Universidade Federal Fluminense

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

Sumário

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 na LGPD:

- **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.

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