APÊNDICE A – PRODUTO TECNOLÓGICO: MANUAL DO PROCESSO ESTRUTRADO PARA COMPLIANCE À LGPD

O processo estruturado aqui proposto atende a um dos requisitos do Programa de Pós-graduação Profissional em Engenharia de Produção (PPGPEP) da Universidade Federal de São Carlos (UFSCAR). Ele atende os requisitos para produtos tecnológicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), categorizado como **Manual,** conforme descrito pela CAPES em documento próprio na página da instituição[6].

O produto tecnológico, resultado da pesquisa, é a elaboração de um manual descrevendo a proposta de processo estruturado para compliance à LGPD para IFES, baseada no framework da SGD do Governo Federal com as adaptações e experiências do processo de adequação dela na UFMT. O processo proposto descreve etapas e marcos otimizados para serem realizados em um período curto, considerando os principais requisitos da lei, o qual será detalhado nas páginas seguintes.

[6] https://www.gov.br/capes/pt-br/centrais-de-conteudo/10062019-producao-tecnica-pdf páginas 54-55.

MANUAL DO PROCESSO ESTRUTRADO PARA COMPLIANCE À LGPD

Willdson Gonçalves de Almeida

O Processo Estruturado

A proposta de Processo Estruturado para Compliance à Lei Geral de Proteção de Dados (LGPD) emerge da necessidade da Universidade Federal de Mato Grosso (UFMT) se adequar à Lei e experiências do projeto na instituição. O processo proposto é fortemente inspirado e adaptado em grande parcela do material da Secretaria de Governo Digital (SGD) do Governo Federal. No entanto, muito do que se propõe é resultante da experiência na UFMT e consolidado de outras fontes.

O processo foi organizado em três etapas formando um fluxo contínuo, conforme pode ser observado na Figura 1:

1. Estrutura de Governança para Proteção de Dados;
2. Tratamento de Dados e Consolidação de Políticas e;
3. Indicadores, Incidentes e Comunicação.

Figura 1 – Etapas do Processo Estruturado Proposto

Fonte: Elaborado pelo autor

Considerando-se as três etapas, foram definidas 11 ações para uma conformidade enxuta com a LGPD. Sendo na Etapa 1 – cinco ações, Etapa 2 – quatro ações e Etapa 3 – duas ações, conforme detalhado na Figura 2:

Figura 2 – Ações das Etapas de Compliance

Fonte: Elaborado pelo autor

A seguir serão descritas as ações, o detalhamento e recomendações.

Etapa 1 – Estrutura de Governança para Proteção de Dados

Figura 3 – Ações da Etapa 1

Fonte: Elaborado pelo autor

1.1 Nomeação do Encarregado pelo Tratamento de Dados

O encarregado pelo tratamento de dados é o responsável pela interface entre o controlador e o externo, em especial com a ANPD e titulares de dados. Deve ter boa capacidade de interlocução com as unidades internas da instituição, visando o atendimento dos requisitos da LGPD, bem como na resposta de demandas externas.

Considerando a similaridade das atividades, recomenda-se a vinculação da função na área de Ouvidoria ou Auditoria Interna.

1.2 Diagnóstico de Maturidade

Avalia o nível de aderência com os requisitos da LGPD anterior ao início da adequação, recomenda-se utilizar o formulário do SGD.

1.3 Criação de estrutura organizacional para Proteção de Dados Pessoais

É indispensável a criação de uma Comissão de Compliance à LGPD, com escopo de trabalho em níveis tático e operacional, deve ser composta preferencialmente representantes de unidades que possuam relevância no ciclo de tratamento de dados pessoais ou que possam colaborar efetivamente no projeto, como: área de TI, Jurídico, Gestão Acadêmica, Gestão de Atividades de Pesquisa, Unidade de Gestão da Extensão, Unid. Gestão Administrativa e Contratos.

O Comitê de Segurança da Informação e Proteção de Dados Pessoais com escopo de trabalho a nível estratégico, delibera sobre a gestão da privacidade, proteção de dados e segurança da informação.

É importante avaliar a criação de uma unidade administrativa com estrutura para abarcar as demandas de privacidade e proteção de dados na instituição.

1.4 Plano Estratégico de Compliance à LGPD

Documento que define o escopo da adequação, as etapas, ações, responsabilidades e prazos. Deve ser construído considerando a estrutura e equipe

para o projeto.

1.5 Cultura Institucional para Proteção de Dados Pessoais

Fomentar e promover iniciativas de treinamentos, eventos, estudos de caso, produção de material sobre Privacy by Design (Privacidade desde a concepção); Privacy by Default (Privacidade por padrão); Security by Design and by Default (Segurança desde a concepção e por padrão); Vazamento de dados; Malwares; Boas Práticas; entre outros.

Podem ser utilizadas as cartilhas do Cert.BR como referencial, disponível em https://cartilha.cert.br/, abarcam conteúdos diversos sobre segurança da informação.

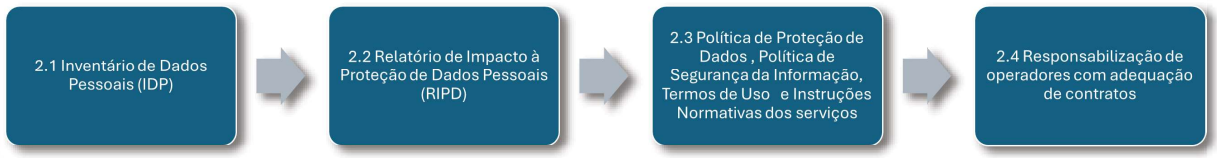
Figura 4 – Coleção de Fascículos disponíveis no Cert.BR

Fonte: Cert.BR, disponível em: https://cartilha.cert.br/fasciculos/

Criação de página da LGPD no portal: A página sobre a LGPD pode ser utilizada como ponto focal de informações sobre o processo de Compliance na instituição e divulgações das ações de cultura de privacidade e proteção e dados.

Etapa 2 – Tratamento de Dados e Consolidação de Políticas

Figura 5 – Ações da Etapa 2



Fonte: Elaborado pelo autor

2.1 Inventário de Dados Pessoais (IDP)

O IDP é uma ação indispensável, também conhecida como mapeamento de dados, é o documento que consolidada todo o tratamento de dados realizado pela instituição, como: bases de dados, titulares de dados, operadores, se existe previsões legais, quais dados e tipos de operações de tratamento.

O Apêndice B contém a estrutura do formulário utilizado na UFMT para a coleta de dados do IDP, adaptado da planilha disponibilizada pelo SGD.

2.2 Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

O RIPD é o documento que visa apurar riscos, responsabilidades e ações de mitigação para os riscos. Sugere-se utilizar o modelo de RIPD apresentado no Apêndice C, adaptado do SGD e com o complemento de informações que provê robustez ao documento.

Uma etapa importante após o IDP e antes do RIPD é filtrar as unidades com tratamento de alto risco. Para isso, foi desenvolvida uma ferramenta que classifica e informa se é necessária a elaboração de RIPD de acordo com critérios definidos pela ANPD, a estrutura da planilha e a fórmula são apresentados no Apêndice C.

2.3 Política de Proteção de Dados, Política de Segurança da Informação, Termos de Uso e Instruções Normativas dos serviços

A SGD disponibiliza modelos as políticas e termos, com atualizações frequentes. Recomenda-se a utilização dos modelos e adaptação à realidade da instituição.

2.4 Responsabilização de operadores com adequação de contratos

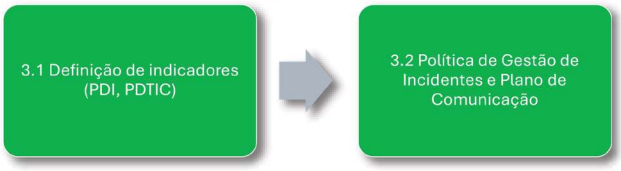
Durante o processo de compliance, especificamente no IDP, são mapeados os dados pessoais que possuem operadores externos. Deve-se identificar todos os

contratos que exista compartilhamento de dados pessoais e consignada a responsabilidade com o ente externo, com termo aditivo contratual inserindo cláusulas de responsabilização.

Importante definir um modelo de termo de responsabilidade de sigilo e privacidade para os agentes externos que realizam tratamento de dados pessoais pelo controlador.

Etapa 3 – Indicadores, Incidentes e Comunicação.

Figura 6 – Ações da Etapa 3



Fonte: Elaborado pelo autor

3.1 Definição de indicadores (PDI, PDTIC)

Visando o acompanhamento da efetividade das ações e garantir o ciclo de compliance, deve-se definir indicadores de controle das ações. A nível estratégico no Plano de Desenvolvimento Institucional (PDI) e a nível tático e operacional de tecnologia da informação no Plano Diretor de Tecnologia da Informação e Comunicação (TIC).

3.2 Política de Gestão de Incidentes e Plano de Comunicação

Um requisito da LGPD é ter medidas eficazes de identificação e comunicação de incidentes relacionados a dados pessoais. Para isso, deve-se construir uma Política de Gestão de Incidentes com Plano de Comunicação que defina a situação e forma que se deve comunicar incidentes ao titular de dados e ANPD.