FUNDAÇÃO EDUCACIONAL DA REGIÃO DE JOINVILLE - FURJ

UNIVERSIDADE DA REGIÃO DE JOINVILLE - UNIVILLE

univille

Manual de Segurança da Informação e Proteçao de Dados

(Anexo a Instrução Normativa Conjunta nº 001/2022 – FURJ/UNIVILLE/INOVAPARQ)

Julho/2022

1 - Introdução

A **Lei Geral de Proteção de Dados Pessoais e Sensíveis – LGPD, Lei nº 13.709**, foi aprovada no ano de 2018, entrando em vigor em agosto de 2020, deixando as sanções explicitas na lei para entrarem em vigor a partir de agosto de 2021.

A LGPD trouxe importante dinâmica a forma como os dados pessoais são tratados pelas empresas privadas e órgãos públicos, ordenando expressamente o direito do Titular dos dados e dos agentes de tratamento de dados (controlador e operador), pessoas jurídicas que utilizam os dados para determinados fins em suas operações e negócios.

A lei apontou de forma cristalina direitos e deveres dos agentes de tratamento de dados, os quais, sem o consentimento do titular "somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, como promoção de suas atividades" ou na proteção do próprio interesse do titular do dado. O descumprimento da legislação acarretará para o infrator multas pesadas, bem como, a possibilidade de suspensão parcial ou total das atividades que envolvem dados pessoais.

Por essa razão, para o cumprimento da Lei Geral de Proteção de Dados, presta-se o presente manual, visando colocar os usuários dos sistemas da FURJ e suas mantidas em sintonia com a referida lei, devendo os usuários, principalmente empregados da Instituição, evitarem o compartilhamento de dados pessoais para terceiros que não estejam relacionados com a atividade laboral de seu setor, bem como, em caso de necessidade ou dúvida, utilizar-se do encarregado de dados a fim de sanar dúvidas ou obter informações e/ou orientações de como proceder.

2 - Definições

Com o objetivo de uniformizar o entendimento, consideram-se as seguintes definições sobre os temas que serão tratados no presente manual:

I - LGPD: – Lei Geral de Proteção de Dados Pessoais e alterações;
II – TIC: Tecnologia da Informação e Comunicação;
III – Usuário Interno: docentes, discentes, pessoal administrativo, estagiários, aprendizes e terceiros que possuem vínculo institucional com a FURJ e suas mantidas;

IV – Usuário Externo: pessoa física ou jurídica que não possui vínculo institucional com a FURJ e suas mantidas, porém acessa serviços e recursos disponibilizados à comunidade externa;
V – ANPD: - Autoridade Nacional de Proteção de Dados;
VI – Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
VII – 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;
VIII – Banco de dados: conjunto estruturado de dados pessoal ou institucional, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
IX – Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
X – Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
XI – Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
XII – Agentes de tratamento: o controlador e o operador;
XIII – Encarregado: pessoa indicada pelo controlador e/ou operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
XIV – 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;
XV – Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
XVI – Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
XVII – Compartilhamento de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XVIII – Relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
XIX – Autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional;
XX – Manual de Segurança da Informação e Proteção de Dados: é o documento informativo que a FURJ coloca à disposição da comunidade acadêmica e terceiros sobre como proceder para com a proteção de dados e sistemas de informações;
XXI – Comunidade acadêmica: Todas as pessoas que acessam os ambientes e/ou serviços disponibilizados pela FURJ e suas mantidas;
XXII – Ativo de informação: é tudo aquilo que tem valor para a organização, podendo ser um processo, uma tecnologia, um ambiente ou pessoas;
XXIII – GTI – Gerência de Tecnologia da Informação.

3 - Abrangência e Responsabilidades

São responsabilidades de todos que utilizam ou têm acesso às informações da FURJ e suas mantidas:

✓ Conhecer e seguir as definições e orientações deste manual e da Instrução Normativa de Segurança da Informação e Proteção de Dados da FURJ e suas mantidas, bem como posteriores alterações;
✓ Reportar para a Gerência de Tecnologia da Informação incidentes que possam atingir a segurança das informações da FURJ e suas mantidas;
✓ Proteger as informações contra divulgação, destruição, modificação e acessos não autorizados;
✓ Zelar e proteger a marca e a reputação da FURJ e suas mantidas;
✓ Zelar pela segurança do patrimônio da FURJ e suas mantidas;
✓ Utilizar os recursos de Tecnologia da Informação e Comunicação – TICs, somente para as atividades que possui vínculo institucional;
✓ Zelar pela correta utilização, tratamento, guarda e confidencialidade dos dados, informações e TICs institucionais;
✓ Manter sigilo da senha de acesso aos sistemas de informação e demais recursos computacionais da FURJ e suas mantidas;
✓ Informar ao gestor imediato sobre eventual problema ocorrido no sistema tecnológico ou acesso não autorizado a esses sistemas;
✓ Manter o seu posto de trabalho organizado de forma a evitar a exposição e vulnerabilidade de dados e informações.

✓ Informar à Gerência de Tecnologia da Informação, imediatamente, caso seu equipamento não possua um software antivírus instalado.

4 - Uso Aceitável dos Ativos

Com a entrada em vigor da Lei Geral de Proteção de Dados, passa a ser obrigatório a todos os usuários internos e externos, a utilização dos ativos disponibilizados pela Instituição, com vistas à proteção da informação considerada estratégica, bem como para a proteção de dados pessoais. Cita-se alguns dos ativos mais importantes, não se limitando a apenas estes:

4.1 - Correio eletrônico/e-mail institucional (@univille.br)

O correio eletrônico é o meio oficial de comunicação interna e externa da FURJ e suas mantidas, sendo assim todos os usuários devem utilizar este recurso levando em consideração que:

• As mensagens do correio eletrônico devem ser escritas em linguagem profissional de forma que não comprometa a imagem da FURJ e suas mantidas. Nesse sentido, utilize na redação do e-mail vocabulário que não atinja a honra ou a dignidade do destinatário; devendo ser clara, objetiva e que não infrinja nenhuma legislação, tampouco os princípios institucionais da FURJ e suas mantidas;

• O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço;

• O conteúdo do correio eletrônico institucional de cada usuário pode ser acessado pela FURJ quando em situações que ponham em risco a sua imagem ou para investigação de ilícito cometido pelo usuário. Essa situação ocorrerá mediante requerimento por escrito do gestor imediato ou Presidente de Comissão de sindicância, inquérito ou processo administrativo, à presidência da FURJ. Com o deferimento do pedido o requerente poderá executar as ações autorizadas;

• É obrigatório o uso do e-mail institucional (@univille.br) para o desenvolvimento das atividades laborais;

O usuário não pode originar ou encaminhar mensagens ou imagens que:

✓ contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;

✓ menosprezem, depreciem, incitem ao preconceito a determinada classe, sexo, raça, orientação sexual, idade, religião, nacionalidade ou deficiência física;

✓ possua informação pornográfica, obscena ou imprópria para um ambiente profissional;

- ✓ possam trazer prejuízos a pessoa física ou jurídica;
- ✓ sejam hostis ou ofensivas;
- ✓ defendam ou possibilitem a realização de atividades ilegais;
- ✓ possam prejudicar a imagem ou serviços da FURJ e suas mantidas;
- ✓ sejam incoerentes com as políticas, valores e missão da Instituição; ou
- ✓ violem a LGPD.

• Quando enviar uma mensagem de correio eletrônico, ela está restrita ao destinatário. Porém, algumas informações exigem um grau de sigilo maior e por isso deve, ser indicado o nível de classificação da mensagem, dentre os níveis de confidencialidade descritos no item Classificação da Informação (pública, interna, confidencial, restrita outlook);
• Tenha muita atenção com o uso da opção “Encaminhar/Forward”, pois esse tipo de ação cria um histórico com todas as mensagens encaminhadas, aumentando o risco de quebra de confidencialidade da informação e leitura indevida de mensagens do correio eletrônico;
• Não abra arquivos de remetentes desconhecidos. Remova esses arquivos do seu ambiente de correio eletrônico;
• Na dúvida, ao receber uma mensagem suspeita, entre em contato com a Gerência de Tecnologia da Informação para obter suporte.

4.2 - Internet

A FURJ e suas mantidas disponibilizam acesso à internet para viabilizar a execução das atividades de ensino, pesquisa, extensão e administrativas, devendo os usuários estarem cientes que:
• Todo e qualquer arquivo recebido/baixado a partir do ambiente de Internet da FURJ e suas mantidas deve ser analisado por software de antivírus homologado pela Gerência de Tecnologia da Informação – GTI;
• No ambiente Web da FURJ e suas mantidas deve ser disponibilizado apenas conteúdo institucional;
• O usuário não deve alterar a configuração do navegador da sua máquina no que diz respeito aos parâmetros de segurança e conexão. Havendo necessidade, a GTI deve ser acionada para informar o procedimento a ser seguido.
• Quando estiver acessando a Internet, o usuário não deve acessar sites ou executar ações que possam violar direitos autorais, marcas, licença de software ou patentes existentes.
• Nenhum material ofensivo ou hostil pode ser disponibilizado nos sites da FURJ e suas mantidas, ou em suas redes sociais oficiais;

• É proibido o acesso a sites de conteúdo pornográfico ou relacionados a sexo, bem como a distribuição, interna ou externa, de qualquer tipo de conteúdo proveniente destes sites, e ainda, que defendam atividades ilegais ou que menosprezem, depreciem e incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, religião, nacionalidade ou pessoas com deficiência.

4.3 - Rede Wi-Fi

A FURJ/Univille disponibiliza acesso à internet via rede Wi-Fi aos seus usuários, os quais devem utilizar de forma consciente e racional, respeitando a legislação em vigor e as normativas institucionais. Para empregados e estudantes:

✓ É permitido o acesso à rede WI-FI através da rede UNIVILLE;
✓ Todo o log de acesso é registrado e salvo em servidor;
✓ O acesso está condicionado às credenciais (matrícula e senha do domínio @univille.br);
✓ É permitido o cadastro e uso simultâneo de até cinco dispositivos por usuário.

› **Aos visitantes e terceiros, será permitido o acesso à rede WI-FI através da rede VISITANTES (rede aberta/pública).**

4.4 - Senha de Acesso

As senhas de acesso para autenticações, como, mas não se limitando a e-mail, teams, computador, devem ser de conhecimento apenas do usuário responsável pela identificação. O usuário não deve compartilhar ou comunicar a sua senha a outra pessoa e deve utilizar memorização para garantir o sigilo da senha.

Ninguém, independentemente do nível hierárquico e da área funcional, tem o direito de solicitar, conhecer ou utilizar a senha de outro usuário, nem mesmo na condição de gestor;

Quando do uso da senha de autenticação, o usuário deve escolher uma sequência de caracteres não óbvios, que não tenham relação direta com o usuário ou familiares e de difícil adivinhação por outra pessoa. Deve-se evitar o uso de nomes de pessoas, datas, nomes diversos (time de futebol, empresas, etc).

A senha deve ser uma sequência de caracteres fácil de ser lembrada pelo usuário e difícil de ser imaginada por outra pessoa. Evite palavras existentes em dicionários, nomes, datas de aniversário e de preferência a caracteres especiais (%, #, &, @, outros), pois, melhora a qualidade da sequência escolhida para a senha. Recomenda-se para uma senha mais forte o uso de todas as opções disponíveis, como letras maiúsculas, minúsculas, números e símbolos.

Altere a sua senha de acesso, no mínimo, uma vez ao ano, sendo possível aterá-la em qualquer estação de trabalho da Univille apertando as teclas CTRL+ALT+DEL e escolhendo a opção “Alterar uma senha”.

4.5 - Armazenamento de Dados e Informações

Todos os usuários, ao armazenar dados e informações, devem seguir as seguintes recomendações:

› **Não utilize dispositivos particulares, por exemplo tablets, notebooks, celular, pendrive, como fonte primária para armazenamento de dados, sejam pessoais ou institucionais.** Todos os dados e informações pertencentes, ou sob a responsabilidade da FURJ e suas mantidas, devem ser tratados em ambientes seguros, indicados pela GTI

› Não armazene, mesmo que temporariamente, arquivos que contenham dados e informações confidenciais, sejam institucionais ou pessoais, em pastas públicas ou compartilhadas, sem autorização do seu gestor.

› O acesso às pastas de trabalho das áreas internas, sites, times do SharePoint ou Teams, está condicionado ao nível de autorização de seus membros, que devem ser autorizados por seus gestores ou criadores. Cabe aos gestores da FURJ e suas mantidas, gerenciar, além do acesso a estas pastas, as permissões de cada membro, como direito a escrita, compartilhamento, alteração de permissões, exclusão de dados, administração, dentre outros.

› O OneDrive é uma plataforma para armazenamento de dados disponibilizada pela FURJ e suas mantidas para todos os seus usuários licenciados. Empregados devem utilizar o SharePoint para compartilhamento de informações institucionais. Em caso de dúvida, os usuários licenciados da FURJ e suas mantidas devem procurar a GTI sempre que acharem necessário para esclarecimento.

4.6 - Dispositivos Removíveis de Armazenamento de Dados

Tendo em vista que os computadores disponibilizados nas salas de aula pertencem a uma rede logicamente independente da administrativa, os docentes, para realização da aula e, os discentes, quando da apresentação de trabalhos, poderão utilizar dispositivo externo removível (pendrive, por exemplo) para não terem prejuízos pedagógicos e/ou acadêmicos.

Recomenda-se não inserir dispositivos de armazenamento removíveis, como pendrive ou cartão de memória, de origem desconhecida, em seu equipamento de trabalho. Estes dispositivos podem conter vírus ou malwares que têm a capacidade de se replicar pela rede local, causando perda ou roubo de dados e informações, além de outras ações maliciosas, como roubo de credenciais de acesso ou perda de integridade em documentos.

Remova o dispositivo imediatamente caso o antivírus detecte alguma ameaça;

5 - Trabalho Remoto

É permitido o acesso remoto aos servidores internos aos empregados e terceirizados desde que autorizados pelo gestor responsável. A conexão deve ser autenticada e necessita da instalação de um cliente VPN (Rede Privada Virtual) no computador. A liberação deste serviço deve ser solicitada via abertura de um chamado técnico (ticket) encaminhado para a GTI. Além de servidores, também é possível aos empregados o acesso remoto à sua máquina local dentro da FURJ/Univille.

É necessária a instalação de software antivírus devidamente atualizado, no computador do empregado ou terceiro que necessite realizar o acesso remoto à rede da Univille via VPN.

6 - Restrições Sobre o Uso e Instalação de Software

O uso de softwares nos equipamentos da FURJ e suas mantidas devem respeitar as seguintes orientações:

- Deverão ser homologados pela GTI;
- Deverão estar legalmente licenciados;
- Todas as compras de software devem ter projeto de investimento, com parecer técnico da GTI;
- Quando da necessidade de se instalar programa a partir da Internet o usuário deve contatar a GTI para a aprovação dessa necessidade e realização dessa instalação;
- Os softwares instalados nos equipamentos pela GTI não podem ser removidos ou alterados pelo usuário;
- Toda a documentação de licença ou equivalente deve permanecer na GTI;
- Não é permitida a instalação e/ou uso de software que não esteja relacionado as atividades da FURJ e suas mantidas;
- A GTI não prestará suporte em equipamentos pessoais, seja de empregados, terceiros ou clientes.

› **Na dúvida consulte a GTI.**

7 - Controle de Acesso

Os gestores são responsáveis pela autorização de acesso ao ambiente computacional de seus subordinados e deverão levar em conta a confidencialidade das informações disponibilizadas e a necessidade de acesso. Além disso, o gestor é responsável pelo uso dos sistemas e serviços de informação (ou parte deles) que possibilitam a realização das atividades Institucionais, administrativas e/ou de apoio. O gestor é a pessoa que garante para a FURJ que o usuário está exercendo normalmente as suas atividades profissionais, competindo-lhe.

✓ Autorizar ou Negar o acesso do usuário à informação, considerando:
- a real necessidade de acesso pelo usuário;
- a confidencialidade da informação;
- o tipo de acesso (leitura, alteração, remoção) a ser autorizado.
- **Revisar mensalmente as autorizações de acesso de seus subordinados ou terceiros;**
- **Solicitar ou realizar o cancelamento do acesso de usuários aos recursos computacionais sob sua responsabilidade;**
- Validar a eventual necessidade de armazenamento de dados pessoais nos sistemas e serviços sob sua responsabilidade;
- Definir e informar à GTI o grau de confidencialidade e disponibilidade das informações sob a sua guarda;
- Definir a necessidade de cópias de segurança e validar as soluções implementadas pela GTI;
- Validar as soluções para situações de desastre e de contingência implementadas pela GTI.

Por sua vez, compete ao usuário em relação ao controle de acesso:

› Solicitar acesso apenas para as informações que vai utilizar nas suas atividades profissionais na FURJ ou suas mantidas;
› **Solicitar ao gestor a alteração das permissões de acesso aos sistemas computacionais, quando suas atividades profissionais na FURJ e suas mantidas não mais exigirem este acesso.**

8 - Classificação da Informação

Em relação a confidencialidade das informações (documentos e e-mail), os níveis de classificação podem ser:
I - Pública: se aplica, normalmente, às informações corporativas da FURJ e suas mantidas que podem ser divulgadas para qualquer pessoa, física ou jurídica.
II - Interna: Indica que a informação somente deve ser acessada por usuários internos da FURJ ou suas mantidas, ou de usuários externos devidamente explicitados na mensagem ou autorizados no documento/compartilhamento. Se aplica normalmente a informações que não possuem segredo, sigilo ou que não comprometem a imagem da instituição.
III - Confidencial: indica que a informação tem forte restrição de uso e um nível de confidencialidade maior que Interna e somente pode ser acessada por destinatários especificados e autorizados pelo emissor. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) às atividades da FURJ e suas mantidas, podendo o divulgador incorrer em ilícito e passível de sanção administrativa.
IV - Restrita-Outlook: indica que a mensagem e seus anexos só poderão ser acessados pelos destinatários da mensagem. Além disso, neste nível de classificação, a mensagem é enviada de forma criptografada. A divulgação não autorizada dessa informação pode causar sérios danos as atividades e/ou comprometer a estratégia de negócio da FURJ e suas mantidas, podendo o divulgador incorrer em ilícito e passível de sanção administrativa.

Também é possível classificar documentos salvos no SharePoint, ou na pasta pessoal de cada usuário no Onedrive. Porém, neste caso, a classificação possui apenas os níveis: Pública, Interna e Confidencial. Detalhes como marca d'agua, informações de cabeçalho e rodapé contendo o nível da classificação serão adicionados automaticamente ao documento.

O encarregado de dados está à disposição para esclarecer as dúvidas em relação a confidencialidade das informações.

9 - Tratamento de Dados Pessoais

É 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.

Apenas os dados pessoais necessários para o cumprimento de obrigações regulatórias devem ser tratados depois que a finalidade para o qual foram coletados terminar.

Todo usuário, seja empregado, terceiro ou estudante, não deve tratar dados pessoais que não sejam relevantes à condução de suas atividades. Aquele que tomar conhecimento de dados pessoais que não sejam relevantes a sua atividade laboral ou a seus propósitos específicos, deverá abster-se de fazer o tratamento.

Dados pessoais em posse da FURJ ou suas mantidas devem ser considerados confidenciais e sigilosos e não podem ser tratados para situações incompatíveis com os objetivos para os quais foram recebidos, a não ser que os indivíduos afetados sejam adequadamente consultados, com autorização na forma de Termo de Consentimento.

A FURJ possui um profissional responsável pelo tratamento de dados pessoais. Trata-se do Encarregado de dados e suas atividades consistem em:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - responder, formalmente, toda e qualquer solicitação pertinente a dados pessoais deliberada pelo Comitê de Gestão de Segurança da Informação e Proteção de Dados da FURJ;

III - receber comunicações da Autoridade Nacional de Proteção de Dados e adotar providências de acordo com a Instrução Normativa de Segurança da Informação e Proteção de Dados;

IV - orientar os funcionários e os contratados da FURJ a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

V - executar atribuições determinadas pela Presidência da FURJ ou estabelecidas em normas pertinentes à matéria.

› **O encarregado pode ser contatado pelo e-mail encarregado@univille.br.**

10 - Armazenamento de Dados Institucionais e Cópias de Segurança (backup)

A Gerência de Tecnologia da Informação não realiza backup de informações salvas em ativos computacionais como, por exemplo, desktops, notebooks, smartphones ou tablets. Sendo assim, documentos institucionais importantes devem sempre ser salvos no SharePoint de cada grupo, ou no Onedrive pessoal do usuário, quando se tratar de um documento pessoal.

Arquivos armazenados tanto no SharePoint quanto no Onedrive possuem controle de versão, ou seja, é possível restaurar uma versão anterior do arquivo quando necessário. Este controle de versão é possível apenas no ambiente web das plataformas. Ainda, no ambiente web, também é possível acessar a lixeira de documentos, onde documentos excluídos são mantidos por até 30 (trinta) dias após sua exclusão.

É dever de todos os usuários verificar periodicamente a integridade dos dados tratados sob sua responsabilidade que estão armazenados no SharePoint e Onedrive.

11 - Segurança Física e do Ambiente

É responsabilidade de todos os usuários manter o ambiente de trabalho e estudo seguro. Todos podem sugerir à Gerência de Tecnologia de Informação ou à Pró-Reitoria de Infraestrutura a criação de barreiras que dificultem o acesso físico não autorizado. Ainda, a integridade física dos ocupantes de determinadas áreas também deve ser informada, caso se perceba que o ambiente frequentado ofereça algum risco.

De toda forma, em relação ao uso dos recursos computacionais nos ambientes físicos, também é importante que medidas simples de segurança sejam aplicadas pelos próprios usuários. Por exemplo, trancar a sala ou ambiente de trabalho ao se ausentar, caso esteja sozinho na sala e ainda a execução da Tela Limpa e Mesa Limpa, sendo:

I - Tela Limpa: o usuário deve bloquear o seu computador quando não estiver em uso, ou quando deixa seu ambiente de trabalho, seja por curto período ou final do expediente.

II - Mesa Limpa: não é permitido armazenar informações confidenciais, como documentos sigilosos ou a senha de acesso, sobre a mesa.

› As senhas de acesso devem ser armazenadas na memória e nunca em papel, agenda, post-its, etc;

› Documentos sigilosos devem ser trancados com chave ou algum tipo de senha, como em um armário ou cofre, por exemplo e, documentos com informações confidenciais, quando impressos em impressoras coletivas, devem ser retirados imediatamente.

12 - Das Sanções estabelecidas na LGPD e as Sanções possíveis de serem aplicadas aos empregados e alunos

A LGPD traz em seu texto de forma explícita algumas sanções que podem ser aplicadas para quem descumprir a legislação e, pela importância transcreve-se o artigo 52 para conhecimento:

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
I - advertência, com indicação de prazo para adoção de medidas corretivas;
II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
III - multa diária, observado o limite total a que se refere o inciso II;
IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
V - **bloqueio dos dados pessoais** a que se refere a infração até a sua regularização;
VI - eliminação dos dados pessoais a que se refere a infração;
VII - (VETADO);
VIII - (VETADO);
IX - (VETADO);
X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019);
XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019);
XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Estas sanções são passíveis de serem aplicadas as empresas que descumprirem a legislação pertinente a Proteção de Dados, porém, o empregado da FURJ ou suas mantidas deve ter plena ciência que **para quem descumprir as orientações postas nas Normas Internas sobre proteção de dados e LGPD e no presente Manual, estará**

sujeito as sanções possíveis de serem aplicadas pela CLT – Consolidação das Leis Trabalhistas e em regulamentação interna, conforme disposto nas Resoluções que "instituíram o regime disciplinar para os empregados da FURJ".

A cultura de proteção de dados e da segurança da informação deve permear todos os atos e atividades realizadas pelos empregados da FURJ ou suas mantidas a fim de garantir que nenhuma irregularidade aconteça com os dados tratados pela Instituição.

Os estudantes de qualquer curso e nível de ensino regularmente matriculado na Univille, nos colégios, nos cursos de graduação (presencial e EaD), Especialização, pós-graduação *stricto sensu* e extensão, que ao tratarem dados pessoais pela Instituição ou não, no ambiente escolar/universitário e, cometerem ilícitos ou desrespeito em relação a LGPD responderão na forma do Regimento da Univille.

13 - Dos trabalhos de ensino, pesquisa e extensão realizados por Docentes e Discentes da Univille que tratam dados pessoais

O tripé da Universidade é balizado no Ensino, na Pesquisa e na Extensão e, por isso, ao longo de um período letivo vários trabalhos de graduação, de projetos de extensão ou de Pesquisa Institucional e/ou de cursos de pós-graduação lato sensu necessitam tratar dados pessoais dos mais variados titulares.

Dessa forma, visando resguardar os direitos dos titulares dos dados, é necessário que todos os empregados da FURJ sigam as seguintes recomendações quanto ao tratamento de dados pessoais a serem utilizados em trabalhos e/ou pesquisas:

I – Em caso de dúvidas, consultar o encarregado de dados da FURJ através do e-mail: encarregado@univille.br. Nunca fornecer dados solicitados pelo requerente antes da resposta do encarregado. Após a aprovação, seguir as orientações para o tratamento adequado e legal dos dados pessoais envolvidos na pesquisa;

IV – Primar para que toda as ações sejam realizadas pela área a que o docente esteja vinculado;

V – Exigir que as pessoas que irão tratar os dados na pesquisa (docentes, acadêmicos, estagiários, voluntários) assinem o Termo de Compromisso e Confidencialidade para com os dados que irão tratar;

VI – Sempre que possível, tratar os dados de forma anonimizada, ou seja, sem identificar o titular;

VII – Fiscalizar a forma com que os dados serão tratados para evitar que sejam subtraídos por terceiros;

VIII – Quando o titular do dado pessoal tiver vínculo com a FURJ ou suas mantidas, evitar a coleta de dados que já estejam no RM (CPF, RG, endereço etc.);
IX – Eliminar de forma segura todos os dados após "verificação de que a finalidade foi alcançada ou que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada".
X - Toda mensagem de solicitação de participação em pesquisas, trabalhos acadêmicos ou questionários, que se pretenda realizar por estudantes ou empregados da FURJ, deverá ser enviada através do e-mail institucional (@univille.br), com expressa menção no corpo do e-mail de que a participação é voluntária, não havendo nenhum prejuízo pela não participação.

Conforme o artigo 7º. da LGPD, existem 10 hipóteses para o tratamento de dados pessoais, sendo que três se enquadram na modalidade deste capítulo. Abaixo as hipóteses e seus respectivos incisos:
I – mediante o fornecimento de consentimento pelo titular;
IV – para a realização de estudos por órgãos de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.
Exceto para pesquisas que tratem dados pessoais anonimizados, deve ficar claro ao titular como seus dados pessoais serão tratados, quem terá acesso a estes dados e onde e por quanto tempo serão armazenados.

14 - Dos direitos dos titulares dos dados

A lei tratou de forma expressa os direitos dos titulares dos dados definindo que o titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
I - confirmação da existência de tratamento;
II - acesso aos dados;
III - correção de dados incompletos, inexatos ou desatualizados;
IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei (Lei 13.709/2018);
VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

Merece aqui especial atenção ao que estabelece o inciso VI que trata da eliminação dos dados pessoais quando requerido pelo titular do mesmo, pois, a Instituição, por ser voltada ao ensino, pesquisa e extensão está enquadrada no inciso I, do artigo 16 da LGPD uma vez que há a obrigatoriedade de "cumprimento de obrigação legal ou regulatória", por ente municipal, estadual e federal.

15 - Do descarte de documentos físicos que contenham dados, fotos, documentos pessoais ou que possam identificar pessoa

Para que a eliminação de documentos, produzidos ou recebidos, tenha respaldo legal é necessária a análise dos documentos. Na Univille essa análise é feita pela Gestão Documental em conjunto com o setor e área responsável pela produção da documentação, obedecendo a legislação pertinente, a missão e visão da Instituição e ainda a Tabela de Temporalidade de Documentos, instituída pela Portaria n° 92 de 2011 do Ministério da Justiça.

Para solicitar orientação e suporte sobre a documentação a ser eliminada, deverá ser aberto um ticket para a Gestão Documental. A área solicitante deverá arquivar os documentos de maneira a que não possam ser manuseados por terceiros que não mantenham relação de trabalho com a respectiva área, até que a Gestão Documental realize uma análise e emita um parecer. Por fim, será elaborado um termo de eliminação que deverá ser assinado pelos responsáveis e ficará sob a guarda da área de Gestão Documental.

Fica vedado o descarte de documentos por qualquer setor da FURJ e suas mantidas que possam conter informações sobre dados pessoais, fotos ou documentos que possam identificar o titular do dado sem análise prévia da Gestão Documental. Em nenhuma hipótese poderá ocorrer o descarte desse tipo de documento no lixo comum, mesmo que seja em área de lixo reciclável.

16 - Disposições Gerais

Além de todas as orientações e procedimentos contidos no presente Manual, **recomenda-se a todos** a fim de evitar ou minimizar problemas em relação ao tratamento de dados pessoais e a Legislação específica:

I – Não tratar dados desnecessariamente;
II – Coletar apenas os dados que realmente sejam necessários para a atividade a ser realizada;
III – O RM armazena os dados pessoais dos titulares que possuem ou que possuíram um vínculo com a Instituição, portando, para esta categoria de titulares, é desnecessária uma nova coleta de dados pessoais;
IV – Orienta-se aos setores reverem seus requerimentos internos para os alunos/acadêmicos/empregados da FURJ, visando não coletar desnecessariamente dados que já estejam na posse da FURJ ou suas mantidas;
V – Não deixar documentos físicos que contenham dados pessoais em qualquer lugar do setor para que não possam ser utilizados para fins ilícitos;
VI – A LGPD não revogou nenhuma outra legislação específica, relacionada a área educacional ou de órgão regulador/fiscalizador, bem como do consumidor;
VII– Na dúvida, consulte o encarregado de dados. Ele estará sempre à disposição para esclarecimentos.

A Presidência da FURJ e a Reitoria da Univille envidarão todos os esforços na continua busca de aprimoramento dos procedimentos a fim de cumprir com o disposto na legislação e em relação as normas emanadas pela ANPD, visando sempre evitar problemas com os dados pessoais dos titulares que estejam sob a guarda da Instituição.

O aprimoramento dos procedimentos operacionais em relação ao tratamento, guarda, sigilo e confidencialidade dos dados pessoais e a segurança da informação **depende de todos.**

A qualquer momento as orientações do presente manual podem sofrer alterações, **sendo responsabilidade de todos os usuários acompanhar a versão atualizada no link http://univille.edu.br/lgpd.**