UNICAMP

INSTRUÇÃO NORMATIVA CGU Nº 02/2021

Estabelece procedimentos para implementação de medidas de segurança, técnicas e administrativas para proteger os dados pessoais no âmbito da Unicamp, desde a fase de concepção do produto ou serviço, até a sua execução.

A Coordenadoria Geral de Universidade no uso de suas atribuições, considerando:

I. O artigo 46 da Lei Geral de Proteção de Dados Pessoais - LGPD, Lei nº 13.709, de 14 de agosto de 2018;

Resolve:

Artigo 1º - Estabelecer procedimentos para implementação de medidas de segurança, técnicas e administrativas, para proteger os dados pessoais de situações ilícitas ou acidentais, que possam resultar em acesso não autorizado, destruição, perda ou compartilhamento indevido, desde a concepção do processo de trabalho, sistema, produto ou serviço, até a sua execução.

Artigo 2º - Para fins desta Instrução Normativa, considera-se

§ 1º Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

§ 2º Classificação: atribuição de graus de sigilo, conforme legislação - no caso, a Lei Geral de Proteção de Dados - a documentos ou às informações neles contidas.

§ 3º Titular: pessoa natural a quem se referem os dados pessoais, que são objeto de tratamento.

§ 4º Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

§ 5º 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.

§ 6º Consentimento: manifestação livre, informada e inequívoca, pela qual o titular concorda com o tratamento de seus dados pessoais, para uma finalidade determinada;

§ 7º Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, retenção (arquivamento e/ou armazenamento), eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

§ 8º Retenção: ação de manter ou conservar dados coletados e/ou arquivar documentos em repositórios, base de dados, sistemas e/ou arquivos físicos.

Artigo 3º - Todas as atividades de tratamento de dados pessoais, no âmbito da Universidade Estadual de Campinas, deverão observar os princípios da Lei Geral de Proteção de dados (artigo 6º): finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas, durante todo o ciclo de vida do tratamento de dados pessoais.

Artigo 4º - Sistemas, processos ou infraestruturas que fazem tratamento de dados pessoais devem ser projetados, de forma a antecipar possíveis riscos à privacidade e incorporar medidas proativas, que neutralizem ou minimizem os riscos.

Artigo 5º - Aplicativos, sistemas, produtos e serviços devem aplicar, automaticamente, as configurações de proteção de dados e exigir a intervenção humana para alterá-los.

Artigo 6º - A privacidade deve ser incorporada ao projeto de sistemas, aplicativos, produtos e serviços, isto é, deve ser um dos requisitos não funcionais e fazer parte desde a concepção do projeto.

Artigo 7º - Novos projetos de processos de trabalho, produtos, serviços ou sistemas deverão realizar a Avaliação de Impacto à Proteção de Dados com a elaboração do Relatório de Impacto à Proteção de Dados - RIPD.

Artigo 8º - As funcionalidades do sistema devem estar em conformidade com a privacidade e atender o objetivo estabelecido.

Artigo 9º - As medidas de segurança devem ser adotadas desde o momento do projeto do sistema e ao longo de todo o ciclo de vida do dado (coleta, registro, classificação, conservação, consulta, distribuição, limitação, eliminação, etc).

Artigo 10 - Os sites da Unicamp devem disponibilizar link para a Política de Privacidade e disponibilizar informações claras, específicas e objetivas sobre as finalidades dos tratamentos de dados pessoais, para os titulares.

Artigo 11 - A concepção dos processos de trabalho deve ser centrada no usuário, de forma a antecipar suas necessidades, para que qualquer procedimento adotado seja realizado, no sentido de garantir a sua privacidade e em consonância com os objetivos institucionais.

Artigo 12 - Os processos de trabalho, serviços, produtos e sistemas devem adotar estratégias de minimização dos dados pessoais, limitação do acesso, limitação dos detalhes de coleta, classificação, retenção limitada ao período de tratamento, promoção da transparência, estruturação dos direitos do titular, aplicação da estrutura que fortaleça a cultura de privacidade e demonstração de conformidade.

Artigo 13 - Os dirigentes dos órgãos devem dar conhecimento da presente instrução normativa a todos os servidores e notificar o Encarregado sobre o cumprimento dos procedimentos.

Artigo 14 - Os servidores responsáveis ou envolvidos em processos de trabalho, com tratamentos de dados pessoais, devem observar os procedimentos acima descritos.

Artigo 15 - O Encarregado deve orientar os dirigentes e servidores sobre os procedimentos necessários e monitorar as evidências de seu cumprimento.

Artigo 16 - O Comitê Gestor de Proteção e Privacidade de Dados prestará esclarecimentos, a respeito da aplicação desta Instrução Normativa.

Artigo 17 - A inobservância ao que está estabelecido nesta Instrução Normativa poderá acarretar a interrupção do processo de trabalho, até a sua adequação.

Esta Instrução Normativa entra em vigor a partir da data de sua publicação.

Cidade Universitária “Zeferino Vaz”
Em 22 de dezembro de 2021

Prof. Dr. Ricardo Dahab
Diretor Geral de Tecnologia da Informação e Comunicação
Coordenadoria Geral da Universidade - CGU

Cartilha sobre Privacidade desde a Concepção e por Padrão

1. Privacidade desde a concepção

1.1 Conceito

O conceito de privacidade desde a concepção vem sendo trabalhado há mais de 20 (vinte) anos e foi aceito, internacionalmente, com a adoção da Resolução sobre Privacidade desde a Concepção[1], realizada em Jerusalém, em 2010. Esta resolução reconhece a privacidade desde a concepção como componente essencial à privacidade, incentiva a adoção dos Princípios Fundamentais, conforme definido por Ann Cavoukian[2] e incentiva as Autoridades de Proteção de Dados a promover a cultura de privacidade desde a concepção.

A Lei Geral de Proteção de Dados, no artigo 46, §2º define que as medidas de segurança, técnicas e administrativas, deverão ser observadas desde a fase de concepção do produto ou serviço. Dessa forma, a privacidade desde a concepção é um dos requisitos estabelecidos pela LGPD.

A privacidade desde a concepção caracteriza-se por ter como foco a gestão de risco e estratégias, que assegurem a privacidade ao longo do ciclo de vida do processo, sistema, produto ou serviço. Para além das fases iniciais do projeto, a privacidade desde a concepção deve levar em consideração todos os processos e práticas que processam dados associados, alcançando assim, uma verdadeira governança de gestão de dados pessoais.

1.2. Princípios

A privacidade desde a concepção fundamenta-se em sete princípios definidos por Ann Cavoukian:

1.2.1. Proativo não reativo; Preventivo, não corretivo

Sistemas, processos ou infraestruturas que fazem tratamento de dados pessoais devem ser projetados desde o início, de forma a antecipar possíveis riscos à privacidade e incorporar medidas proativas que neutralizem ou minimizem os riscos.

A prática deste princípio irá requerer atenção especial em alguns aspectos, como o comprometimento de toda a comunidade interna, desde a administração superior. Outro aspecto importante é desenvolver a cultura da privacidade, para que este princípio seja traduzido em ações práticas de melhoria contínua, em relação à proteção dos dados. Deve-se considerar também, que o desenvolvimento de métodos de análise, baseados em indicadores, poderá evidenciar processos, sistemas e infraestruturas com vulnerabilidades e que necessitem de adequações.

Figura 1: Ações necessárias para o Princípio 1. Proativo não reativo, Preventivo não corretivo

1.2.2. Privacidade como Configuração Padrão

A privacidade como configuração padrão consiste em fornecer os mais altos níveis de privacidade, por padrão nos sistemas e processos para os usuários. Dessa forma, aplicativos, sistemas, produtos e serviços devem aplicar automaticamente as configurações de proteção de dados e exigir a intervenção humana para alterá-los. Este princípio baseia-se na minimização dos dados ao longo do ciclo de vida.

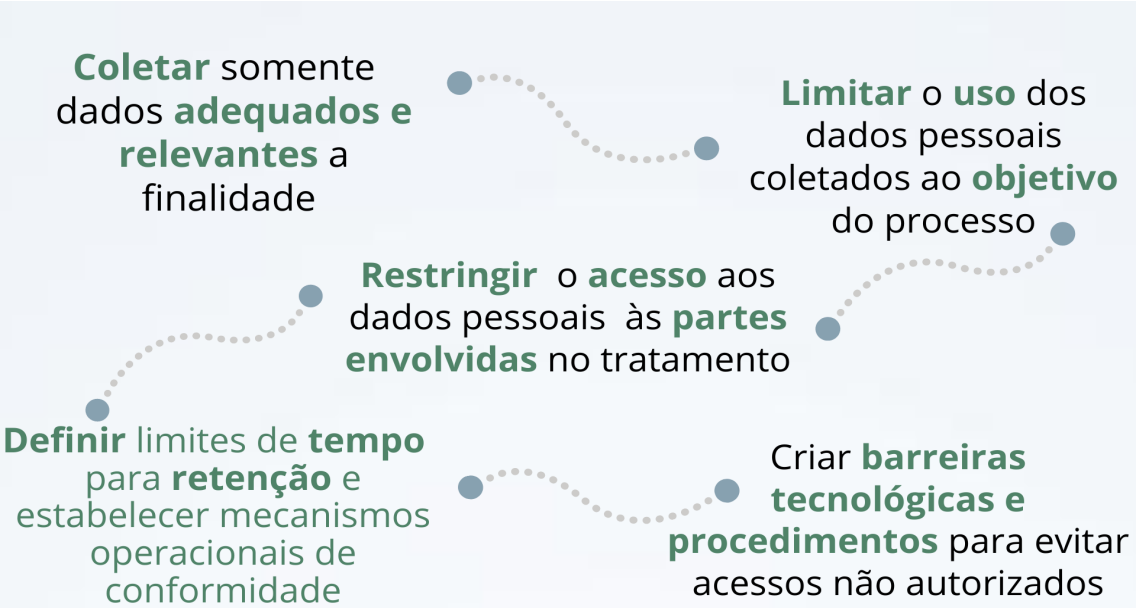

Figura 2: Ações recomendadas para a prática do princípio *Privacidade como configuração padrão*

É importante destacar que os sistemas devem ser configurados, de forma a restringir o acesso aos dados pessoais pelas partes efetivamente envolvidas no tratamento, aplicando o princípio da "*Necessidade de Saber".*

Além disso, os dados devem ser retidos somente pelo tempo necessário para o tratamento e nas exceções previstas na Lei: obrigação legal; estudos por órgãos de pesquisa e/ou uso exclusivo do controlador, desde que anonimizado.

1.2.3 Privacidade Incorporada ao Design

A privacidade deve ser incorporada aos projetos de sistemas, aplicativos, produtos e serviços. Ela deve ser um dos requisitos não funcionais e fazer parte desde a concepção do projeto. A privacidade não deve ser configurada como um módulo adicional, ou como uma camada posterior ao projeto.

Novos projetos devem considerar a privacidade como um requisito. Além disso, recomenda-se realizar a Avaliação de Impacto à Proteção de Dados, com a elaboração do Relatório de Impacto à Proteção de Dados - RIPD em todos os novos projetos.

Figura 3: Ações recomendadas para a prática do princípio *Privacidade incorporada ao design*

1.2.4 Funcionalidade total, soma positiva, não soma zero

Este princípio visa estabelecer o equilíbrio entre a finalidade do processo e a privacidade, ou seja, as funcionalidades do sistema devem estar em conformidade

com a privacidade e atender o objetivo estabelecido. Não se trata de uma dicotomia entre privacidade *versus* usabilidade ou necessidades do processo, mas uma nova abordagem que produza uma solução eficaz e eficiente, não somente em relação à privacidade, mas também para o interesse institucional.

Dentre as ações recomendadas estão a busca por novas soluções, que atendam as necessidades do processo e estejam em consonância com os requisitos de privacidade. Estabelecer canais de comunicação, para que os usuários possam colaborar na identificação de processos e sistemas, que não estão adequados, além de equilibrar, em conformidade, os interesses dos usuários e dos processos de trabalho.

1.2.5 Segurança de ponta a ponta: Proteção total do ciclo de vida

Este princípio refere-se à segurança desde o momento do projeto do sistema e ao longo de todo o ciclo de vida do dado (coleta, registro, classificação, conservação, consulta, distribuição, limitação, eliminação etc.).

A segurança da informação caracteriza-se pela confidencialidade, integridade, disponibilidade e resiliência dos sistemas de informação. Dentre as ações recomendadas estão: análise da possibilidade de pseudoanonimização ou anonimização dos dados, classificação e organização de dados e operações de tratamento, com base em perfis de acesso, análise da possibilidade de criptografia padrão e eliminação segura e efetiva dos dados pessoais ao final do ciclo de vida.

1.2.6. Visibilidade de transparência: mantenha aberto

Além de adotar medidas que viabilizem a proteção dos dados, deve-se demonstrar claramente, que as ações estão sendo executadas. A transparência em relação ao tratamento de dados pessoais é uma exigência legal e promove a confiabilidade, em relação aos titulares dos dados.

Para promover a transparência, recomenda-se as seguintes ações:

- Divulgar a Política de Privacidade (Deliberação CAD - A - 003/2020);
- Elaborar e publicar informações claras, específicas e objetivas sobre os processos de tratamento de dados pessoais para os titulares.

1.2.7. Respeito pela Privacidade do Usuário: mantenha-o centrado no usuário

A concepção dos processos de trabalho deve ser centrada no usuário, de forma a antecipar suas necessidades, para que qualquer procedimento adotado seja realizado, no sentido de garantir a sua privacidade, mas sem esquecer os objetivos institucionais.

Projetos de processos, aplicativos, produtos e serviços que têm como foco garantir a privacidade dos titulares dos dados envolvem:

• Implementar configurações de privacidade que são "robustas" por padrão e onde os usuários são informados das consequências para a sua privacidade, quando parâmetros estabelecidos são modificados;

• Disponibilizar informações completas e adequadas que conduzam a um consentimento informado, livre, específico e inequívoco, que deve ser explícito em todos os casos que o exijam;

• Fornecer aos titulares dos dados o acesso aos seus dados e as informações detalhadas, sobre as metas de processamento e comunicações realizadas;

• Implementar mecanismos eficientes e eficazes, que permitam aos titulares dos dados exercer os seus direitos em matéria de proteção de dados.

2. Estratégias de Privacidade na Modelagem de Projetos

Hoepman[3] identifica oito estratégias de privacidade desde a concepção:

1. Minimizar
2. Limitar o acesso
3. Separar
4. Resumir
5. Informar
6. Controlar
7. Aplicar
8. Demonstrar

Tais estratégias podem ser divididas em duas categorias: estratégias de privacidade relacionadas a dados e estratégias de privacidade relacionadas a processos.

Figura 4: Estratégias de privacidade na modelagem de projetos

As estratégias de privacidade, relacionadas a dados, referem-se aos procedimentos no tratamento de dados pessoais. As estratégias relacionadas a processos referem-se à definição organizacional para a gestão responsável.

Embora, dependendo do contexto, certas estratégias possam ser mais aplicáveis do que outras, dentro do quadro de desenvolvimento de um sistema, essas oito estratégias, consideradas a partir dos estágios iniciais de desenvolvimento e análise de conceito e aplicadas em conjunto, permitem a inclusão de salvaguardas e medidas de proteção, nas operações de tratamento de dados pessoais e procedimentos, tornando possível que os resultados finais levem em consideração os requisitos de privacidade.

1. Minimizar	
O que é?	Coletar e tratar a menor quantidade de dados pessoais possível
Para que?	Evitar o tratamento de dados desnecessários e limitar possíveis riscos
Como?	- Selecione somente dados relevantes para a coleta e tratamento - Exclua da coleta e tratamento os dados que não sejam absolutamente necessários para o objetivo necessário - Apague completamente os dados assim que deixarem de ser relevantes conforme a tabela de temporalidade do processo

2. Limitar o Acesso	
O que é?	Limitar a observabilidade dos dados estabelecendo os meios necessários para controlar a abrangência de acessos.
Para que?	Garantir a confidencialidade dos dados
Como?	- Restringir o acesso a dados pessoais conforme a "necessidade de saber" considerando os tipos de dados e etapas de tratamento; - Quando possível, torne os dados ininteligíveis para pessoas não-autorizadas

3. Separar	
O que é?	Manter contextos de tratamento independentes
Para que?	Minimizar o risco de que, durante o tratamento, diferentes dados pessoais do mesmo indivíduo que são usados em processos independentes, possam ser combinados para criar um perfil completo
Como?	- Isolar: coletar e armazenar dados pessoais em diferentes bancos de dados ou aplicativos que são independentes; - **distribuir** a coleta e tratamento de diferentes subconjuntos de dados pessoais.

4. Resumir	
O que é?	Limitar os detalhes dos dados pessoais coletados
Para que?	Limitar possíveis riscos
Como?	- Generalizar os valores dos atributos usando intervalos de valores em substituição a um campo de valor definido; - Agregar informações em categorias em substituição a utilizar informações detalhadas

5. Promover a Transparência	
O que é?	Dar ciência aos titulares sobre o tratamento dos dados pessoais
Para que?	Cumprir o princípio da transparência
Como?	- Fornecer todas as informações exigidas pela LGPD - Explicar de forma concisa, transparente, inteligível, acessível e com linguagem clara e simples - Notificar dados de outras origens, compartilhamentos e violações

6. Controlar	
O que é?	Implementar mecanismos para que o titular exerça seus direitos
Para que?	Cumprir as exigências da LGPD
Como?	- Adquirir o consentimento em processos que não tenham outra base legal; - Notificar os titulares - Atualizar os dados por meio de mecanismos simplificados para os titulares;

7. Aplicar	
O que é?	Implementar uma estrutura que fortaleça a cultura da privacidade
Para que?	Cumprir as exigências da LGPD
Como?	- Criar um plano de treinamento e conscientização - Apoiar a política definida, estabelecendo procedimentos e implementar as medidas técnicas e organizacionais necessárias - Manter os procedimentos em conformidade com a política de privacidade

8. Demonstrar	
O que é?	Registrar as evidências das decisões sobre privacidade no tratamento de dados pessoais e documentação sobre gestão de dados pessoais na instituição
Para que?	Demonstrar que os requisitos legais estão sendo cumpridos
Como?	- Documentar todas as decisões relacionadas à privacidade - Auditar os processos que envolvam tratamento de dados pessoais - Elaborar os relatórios de impacto a proteção de dados

3. Considerações Finais

Considerando o contexto da instituição e os processos de trabalho, baseando-se no uso intensivo de dados pessoais e cujo impacto à privacidade é visivelmente fortalecido pela utilização de tecnologias disruptivas, é essencial a adoção de medidas técnicas e organizacionais eficientes e eficazes que assegurem a proteção e privacidade dos dados pessoais, durante seu tratamento.

Garantir a privacidade e estabelecer uma estrutura de governança não deve representar obstáculos à inovação. Pelo contrário, a privacidade e governança dos dados oferecem vantagens e oportunidades como:

- Para a instituição: otimizar processos proporcionando maior eficiência;
- Para a sociedade: acessar os serviços, beneficiando-se das tecnologias, sem comprometer a privacidade de suas informações.

A implementação eficiente e eficaz dos princípios de privacidade exige que eles sejam parte integrante da natureza dos produtos e serviços e, para isso, devem ser levados em consideração desde os estágios iniciais de desenvolvimento de conceito, modelagem e desenvolvimento.

A privacidade desde a concepção é obrigação legal do controlador e, como parte do cumprimento de seu dever, é necessário definir os requisitos continuamente; monitorar sua correta implementação e verificar sua plena operacionalidade, perante o sistema em produção, de modo que a privacidade dos indivíduos, cujos dados serão processados, seja garantida.

Referências

1. Resolution on Privacy by Design. 32nd International Conference of Data Protection and Privacy Commissioners. Jerusalem (Israel) 27-29/10/2010 https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolution_privacybydesign_en.pdf
2. Ann Cavoukian, Identity in the Information Society, Aug 2010, Volume 3, Issue 2, pp 247-251. Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D https://link.springer.com/content/pdf/10.1007%2Fs12394-010-0062-y.pdf
3. Jaap-Henk Hoepman. Privacy Design Strategies (The Little Blue Book), Mar 2019 https://www.cs.ru.nl/~jhh/publications/pdsbooklet.pdf

Documento assinado eletronicamente por **Ricardo Dahab**, **DIRETOR GERAL DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO**, em 22/12/2021, às 15:57 horas, conforme Art. 10 § 2º da MP 2.200/2001 e Art. 1º da Resolução GR 54/2017.

A autenticidade do documento pode ser conferida no site: sigad.unicamp.br/verifica, informando o código verificador: **8CD23308 6BEC4B8A 972E06CB 05AC2C6B**

UNICAMP
SIGAD