UNIVERSIDADE FEDERAL DO CEARÁ

PLANO DE ADEQUAÇÃO DA UFC À LGPD

CPPDP Comitê de Privacidade e Proteção de Dados Pessoais

CISI *Coordenadoria de Infraestrutura e Segurança da Informação*

STI *Superintendência de Tecnologia da Informação*

VERSÃO

2.0

ORIGEM

Coordenadoria de Infraestrutura e Segurança da Informação – CISI

REFERÊNCIA NORMATIVA

Lei Federal nº 12.965 de 23 de abril de 2014 (Marco Civil da Internet)
Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei de Proteção de Dados Pessoais)
Guia Orientativo - Tratamento de Dados Pessoais pelo Poder Público. ANPD. Versão 1.0. jan/22.

CAMPO DE APLICAÇÃO

Este plano se aplica no âmbito da Universidade Federal do Ceará.

SUMÁRIO

1. INTRODUÇÃO

A Universidade Federal do Ceará vem buscando a conformidade com a Lei Nº 13.709, de 14 de Agosto de 2018, a Lei Geral de Proteção de Dados, para que seja possível realizar de maneira adequada o tratamento dos dados dos seus usuários. Para isso torna-se necessário o estabelecimento de um conjunto de ações que possam promover a adaptação da universidade a este normativo. É válido salientar que a UFC, como instituição de ensino superior, possui um conjunto de dados relativos a servidores, discentes e docentes. Nesse contexto, dada a natureza de pessoa jurídica de direito público, a UFC possui o dever de atender aos preceitos normativos no que se refere ao tratamento de dados pessoais, sejam eles digitais ou não. Dessa forma, a fim de tornar transparente à comunidade em geral acerca da execução das ações, torna-se relevante publicizá-las por meio deste plano.

Foi desenvolvido uma versão 1 deste plano de ações, contudo não foi possível avançar conforme o cronograma e às ações que haviam sido previstas, por isso a necessidade da reformulação desse plano e das estratégias para que se consiga de fato avançar com a adequação da UFC. Outro fator motivacional para elaboração de um novo plano são os resultados apresentados no Acórdão 1.384/2022-TCU-Plenário relativos à auditoria realizada pelo TCU entre novembro de 2020 e maio de 2021 para avaliar as ações governamentais e os riscos à proteção de dados pessoais por meio da elaboração de diagnóstico acerca dos controles implementados pelas organizações públicas federais. Conforme os resultados apresentados, foram identificados diversos pontos que precisam de avanços e portanto serão apontados nos objetivos e nas ações que serão abordadas neste novo plano.

2. OBJETIVOS

O Objetivo geral deste plano é realizar a adequação da LGPD à UFC, em seus processos e serviços, dando garantia aos titulares quanto à proteção e privacidade dos dados salvaguardados por esta instituição.

Além desse objetivo geral podemos citar como objetivos específicos:

- Desenvolver tecnologias e processos que garantam os direitos dos titulares de dados pessoais;
- Desenvolver plano de capacitação sobre privacidade e proteção de dados pessoais, para técnicos administrativos, discentes e docentes;
- Garantir ações de segurança da informação aos dados pessoais tratados pela UFC;
- Realizar o inventário de dados pessoais
- Adotar controles de segurança adequados para o tratamento dos dados;
- Adequar os processos e serviços seguindo boas práticas de minimização de dados pessoais, privacidade por padrão e privacidade desde a concepção;
- Produzir relatórios de Impacto e Proteção de Dados Pessoais;
- Estabelecer processo de comunicação de incidentes de segurança ou vazamento de dados pessoais.

3. PLANO DE AÇÃO

Dado esse contexto, é necessário primeiramente o estabelecimento de políticas que possam orientar e promover a transparência a respeito do que a universidade vem executando e do que busca executar em relação aos dados que são coletados, classificados, tratados e principalmente em relação a sua segurança. Para que seja possível realizar essa adequação foi elencado um conjunto de políticas que serão necessárias: Política de Classificação de Dados, Política de Proteção de Dados Pessoais, Política de Privacidade, Política de Tratamento de Incidentes.

Por outro lado, é preciso que seja executado um amplo trabalho dentro da UFC abrangendo todos os setores para identificar dentre eles quais os dados coletados e como eles estão sendo tratados. Para atender a esse objetivo será realizada de maneira in loco a aplicação do Questionário de Adequação (QA) buscando identificar o quão aderente aquele setor está aos normativos vigentes. Importante ressaltar que a partir desse questionário será possível a UFC responder com maior assertividade os levantamentos que são realizados pelo Tribunal de Contas da União sobre adequação à LGPD. Além desse questionário é fundamental que haja o levantamento de Inventário de Dados Pessoais (IDP) de cada um desses setores, dessa forma será possível uma junção de todas essas informações que irão compor um amplo inventário de dados utilizados pela universidade. De forma, similar é necessário, que também de maneira in loco, sejam desenvolvidos Relatórios de Impacto de Proteção de Dados (RIPD) para demonstrar como os dados pessoais são tratados, usados, compartilhados e quais medidas são adotadas para mitigação dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados.

Figura 1 - Estrutura do Plano de Ações

Fonte: Coordenadoria de Infraestrutura e Segurança da Informação

Como base para aplicação das Políticas que serão instrumentalizadas bem como o Questionário de Adequação, Inventário de Dados e o Relatório de Impacto de Proteção de dados é fundamental que seja desenvolvido um Plano de Capacitações dentro dessa temática para que a comunidade acadêmica possa, além de assimilar de maneira ampla os conceitos e definições que envolvem a LGPD, ter conhecimento a respeito dos documentos que precisarão ser desenvolvidos com cada unidade que realiza a gestão de dados. Na Figura 1 podemos ver como o Plano de Capacitação abrange todas as ações que serão desenvolvidas bem como as Políticas que serão desenvolvidas de maneira ampla para a Universidade servem como orientação base para as atividades que serão desenvolvidas de maneira individual em cada setor envolvido. A seguir iremos apresentar um descritivo a respeito do que se trata cada um desses artefatos e os elementos que os compõem.

3.1 Questionário de Adequação

Ocasionalmente, o Tribunal de Contas da União (TCU) realiza a verificação da conformidade da UFC em relação à LGPD. O questionário, em seu último ciclo, contemplou 60 questões que foram organizadas em duas perspectivas e nove dimensões. As questões tiveram como referência a própria LGPD e a norma técnica ABNT NBR ISO/IEC 27701:2019 (extensão das normas de segurança da informação ABNT NBR ISO/IEC 27.001 e ABNT NBR ISO/IEC 27.002 para gestão da privacidade da informação).

É importante mencionar que essa avaliação é realizada de maneira ampla na UFC, por isso torna-se necessário a avaliação individual de como é tratada a gestão de dados pessoais individualmente dentro de cada setor, para que assim possa ser construída uma resposta coletiva, concisa e com informações adequadas para a real situação da universidade em relação a este tema.

O Questionário de Adequação será uma ferramenta desenvolvida com base nesse questionário do TCU para captar as informações dos setores avaliados de maneira individual. Após a sua aplicação, haverá o trabalho de convergência de todas as informações levantadas nos mais diversos setores.

3.2 Inventário de Dados Pessoais

O Inventário de Dados Pessoais consiste no registro das atividades de tratamento de dados pessoais realizadas por uma instituição. Fundamentado no art. 37 da LGPD o IDP tem como objetivo mapear de maneira detalhada o ciclo de vida dos dados pessoais, desde a sua coleta até a conclusão do tratamento. O IDP deve conter informações sobre como os dados são coletados, utilizados e compartilhados, além de quem os manipula, por quanto tempo são retidos, sua previsão legal de uso, sua finalidade e as medidas de segurança adotadas para protegê-los de violações. Eventuais outros registros também podem ser necessários para que o IDP seja capaz de descrever as operações de tratamento de dados aplicadas por uma instituição.

A elaboração deste documento está em conformidade com a LGPD e corresponde a base fundamental para identificação de riscos e aprimoramento dos controles e procedimentos de proteção de dados pessoais. O IDP é um requisito para a preparação do

Relatório de Impacto de Proteção de Dados.

3.3 Relatório de Impacto de Proteção de Dados.

O tratamento de dados pessoais envolve riscos associados às liberdades civis e aos direitos fundamentais dos titulares, principalmente nos casos em que houver tratamento de dados sensíveis. Nesse cenário, a LGPD em seu art. 5º, inciso XVII regulamenta a implementação do Relatório de Impacto de Proteção de Dados (RIPD). De responsabilidade do controlador, este documento tem a função de descrever os processos de tratamento de dados e identificar e avaliar os riscos à privacidade dos titulares além das ações e os mecanismos necessários para mitigar esses riscos.

O RIPD deve conter, dentre outras informações: a descrição dos processos que possam gerar riscos, uma análise sobre a harmonia entre tratamento e finalidade, a identificação e avaliação de riscos e por fim a especificação de técnicas e métodos para assegurar a prevenção contra incidentes e proteção dos dados pessoais.

A elaboração do RIPD permite ainda à instituição avaliar a conformidade de seus processos de tratamento com a LGPD e consequentemente manifestar consonância ao princípio da prestação de contas, demonstrando medidas de gerenciamento de risco e garantias de segurança dos dados de titulares.

3.4 Política de Classificação de Dados.

Uma Política de Classificação de Dados é um documento que estabelece as regras para a classificação dos dados pessoais armazenados e tratados por uma organização. Sua importância no contexto da LGPD deriva da necessidade em garantir que os dados pessoais sejam tratados de forma adequada e segura, de acordo com as exigências legais.

A classificação de dados é um passo fundamental para a proteção de dados pessoais, pois permite identificar por exemplo quais informações são consideradas confidenciais, quais são sensíveis ou ainda se há classificação para dados de crianças e adolescentes, e portanto, precisam de medidas de segurança adicionais. Para este fim, a política precisa considerar os diferentes tipos de dados que a organização possui e qual o nível de proteção que eles requerem. Além disso, é importante garantir que a política seja de fácil entendimento para todos os usuários, incluindo funcionários, parceiros e terceiros, e que seja revisada e atualizada regularmente para se adequar às mudanças na tecnologia e nas leis.

3.5 Política de Proteção Dados

O direito à proteção dos dados pessoais é uma garantia fundamental expressa no Art. 5º da Constituição Federal de 1988 em seu inciso LXXIX e também assegurada pela LGPD. A proteção de dados pessoais se refere ao conjunto de medidas técnicas e administrativas aplicadas para garantir a segurança dos dados pessoais contra acessos não autorizados. Como mecanismo de proteção, a Política de Proteção de Dados estabelece regras e diretrizes basilares que devem ser adotadas pelas organizações para garantir a segurança

dos dados dos titulares.

Para ser eficaz, uma política de proteção deve ser escrita em linguagem clara e acessível, conter os direitos dos titulares e garantias de segurança contra acessos não autorizados. Além disso, deve incluir a finalidade de usos de seus dados, assim como a fundamentação legal para isso. Também é importante tratar de compartilhamento de dados, explicitar as responsabilidades de implementação e monitoramento das regras estabelecidas e, não obstante, manter-se atualizada.

3.6 Política de Privacidade

Previsto no art. 6 da LGPD, o princípio da transparência garante aos titulares acesso a informações claras sobre os procedimentos de tratamento realizados com seus dados pessoais, bem como sobre quem os realiza. A política de Privacidade é o documento necessário para adequação a esse princípio e sua importância se reflete na obrigação dos agentes de tratamento em garantir a transparência e a sua responsabilidade perante os titulares.

A política de privacidade deve ser elaborada em linguagem simples e acessível com informações precisas e completas sobre como os dados pessoais são tratados. Ela deve incluir um tópico de definições para ajudar os titulares a entender os termos utilizados ao longo do documento. Toda a política precisa estar em conformidade com a legislação e por esta razão é necessário apresentar um tópico contendo a base legal utilizada. Em seguida, deve trazer a identificação dos agentes de tratamento e incluir informações sobre como os titulares podem entrar em contato para exercitar seus direitos além de como essas solicitações serão tratadas. Os direitos dos titulares também devem estar elencados e as medidas adotadas pela organização para atendê-los. Conter o detalhamento de quais dados são coletados, como são coletados e para qual finalidade são utilizados, bem como as medidas de segurança praticadas para protegê-los. O compartilhamento de dados(inclusive internacionalmente), o uso de cookies e possível tratamento posterior precisam estar evidenciados quando ocorrerem. Informações de tratamento de dados sensíveis ou de crianças e adolescentes também precisam estar em um tópico destacado se forem realizados.

Por fim, a política de privacidade deve estar exposta em um local de fácil acesso e visualização para alcançar todos os titulares e conter informações sobre a periodicidade de revisão para garantir que esteja sempre atualizada conforme a legislação.

3.7 Política de Tratamento de Incidentes

A Política de Tratamento de Incidentes de Segurança é um conjunto de diretrizes que visa garantir a proteção das informações pessoais dos indivíduos, em caso de incidentes de segurança da informação, como vazamentos de dados, ataques cibernéticos, entre outros. Essa política é essencial para garantir a confidencialidade, integridade e disponibilidade dos dados pessoais, bem como garantir a conformidade com as regulamentações de privacidade da LGPD.

A importância deste documento reside no fato de que os incidentes de segurança podem causar, além das sanções legais, danos irreversíveis à reputação da organização e danos financeiros e emocionais aos indivíduos cujos dados foram expostos ou roubados. A

elaboração da política é, portanto, essencial para garantir a proteção dos dados pessoais e minimizar os riscos de segurança existentes.

A Política de Tratamento de Incidentes de Segurança define a criação de uma equipe especializada para tratar incidentes de segurança e estabelece ações e procedimentos formais para o tratamento desses incidentes, bem como procedimentos de notificação, planos de resposta e recuperação. Dentre essas ações existem atividades como triagem, análise e suporte aos incidentes de segurança, e atividades como detectar, monitorar e notificar incidentes envolvendo dados pessoais também fazem parte da política. Todas as atividades e respostas devem ser registradas em sistema apropriado. A política deve ainda seguir as melhores práticas de mercado e os padrões e procedimentos técnicos e normativos fornecidos pela pasta responsável pela segurança da informação do Governo Federal. Os incidentes devem ser registrados e classificados, e deve haver uma interface com as entidades relacionadas ao tratamento de incidentes nacionais e internacionais, além de uma formalização para a troca de informações e comunicação entre entidades com as quais a equipe especializada estabeleça cooperação. Por fim, deve incluir mecanismos para comunicação de incidentes de segurança à autoridade competente, que no caso de se tratar de dados pessoais será a Autoridade Nacional de Proteção de Dados.

3.8 Plano de Capacitação

O Plano de Capacitação é um documento que visa apresentar as ações que serão desenvolvidas para que seja possível tornar de amplo conhecimento os conhecimentos básicos sobre LGPD bem como as Políticas e Documentos que a UFC utiliza para sua implementação. Essa conscientização é importante para que a comunidade acadêmica conheça as políticas organizacionais relacionadas à proteção de dados pessoais e para que reconheça como suas ações são importantes para a preservação da privacidade dos titulares.

Além dessas características, esse Plano é um dos itens que são avaliados pelo TCU. Segundo esse Tribunal, as ações de capacitação devem considerar diferentes níveis de envolvimento dos colaboradores no tema, de forma que aqueles que ocupam funções com responsabilidades essenciais relacionadas à proteção de dados pessoais recebam treinamento diferenciado, além do nível básico fornecido aos demais.

4. CRONOGRAMA

Abaixo segue a previsão de execução das atividades descritas no Plano de Ação. Ressalta-se que a aplicação dos instrumentos que serão utilizados dentro dos setores analisados será iniciada após o desenvolvimento de todas essas ferramentas, estando sujeita a disponibilidade dos mesmos.

	JAN 23	FEV 23	MAR 23	ABR 23	MAI 23
Plano de Adequação					

Política de Privacidade					
Política de Proteção de Dados					
Política de Tratamento de Incidentes					
Política de Classificação de Dados					
Questionário de Adequação					
Inventário de Dados Pessoais					
Relatório de Impacto de Proteção de Dados					
Plano de Capacitação					