto de extensão
- [ ] Registro de eventos de extensão
- [ ] Não se aplica

DA ADOÇÃO DE BOAS PRÁTICAS DE SUAS ATIVIDADES NO SETOR DE TRABALHO

DA SEGURANÇA DA INFORMAÇÃO

47. 47. Você adota em seu setor de trabalho medidas de segurança, conforme as recomendações de boas práticas no desempenho das suas atividades? *

Exemplo: trocar de senhas de forma periódica, não compartilhamento de senhas, guarda de documentos com dados pessoais em local apropriado, etc.

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei

48. Você adota em seu setor de trabalho medidas de segurança, como controle de acesso baseado na necessidade de uso, isto é, o acesso só será concedido para desempenho de tarefas por setor específico, assegurado o acesso a usuário autorizado, prevenindo o acesso a sistemas e serviços desnecessariamente por usuário não autorizado/habilitado para esse fim

48. Marcar apenas uma opção *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei

CONSIDERAÇÕES FINAIS

Agradecemos sua participação e deixamos aqui um espaço para complementação de informações ou observações

49.

Plano de Capacitação em Proteção de Dados Pessoais na UFF conforme a LGPD

ETAPA 1: Incentivar todos os servidores da UFF a realizar cursos de nível básico de conhecimento

Objetivo	Meta	Cursos (*)	Prazo	Indicador	Unidade responsável pela capacitação	Monitoramento da atividade (**)
Incentivar a capacitação dos servidores da UFF na aplicação da LGPD em seus postos de trabalho Nível de conhecimento: Básico	Incentivar a todos os servidores por meio dos canais de comunicação da UFF	1. COMPETÊNCIA: PROTEÇÃO DE DADOS Curso: **Fundamentos da Lei Geral de Proteção de Dados** - 15 horas - ENAP - Disponível em: https://www.escolavirtual.gov.br/curso/603 2. COMPETÊNCIA: PROTEÇÃO DE DADOS Curso: **Introdução à Lei Brasileira de Proteção de Dados Pessoais** - 10 horas - ENAP - Disponível em: https://www.escolavirtual.gov.br/curso/153	Atividade contínua	Número de servidores informados	Escola de Governança em Gestão Pública, selecionando cursos disponíveis sobre o tema, observando a indicação do CGPD	Os servidores devem informar a suas chefias imediatas as ações de capacitação que forem concluídas e a chefia deve orientar que os servidores registrem as capacitações realizadas em formulário próprio.

Observação:

* Os temas sobre proteção de dados pessoais, tratamento dos dados, proteção dos dados e segurança da informação serão inseridos em outros treinamentos para uso dos sistemas UFF, bem como em qualquer curso ofertado pela EGGP em que o tema se aplique, destacando a importância dos servidores participarem dos cursos indicados.

** O monitoramento a ser realizado pela chefia imediata contará com formulário próprio para registro a ser disponibilizado na página da LGPD na UFF. (Link do formulário: https://forms.gle/V7LioYJeK6aQTEmMA).

ETAPA 2: Incentivar os gestores e demais servidores da UFF a realizar cursos de nível intermediário de conhecimento (*)

Objetivo	Meta	Cursos (**)	Prazo	Indicador	Unidade responsável pela capacitação	Monitoramento da atividade (***)
Incentivar a capacitação dos gestores e demais servidores da UFF na aplicação da LGPD em seus postos de trabalho Nível de conhecimento: Intermediário	Incentivar os gestores e demais servidores por meio dos canais de comunicação da UFF	1. COMPETÊNCIA: PROTEÇÃO DE DADOS Curso: **Proteção de Dados Pessoais no Setor Público** - 15 horas - ENAP - Disponível em: https://www.escolavirtual.gov.br/curso/290 2. COMPETÊNCIA: GOVERNANÇA DE DADOS Curso: **Como implementar a LGPD: bases, mecanismos e processos** - 15 horas - ENAP - Disponível em: https://www.escolavirtual.gov.br/curso/529 3. COMPETÊNCIA: SEGURANÇA DA INFORMAÇÃO Curso: **Fundamentos de Segurança da Informação na Transformação Digital** - 25 horas - ENAP - Disponível em: https://www.escolavirtual.gov.br/curso/916 4. COMPETÊNCIA: GOVERNANÇA DE DADOS Curso: **Governo Aberto** - 40 horas - ENAP - Disponível em: https://www.escolavirtual.gov.br/curso/140	Atividade contínua	Número de gestores e de servidores informados	Escola de Governança em Gestão Pública, selecionado cursos sobre o tema, observando a indicação do CGPD e da alta gestão para realização dos cursos pertinentes	Os gestores e demais servidores devem informar a suas chefias superiores as ações de capacitação que forem concluídas e registrarem as capacitações realizadas em formulário próprio.

Observação:

* Os cursos de nível de conhecimento intermediário são recomendados para gestores e demais servidores que queiram se aprofundar no assunto.

** Os temas sobre proteção de dados pessoais, tratamento dos dados, proteção dos dados e segurança da informação serão inseridos em outros treinamentos para uso dos sistemas UFF, bem como em qualquer curso ofertado pela EGGP em que o tema se aplique, destacando a importância dos servidores participarem dos cursos indicados.

*** O monitoramento a ser realizado pela chefia imediata contará com formulário próprio para registro a ser disponibilizado na página da LGPD na UFF. (Link do formulário: https://forms.gle/V7LioYJeK6aQTEmMA).

ETAPA 3: Incentivar servidores da UFF de áreas específicas afins a realizar cursos de nível alto de conhecimento

Objetivo	Meta	Cursos (*)	Prazo	Indicador	Unidade responsável pela capacitação	Monitoramento da atividade (***)
Incentivar a capacitação dos servidores das UORGS responsáveis pelos sistemas UFF, pela manutenção, proteção e segurança, os desenvolvedores de sistemas, responsáveis pela segurança da informação, privacidade por padrão e privacidade desde a concepção Nível de conhecimento: Alto	Incentivar os servidores das áreas específicas por meio dos canais de comunicação da UFF	1. COMPETÊNCIA: SEGURANÇA DA INFORMAÇÃO / GESTÃO DE RISCO Curso: **Segurança da Informação no contexto da transformação digital** - 25 horas - ENAP - Disponível em: https://www.escolavirtual.gov.br/curso/378 2. Cursos pagos específicos indicados pela chefia imediata (AIC **) **Cursos financiados pela EGGP/Progepe**: https://capacitacaoeggp.vr.uff.br/?page_id=80 3. Cursos exclusivos desenvolvidos e/ou contratados pela EGGP/Progepe (DDI **) **Cursos solicitados por gestores de áreas específicas**: https://capacitacaoeggp.vr.uff.br/?page_id=54	Atividade contínua e/ou mediante solicitação, observando os prazos regulamentares para a EGGP contratar, planejar e/ou desenvolver o curso	Número de servidores informados e/ou número de servidores capacitados quando se tratar de ações específicas oferecidas pela EGGP	Escola de Governança em Gestão Pública, selecionando cursos disponíveis em outras instituições e/ou oferecendo cursos específicos sobre o tema, observando a indicação do CGPD e dos gestores responsáveis pelos sistemas UFF	Os servidores de áreas específicas devem informar a suas chefias superiores as ações de capacitação que forem concluídas e registrarem as capacitações realizadas em formulário próprio.

Observação:

* Os temas sobre proteção de dados pessoais, tratamento dos dados, proteção dos dados e segurança da informação serão inseridos em outros treinamentos para uso dos sistemas UFF, bem como em qualquer curso ofertado pela EGGP em que o tema se aplique, destacando a importância dos servidores participarem dos cursos indicados.

** O AIC (Apoio a Iniciativas de Capacitação) é um serviço oferecido pela EGGP/Progepe que financia a capacitação individual dos servidores voltada para o desenvolvimento das competências institucionais. Já a DDI (Demanda de Desenvolvimento Institucional) é um instrumento que permite ao gestor registrar demandas de ações de desenvolvimento de maior abrangência no escopo institucional, destinando-se a um quantitativo maior de servidores e não se restringem necessariamente a um único setor ou unidade.

*** O monitoramento a ser realizado pela chefia imediata contará com formulário próprio para registro a ser disponibilizado na página da LGPD na UFF. (Link do formulário: https://forms.gle/V7LioYJeK6aQTEmMA).

Observações finais:

Consultando o portal da transparência da UFF em 10/08/23, verificou-se que a instituição conta com o total de 6.828[1] servidores, entre docentes e técnicos, dos quais 121 são gestores ocupantes de cargos de direção (CD-1 a CD-4) e 316 são ocupantes de funções comissionadas (FG-1 a FG-3), todos em efetivo exercício na instituição.

Acreditamos que as ações de capacitação mapeadas e apresentadas no presente plano são adequadas para instruir os servidores da UFF, contribuindo para o desenvolvimento das competências requeridas, conforme segmentação estabelecida nos respectivos níveis de conhecimento (básico, intermediário e alto).

Em relação às ações de capacitação que venham a precisar de contratação e/ou desenvolvimento exclusivo pela EGGP, destinadas a servidores de áreas específicas, orientamos que os gestores das respectivas áreas identifiquem as competências que precisam ser desenvolvidas (conhecimentos, habilidades e atitudes) que não são abordadas pelos cursos já mapeados e apontem, por meio dos instrumentos de AIC e DDI, conforme o caso, o quantitativo de servidores que precisam se desenvolver nas competências identificadas. A partir da submissão por meio dos referidos instrumentos, a EGGP poderá analisar as especificidades apresentadas e realizar a contratação e/ou o desenvolvimento de cursos exclusivos para os servidores em questão, observando os prazos regulamentares para a EGGP planejar, contratar e/ou desenvolver o curso.

Por fim, no que diz respeito ao monitoramento do quantitativo de servidores capacitados, acreditamos que a elaboração de orientações e/ou instrumentos unificados poderá contribuir para sistematizar o efetivo controle por parte das chefias imediatas e gestores, além de facilitar o acompanhamento pelo CGPD.

[1] Dados disponíveis em: https://analytics.uff.br/superset/dashboard/progepe_servidores/

Plano de Capacitação em Privacidade e Segurança da Informação na UFF

ETAPA1:Incentivar todos os servidores da UFF a realizar cursos de nível básico deconhecimento

Objetivo	Meta	Cursos(*)	Prazo	Indicador	Unidade responsável pela capacitação	Monitoramento da atividade (**)
Incentivar a capacitação dos servidores da UFF na aplicação das condutas e práticas de segurança da informação e privacidade em seus postos detrabalho Nível de conhecimento: Básico	Incentivar a todos os servidores por meio dos canais de comunicação da UFF	1. COMPETÊNCIA: SEGURANÇA DA INFORMAÇÃO Curso:**Segurança da Informação para todos**- 24 horas - ENAP - Disponível em:https://www.escolavirtual.gov.br/curso/1256	Atividade contínua	Número de servidores informados	Escola de Governança em Gestão Pública, selecionando cursos disponíveis sobre o tema, observando a indicação do CGPD	Os servidores devem informar a suas chefias imediatas as ações de capacitação que forem concluídas e a chefia deve orientar que os servidores registrem as capacitações realizadas em formulário próprio.

Observação:

* Os temas sobre privacidade e segurança da informação serão inseridos em outros treinamentos para uso dos sistemas UFF, bem como em qualquer curso ofertado pela EGGP em que o tema se aplique, destacando a importância dos servidores participarem dos cursos indicados.

**O monitoramento a ser realizado pela chefia imediata contará com formulário próprio para registro a ser disponibilizado na página da LGPD naUFF.(Link do formulário:https://forms.gle/V7LioYJeK6aQTEmMA).

ETAPA 2: Incentivar os gestores e demais servidores da UFF a realizar cursos de nível intermediário de conhecimento(*)

Objetivo	Meta	Cursos(**)	Prazo	Indicador	Unidade responsável pela capacitação	Monitoramento da atividade (***)
Incentivar a capacitação dos gestores e demais servidores da UFF na aplicação das condutas e práticas de segurança da informação e privacidade da em seus postos de trabalho Nível de conhecimento: Intermediário	Incentivar os gestores e demais servidores por meio dos canais de comunicação da UFF	1. COMPETÊNCIA: SEGURANÇA DA INFORMAÇÃO Curso:**Fundamentos de Segurança da Informação na Transformação Digital**- 25 horas - ENAP - Disponível em:https://www.escolavirtual.gov.br/curso/916	Atividade contínua	Número de gestores e de servidores informados	Escola de Governança em Gestão Pública, selecionado cursos sobre o tema, observando a indicação do CGPD e da alta gestão para realização doscursos pertinentes	Os gestores e demais servidores devem informar a suas chefias superiores as ações de capacitação que forem concluída se registrarem as capacitações realizadas em formulário próprio.

Observação:

* Os cursos de nível de conhecimento intermediário são recomendados para gestores e demais servidores que queiram se aprofundar no assunto.

** Os temas sobre privacidade e segurança da informação serão inseridos em outros treinamentos para uso dos sistemas UFF, bem como em qualquer curso ofertado pela EGGP em que o tema se aplique, destacando a importância dos servidores participarem dos cursos indicados.

***O monitoramento a ser realizado pela chefia imediata contará com formulário próprio para registro a ser disponibilizado na página da LGPD na UFF. (Link do formulário:https://forms.gle/V7LioYJeK6aQTEmMA).

ETAPA3:Incentivar servidores da UFF de áreas específicas afins a realizar cursos de nível alto de conhecimento

Objetivo	Meta	Cursos(*) TRILHA DE APRENDIZAGEM: Disponível em https://www.escolavirtual.gov.br/trilha/246	Prazo	Indicador	Unidade responsável pela capacitação	Monitoramento da atividade(***)
Incentivar a capacitação dos servidores das UORGS responsáveis pelos sistemas UFF, pela manutenção, proteção e segurança, os desenvolvedores de sistemas, responsáveis pela privacidade e segurança da informação, privacidade por padrão e privacidade desde a concepção Nível de conhecimento: Alto	Incentivar os servidores das áreas específicas por meio dos canais de comunicação da UFF	Trilho 1 . Curso:**Conhecendo a legislação de proteção de dados pessoais-20**horas-ENAP Trilho 2 . Curso: **Atuando na governança e na aplicação de medidas de proteção de dados pessoais- 34** horas-ENAP Trilho 3 . Curso: **Detalhando as atribuições do encarregado pelo tratamento de dados pessoais – 5** horas-ENAP Trilho 4 . Curso:**Criando uma estrutura básica em segurança da informação – 127** horas-ENAP Trilho 5 . **Curso: Protegendo os ativos institucionais e o ambiente tecnológico da organização – 5 h – ENAP** Trilho 6 . **Curso: Respondendo a um incidente de segurança– 16 h – ENAP** 1. Cursos pagos específicos indicados pela chefia imediata (AIC **) **Cursos financiados pela EGGP/Progepe**:https://capacitacaoeggp.vr.uff.br/?page_id=80 2. Cursos exclusivos desenvolvidos e/ou contratadospelaEGGP/Progepe(DDI**) **Cursos solicitados por gestores de áreas**	Atividade contínua e/ou mediante solicitação, observando os prazos regulamentares para a EGGP contratar, planejar e/ou desenvolver o curso	Número de servidores informados e/ou número de servidores capacitados quando se tratar de ações específicas oferecidas pela EGGP	Escola de Governança em Gestão Pública, selecionando cursos disponíveis em outras instituições e/ou oferecendo cursos específicos sobre o tema, observando a indicação do CGPD e dos gestores responsáveis pelos sistemas UFF	Os servidores de áreas específicas devem informar a suas chefias superiores as ações de capacitação que forem concluídas e registrarem as capacitações realizadas em formulário próprio.

ETAPA3:Incentivar servidores da UFF de áreas específicas afins a realizar cursos de nível alto de conhecimento

		específicas:https://capacitacaoeggp.vr.uff.br/?page_id=54				

Observação:

* Os temas sobre privacidade e segurança da informação serão inseridos em outros treinamentos para uso dos sistemas UFF, bem como em qualquer curso ofertado pela EGGP em que o tema se aplique, destacando a importância dos servidores participarem dos cursos indicados.

** O AIC (Apoio a Iniciativas de Capacitação) é um serviço oferecido pela EGGP/Progepe que financia a capacitação individual dos servidores voltada para o desenvolvimento das competências institucionais. Já a DDI(Demanda de Desenvolvimento Institucional) é um instrumento que permite ao gestor registrar demandas de ações de desenvolvimento de maior abrangência no escopo institucional, destinando-se a um quantitativo maior de servidores e não se restringem necessariamente a um único setor ou unidade.

***O monitoramento a ser realizado pela chefia imediata contará com formulário próprio para registro a ser disponibilizado na página da LGPDnaUFF. (Link do formulário:https://forms.gle/V7LioYJeK6aQTEmMA).

Observaçõesfinais:

Consultando o portal da transparência da UFF em 10/08/23, verificou-se que a instituição conta com o total de 6.828 [1]servidores, entre docentes e técnicos,dos quais 121 são gestores ocupantes de cargos de direção (CD-1 a CD-4) e 316 são ocupantes de funções comissionadas (FG-1aFG-3), todos em efetivo exercício na instituição.

Acreditamos que as ações de capacitação mapeadas e apresentadas no presente plano são adequadas para instruir os servidores da UFF, contribuindo para o desenvolvimento das competências requeridas,conforme segmentação estabelecida nos respectivos níveis de conhecimento (básico,intermediário e alto).

Em relação às ações de capacitação que venham a precisar de contratação e/ou desenvolvimento exclusivo pela EGGP, destinadas a servidores de áreas específicas, orientamos que os gestores das respectivas áreas identifiquem as competências que precisam ser desenvolvidas(conhecimentos, habilidades e atitudes) que não são abordadas pelos cursos já mapeados e apontem, por meio dos instrumentos de AIC e DDI, conforme o caso, o quantitativo de servidores que precisam se desenvolver nas competências identificadas. A partir da submissão por meio dos referidos instrumentos, a EGGP poderá analisar as especificidades apresentadas e realizar a contratação e/ou o desenvolvimento de cursos exclusivos para os servidores em questão, observando os prazos regulamentares para a EGGP planejar, contratar e/ou desenvolver o curso.

Por fim, no que diz respeito ao monitoramento do quantitativo de servidores capacitados, acreditamos que a elaboração de orientações e/ou instrumentos unificados poderá contribuir para sistematizar o efetivo controle por parte das chefias imediatas e gestores, além de facilitar o acompanhamento pelo CGPD.

[1]Dadosdisponíveisem:https://analytics.uff.br/superset/dashboard/progepe_servidores/

Plano de Comunicação Interna em Proteção de Dados Pessoais na UFF

Apresentação

O presente documento, elaborado pela Superintendência de Comunicação Social (SCS), visa apresentar à comunidade acadêmica e demais interessados as principais ações de comunicação previstas para tratar da temática de proteção de dados pessoais no âmbito universitário.

A iniciativa faz-se necessária tendo em vista a Lei Geral de Proteção de Dados, oficialmente publicada em 2018, que 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.

Desde então, a UFF vem fortalecendo o uso dos mecanismos previstos na LGPD, prevenindo abusos no uso e compartilhamento de dados pessoais, o uso indevido em práticas prejudiciais com desvio de finalidade, além de promover a confiança entre a instituição e a comunidade universitária, sendo este plano a consolidação de mais uma etapa de conscientização dos públicos diretamente envolvidos, como técnicos administrativos e docentes.

Abaixo, discriminamos as ações de comunicação alinhadas aos princípios e diretrizes organizacionais, e em consonância com as atividades educativas e de capacitação planejadas pela instituição.

Produto	**Público**	**Canal**	**Objetivo**	**Status**
Matéria	Técnicos e docentes (todos os níveis, incluindo as chefias)	Boletim Comunica UFF	Apresentar de modo geral o tema "LGPD", explicando do que se trata a lei e alguns exemplos práticos para a proteção de dados na universidade.	Finalizado (ação realizada em abril/2023)
Informe	Técnicos e docentes	Boletim Minuto Gestão de	Divulgar 3 cursos básicos	Finalizado (ação realizada

	(todos os níveis, incluindo as chefias)	Pessoas	de formação em LGPD: Lei Geral de Proteção de Dados; Fundamentos de Proteção de Dados; e Como implantar a LGPD	em maio/2023)
Matéria	Técnicos e docentes (todos os níveis, incluindo as chefias)	Boletim Comunica UFF	Compartilhar com a comunidade interna o formulário de mapeamento do nível de maturidade em relação à LGPD.	Finalizado (ação realizada em julho de 2023)
Informe	Técnicos e docentes (todos os níveis, incluindo as chefias)	Boletim Minuto Gestão de Pessoas	Divulgar 3 cursos básicos de formação em LGPD: Você está por dentro da LGPD; Introdução Brasileira à Lei de Proteção de Dados; e Proteção de Dados	Finalizado (ação realizada em julho de 2023)
Vídeo	Diretores de unidades acadêmicas	Grupo de Whatsapp	Veicular vídeo do reitor explicando para o grupo de gestores a importância da proteção de dados e a importância de capacitação de todos os servidores em cursos gratuitos sobre o tema	Finalizado (ação realizada em agosto de 2023)
Informe	Técnicos e docentes (todos os níveis, incluindo as chefias)	Boletim Pílula do SEI	Dica sobre cuidados com informações pessoais no sistema, como a classificação de emails e documentos que contenham esses dados como restritos	Finalizado (ação realizada em agosto de 2023)

Informe	Técnicos e docentes (todos os níveis, incluindo as chefias)	Boletim Minuto Gestão de Pessoas	Divulgar 3 cursos básicos de formação em LGPD: proteção de dados pessoais no setor público; fundamentos de segurança da informação; governança de dados	Finalizado (ação realizada em setembro de 2023)
Informe	Chefias em todos os níveis	Boletim UFF Informa	Divulgar plano de capacitação sobre proteção de dados pessoais	Previsto para setembro de 2023
Banner	Técnicos e docentes	Boletim Comunica UFF	Inserir banner no Comunica UFF com chamariz para a área de perguntas e respostas na página da LGPD. A ideia é não deixar o assunto "esfriar".	Previsto para outubro de 2023
Notas/informes	Comunidade interna e externa	Página da LGPD no site institucional (www.uff.br/lgpd)	Atualização da página da LGPD, com dados administrativos, e informações sobre capacitação, entre outros	Ação contínua
Webinário	Comunidade interna e externa	Página da LGPD no site institucional e boletins enviados por e-mail	Produção de vídeo com a participação de professores e outras autoridades nos temas “Lei Geral de Proteção de Dados”, “Segurança da Informação com recomendação de boas práticas” e “Gestão de	Ação contínua

			Riscos nas unidades”. A ideia é oferecer um treinamento contínuo à comunidade interna.	

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL FLUMINENSE
CONSELHO UNIVERSITÁRIO

RESOLUÇÃO CUV/UFF Nº 161 DE 07 DE DEZEMBRO DE 2022

Dispõe sobre a Política de Gestão de Riscos da Universidade Federal Fluminense.

O CONSELHO UNIVERSITÁRIO da UNIVERSIDADE FEDERAL FLUMINENSE, no uso de suas atribuições estatutárias e regimentais, e considerando o que mais consta do Processo nº 23069.176740/2022-41,

R E S O L V E :

Art. 1º - Aprovar a ***Política de Gestão de Riscos*** da Universidade Federal Fluminense.

Art. 2º - A presente Resolução entrará em vigor na data de sua publicação.

* * * *

Sala das Sessões, 07 de dezembro de 2022.

ANTONIO CLAUDIO LUCAS DA NÓBREGA
Presidente
# # # # # #

Anexo da Resolução CUV/UFF nº 161 de 07 de dezembro de 2022

POLÍTICA DE GESTÃO DE RISCOS

CAPÍTULO I
DOS OBJETIVOS E PRINCÍPIOS

Art. 1º A Política de Gestão de Riscos da Universidade Federal Fluminense, denominada PGRISCOS-UFF, tem por objetivo estabelecer os princípios, as diretrizes e as responsabilidades sobre o gerenciamento de riscos da UFF, contribuindo para o alcance dos objetivos estratégicos dainstituição.

Art. 2º A PGRISCOS-UFF deve estar alinhada com os objetivos institucionais definidos no Plano de Desenvolvimento Institucional (PDI), por meio da identificação dos riscos vinculados aos objetivos estratégicos da UFF, e será regida pelos seguintes princípios:

I. gestão de riscos de forma sistemática, estruturada e oportuna, subordinada ao interesse público;
II. estabelecimento de níveis de exposição a riscos adequados;
III. estabelecimento de procedimentos de controle interno proporcionais ao risco, observada a relação custo-benefício, e destinados a agregar valor à organização;
IV. utilização do mapeamento de riscos para apoio à tomada de decisão e à elaboração do planejamento estratégico;
V. utilização da gestão de riscos para apoio à melhoria contínua dos processos organizacionais.

Parágrafo único. A metodologia aplicada está descrita no Plano de Gestão de Riscos a ser submetidoao Comitê de Governança, Integridade, Riscos e Controles (CGIRC) para atualização e aprovação.

CAPÍTULO II
DA GOVERNANÇA DA GESTÃO DE RISCOS

Art. 3º A Gestão de Riscos da UFF será definida em três documentos, sendo eles: a Política de Gestão de Riscos, o Plano de Gestão de Riscos e o Relatório de Gestão de Riscos.

I. A Política de Gestão de Riscos, constituída do presente documento, que define as regras de alto nível (estratégico) que representam os princípios básicos que a UFF decidiu incorporar à sua gestão, no que se refere à Gestão de Riscos.
II. O Plano de Gestão de Riscos, documento que especifica, no nível operacional, os controles,os conceitos, a metodologia e as ferramentas que deverão ser utilizadas para alcançar a estratégia definida na PGRISCOS-UFF.
III. O Relatório de Gestão de Riscos, que tem a finalidade de avaliar e monitorar o Plano de Gestão de Riscos da UFF.

Art.4º Esta Política e seus documentos complementares podem ser reavaliados de acordo com as determinações do Comitê de Governança, Integridade, Riscos e Controles (CGIRC).

Art. 5º A PGRISCOS-UFF deve ser amplamente divulgada no âmbito da Universidade.

CAPÍTULO III DAS DIRETRIZES

Art. 6º A UFF deverá contemplar, em seu Plano Anual de Capacitação, ações voltadas para o desenvolvimento contínuo dos agentes públicos em Gestão de Riscos.

Art. 7º Cabe ao Comitê de Governança, Integridade, Riscos e Controles - CGIRC aprovar a elaboração e revisão de políticas, diretrizes, metodologias e mecanismos para comunicação e institucionalização da integridade, da gestão de riscos e dos controles internos.

Art. 8º O monitoramento e o tratamento dos riscos devem ser contínuos, e a identificação e a avaliação dos riscos devem ser realizadas anualmente.

CAPÍTULO IV DA ABRANGÊNCIA DA POLÍTICA

Art. 9º A PGRISCOS-UFF deverá ser observada em todos os níveis da Instituição e por todos os seus servidores e agentes.

Art. 10. Esta Política de Gestão de Riscos abrange as seguintes tipologias de riscos:

I. riscos estratégicos
II. riscos operacionais
III. riscos legais
IV. riscos de integridade
V. riscos financeiros/orçamentários
VI. riscos de imagem/reputação

CAPÍTULO V DAS INSTÂNCIAS

Art. 11. São instâncias da Política da Gestão de Riscos, na UFF:

I – **Comitê de Governança, Integridade, Riscos e Controles (CGIRC)** - composto pelo Reitor, que o preside; Vice-Reitor; Chefe de Gabinete; Pró-Reitores; Superintendentes, e Coordenador(a) da Unidade de Gestão da Integridade.

II - **Coordenação de Planejamento e Desenvolvimento (PLAD/PROPLAN)** – Unidade da Pró- Reitoria de Planejamento (PROPLAN), responsável pela coordenação e monitoramento da implementação da gestão de riscos na UFF.

III – **Subcomitê de Gestão de Riscos** – o Subcomitê deverá ser composto por servidores das unidades acadêmicas e administrativas, com alçada suficiente para decidir sobre medidas de mitigação e tratamento dos riscos, além de orientar e acompanhar as ações de mapeamento e avaliação do risco;

IV – **Gestor de Riscos**– agente responsável pelo gerenciamento de risco, com alçada suficiente para orientar e acompanhar as ações de mapeamento, avaliação e mitigação do risco. Dirigente de unidade acadêmica ou administrativa, responsável por gerir os riscos referentes ao seu nível organizacional, bem como apoiar e orientar as ações dos Proprietários de Risco de suas subunidades.

V – **Proprietário do Risco** – corresponde a todo e qualquer servidor responsável pela execução deum determinado processo de trabalho, inclusive sobre a gestão de riscos.

CAPÍTULO VI
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 12. As principais atribuições dos atores envolvidos no processo de gerenciamento de riscos estão relacionadas abaixo. O rol de atribuições do CGIRC é definido conforme a IN MPOG/CGU 01/2016 e a Portaria UFF nº 68.259 de 10 de agosto de 2021.

I - **Comitê de Governança, Integridade, Riscos e Controles - CGIRC**

a) promover práticas e princípios de conduta e padrões éticos de comportamentos;

b) institucionalizar estruturas adequadas de governança, integridade, gestão de riscos e controles internos;

c) promover o desenvolvimento contínuo dos agentes públicos e incentivar a adoção de boas práticas de governança, de integridade, de gestão de riscos e de controles internos;

d) garantir a aderência às regulamentações, leis, códigos, normas e padrões, com vistas à condução das políticas e à prestação de serviços de interesse público;

e) promover a integração dos agentes responsáveis pela governança, pela integridade, pela gestão de riscos e pelos controles internos;

f) promover a adoção de práticas que institucionalizem a responsabilidade dos agentes públicosna prestação de contas, na transparência e na efetividade das informações;

g) aprovar a elaboração e revisão de políticas, diretrizes, metodologias e mecanismos para comunicação e institucionalização da integridade, da gestão de riscos e dos controles internos;

h) supervisionar o mapeamento e a avaliação dos riscos-chave que podem comprometer a prestação de serviços de interesse público;

i) liderar e supervisionar a institucionalização da gestão da integridade, da gestão de riscos e dos controles internos, oferecendo suporte necessário para sua efetiva implementação no órgão ou unidade;

j) estabelecer limites de exposição a riscos globais da UFF, bem como os limites de alçada ao nível de unidade;

k) aprovar e supervisionar método de priorização de temas e macroprocessos para gerenciamento de riscos e implementação dos controles internos da gestão;

l) emitir recomendação para o aprimoramento da governança, da gestão da integridade, da gestão de riscos e dos controles internos; e

m) acompanhar a implementação das recomendações e orientações do Comitê.

II – Coordenação de Planejamento e Desenvolvimento (PLAD/PROPLAN)

a) implantar e manter a PGRISCOS-UFF;
b) propor ao CGIRC a metodologia de Gestão de Riscos e suas revisões;
c) requisitar aos proprietários dos riscos as informações necessárias para a consolidação dos dadose a elaboração de relatórios gerenciais;
d) elaborar e divulgar o Relatório de Gestão de Riscos;
e) coordenar as ações do Subcomitê de Gestão de Riscos
f) Diligenciar para que as informações adequadas sobre os riscos estejam disponíveis em todos os níveis da Instituição.

III– Subcomitê de Gestão de Riscos

a) Propor o Plano de Gestão de Riscos para aprovação do CGIRC;
b) identificar, analisar, tratar e monitorar os riscos de forma contínua;
c) divulgar, atualizar e gerenciar as questões que envolvem a Gestão de Riscos.

IV – Gestor do Risco

a) garantir que os riscos sejam gerenciados de acordo com a Política de Gestão de Riscos da UFF;
b) elaborar e assegurar a implementação do plano de ação para tratamento dos riscos sob sua responsabilidade
c) monitorar, no respectivo âmbito, os riscos ao longo do tempo, de modo a garantir que as medidasde mitigação adotadas resultem na manutenção dos riscos em níveis adequados, de acordo com a PGRISCOS-UFF;
c) garantir que as informações adequadas sobre os riscos estejam disponíveis em todos os níveis da Instituição;
c) comunicar à PLAD sobre situações que envolvam risco.
g) requisitar aos proprietários dos riscos as informações necessárias para a consolidação dos dadose elaborar os relatórios gerenciais para a PLAD/PROPLAN;

V – Proprietário do Risco

a) contribuir nas atividades de identificação, análise e avaliação dos riscos inerentes aos processos sob sua responsabilidade;
b) comunicar tempestivamente ao Gestor de Risco eventos inerentes aos processos de sua responsabilidade;
c) executar os planos de tratamento e respostas aos riscos;
h) elaborar os relatórios anuais para o Gestor de Riscos.

CAPÍTULO VI
DAS DISPOSIÇÕES FINAIS

Art. 13. Os casos omissos serão dirimidos pelo Comitê de Governança, Integridade, Riscos e Controles da UFF.

CONCEITOS
(Anexo I)

I. **Apetite ao risco**: é o nível de risco que uma organização está disposta a aceitar, dentro de padrões considerados institucionalmente aceitáveis;

II. **Evento:** ocorrência gerada com base em fontes internas ou externas que pode causar impacto negativo, positivo ou ambos;

III. **Gerenciamento de riscos**: processo contínuo que consiste no desenvolvimento de um conjunto de ações destinadas a identificar, avaliar, administrar e controlar potenciais eventos ou situações,capazes de afetar os objetivos, processos e projetos da organização;

IV. **Impacto**: resultado ou efeito de um evento, podendo ser positivo ou negativo em relação aos objetivos de uma organização;

V. **Incerteza**: diz respeito à incapacidade de conhecer antecipadamente a probabilidade exata ou o impacto de eventos futuros;

VI. **Matriz de riscos**: documento onde são registrados os riscos identificados e a avaliação de seus impactos e probabilidades de ocorrência para os processos, etapas e atividades das unidades acadêmicas ou administrativas;

VII. **Mensuração de risco**: significa estimar a importância de um risco e calcular a probabilidade e oimpacto de sua ocorrência.

VIII. **Nível de risco**: é o nível de criticidade do risco, assim compreendido o quanto um risco pode afetar os objetivos, processos de trabalho e projetos da organização, a partir da escala predefinida de criticidades possíveis.

IX. **Política de Gestão de Riscos**: declaração das intenções e diretrizes gerais de uma organização relacionadas à Gestão de Riscos.

X. **Probabilidade**: é a chance de o risco acontecer, estabelecida a partir de uma escala predefinida de probabilidades possíveis;

XI. **Risco**: possibilidade de que um evento ocorra e afete, positiva (oportunidade) ou negativamente (ameaça) os objetivos da instituição. O risco é medido em termos de impacto e probabilidade.

XII. **Riscos estratégicos**: impactam diretamente no atingimento dos objetivos estratégicos definidos no Planejamento Estratégico da Instituição;

XIII. **Riscos financeiros/orçamentários**: eventos que podem comprometer a capacidade do órgão ou entidade de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações.

XIV. **Riscos de imagem/reputação**: eventos que podem comprometer a confiança da sociedade (ou de parceiros, clientes ou fornecedores) em relação à capacidade do órgão ou da entidade em cumprir sua missão institucional.

XV. **Riscos operacionais**: eventos que podem comprometer as atividades do órgão ou entidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas.

XVI. **Riscos legais**: eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades do órgão ou entidade;

XVII. **Riscos de Integridade**: riscos que configurem ações ou omissões quepossam favorecer aocorrência de fraudes ou atos de corrupção;

XVIII. **Risco inerente**: risco a que uma organização está exposta sem considerar quaisquer açõesgerenciais que possam reduzir a probabilidade desua ocorrência ou seu impacto.

XIX. **Risco residual**: risco a que uma organização está exposta após aimplementação de açõesgerenciais para o tratamento do risco;

XX. **Risco aceitável ou baixo**: de baixo impacto e frequência, não havendo necessidade demonitoramento contínuo;

XXI. **Risco inaceitável ou alto**: demanda ação gerencial prioritária para eliminar acomponente de riscoou reduzir sua severidade e/ou frequência;

XXII. **Risco provável ou médio**: risco que deve ser tratado em médio prazo. O risco deve ser monitoradofrequentemente.