Agência Nacional do Cinema

Programa de Governança em Privacidade - PGP

Alex Braga Muniz
Diretor-Presidente

Vinicius Clay Araújo Gomes
Diretor

Tiago Mafra dos Santos
Diretor

Mauro Gonçalves de Souza
Diretor Substituto

Comitê de Segurança da Informação e Comunicações – CSIC

Eduardo Fonseca de Moraes
Secretário de Gestão Interna e Gestor de Segurança da Informação e Comunicações

Gabriel Fliege de Lucena Stuckert
Secretário de Políticas de Financiamento Substituto

André Luiz de Souza Marques
Secretário de Políticas Regulatórias

Bruno Schneider
Gerente de Tecnologia da Informação

João Paulo Machado Gonçalves
Ouvidor-Geral e Encarregado pelo tratamento de dados pessoais

Rafael da Silva Pereira
Coordenador de Documentação e Patrimônio - Gerência de Administração

HISTÓRICO DE ALTERAÇÕES

Data	Versão	Descrição	Autor
31/03/2021	1.0	Versão Inicial	GT Implantação LGPD
31/01/2022	2.0	Alteração do Encarregado, Diretores e componentes do CSIC Atualização do Plano de Ação e das metas para 2022	SGI e OUV

SUMÁRIO

1 IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

CONTROLADOR	
AGÊNCIA NACIONAL DO CINEMA – CNPJ 04.884.574/0003-92	
OPERADOR	
AGÊNCIA NACIONAL DO CINEMA – CNPJ 04.884.574/0003-92	
ENCARREGADO	
JOÃO PAULO MACHADO GONÇALVES **PORTARIA ANCINE N.º 474-E, DE 6 DE NOVEMBRO DE 2020**	
E-MAIL ENCARREGADO	**TELEFONE ENCARREGADO**
ENCARREGADO@ANCINE.GOV.BR	**21 3037-6086**

2 INTRODUÇÃO

A Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018) dispõe sobre o "tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural". Em outras palavras, trata-se da legislação brasileira que visa regulamentar a aquisição e o tratamento de dados pessoais no Brasil.

No que se refere ao poder público, essa Lei define que:

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:
>
> I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; (...)

No que concerne às boas práticas de governança e ao Programa de Governança em Privacidade – PGP, a Lei define que:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

I - implementar programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) conte com planos de resposta a incidentes e remediação; e

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

(...)

Dessa forma, o Programa de Governança em Privacidade – PGP deve capturar e consolidar os requisitos de privacidade com o intuito de ditar e influenciar como os dados pessoais serão manuseados ao longo do seu ciclo de vida, de forma integrada à estrutura de governança da organização. Além disso, a fim de orientar e alinhar as futuras ações que impactem a privacidade e o tratamento dos dados pessoais, deve estabelecer um plano de melhorias e aperfeiçoamentos em processos, normas e ferramentas para mitigar os riscos de segurança de informação e comunicação, aprimorando os controles internos e a cultura organizacional voltada à gestão da informação.

No contexto da ANCINE, o monitoramento do PGP se insere no escopo de atuação do Comitê de Segurança da Informação e Comunicações – CSIC, estando inclusive alinhado às suas competências regimentais:

Resolução de Diretoria Colegiada nº 60[1]

7. Atribuições
.....
Item 7.2.73. São atribuições do Comitê de Segurança da Informação e Comunicações – CSIC:

[1] Resolução de Diretoria Colegiada nº 60, de 2 de abril de 2014, e suas alterações, disponível em https://www.gov.br/ancine/pt-br/acesso-a-informacao/legislacao/resolucoes-diretoria-colegiada/resolucao-no-60.

.....
IX. dar suporte ao Encarregado de Dados Pessoais, Monitoramento dos Incidentes e o Acompanhamento da Política de Privacidade, nos termos da Lei n.º 13.709, de 14 de agosto de 2018.

Dentre outras funções, o CSIC tem a responsabilidade de formular a Política de Segurança da Informação e normas correlatas, bem como subsidiar a elaboração do rol anual de informações desclassificadas e documentos classificados em cada grau de sigilo. É constituído por representantes das três Secretarias (Gestão Interna, Políticas Regulatórias, Políticas de Financiamento), além da Gerência de TI, Coordenação de Documentação e Patrimônio, e Ouvidoria-Geral.

Ressalte-se que o titular da Ouvidoria-Geral também exerce o papel de Encarregado pelo tratamento de dados pessoais conforme a Portaria ANCINE N.º 474-E, de 6 de novembro de 2020, possibilitando a integração das ações institucionais e a governança centralizada dos temas de segurança de informação e proteção de dados pessoais.

Importante observar que o acompanhamento das ações do PGP será realizado no âmbito de duas estruturas de governança da ANCINE: inicialmente pelo CSIC, que fará o monitoramento contínuo das ações previstas no Programa, e de forma complementar pelo Comitê de Governança, Riscos e Controles, que fará o monitoramento e avaliação dos riscos institucionais associados ao tratamento de dados pessoais, descritos no Relatório de Impacto à Proteção de Dados Pessoais – RIPD.

3 METODOLOGIA

Para a elaboração do PGP da ANCINE, foi constituído um grupo de trabalho interdisciplinar nomeado por meio da Portaria SGI N.º 402-E, de 8 de dezembro de 2020. Esse grupo avaliou que o modelo apresentado pela Secretaria de Governo Digital do Ministério da Economia[2] era o mais adequado, pois foi inspirado nas normas ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27701:2019 Tecnologia da Informação - Técnicas de Segurança – Código de Prática para controles de segurança da informação e ABNT NBR ISO/IEC 27005:2011 Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.

De acordo com esse modelo, o PGP é estruturado nas seguintes etapas:

[2] https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaProgramaGovernanaemPrivacidade.pdf

Figura 1 - Etapas do PGP. Fonte: SGD/ME

A etapa de Iniciação e Planejamento busca compreender quais são as primeiras informações e os dados importantes que devem ser conhecidos. Um item relevante é a avaliação da maturidade da organização, observando fatores como a rastreabilidade de dados, a comunicação com o cidadão e a transparência, podendo ser utilizada a ferramenta desenvolvida pela Secretaria de Governo Digital do Ministério da Economia – SGD/ME para fornecer um diagnóstico do atual estágio de adequação à LGPD e um índice de maturidade para avaliação do ciclo PDCA de melhorias e aperfeiçoamentos.

Outro aspecto fundamental da etapa de Iniciação e Planejamento é o alinhamento das atividades do encarregado provenientes de sua atuação como canal de comunicação entre o controlador, os titulares dos dados e a ANPD, com a estrutura organizacional para governança e gestão da proteção de dados pessoais.

Por fim, um dos produtos estratégicos gerados nessa etapa é o Inventário de dados pessoais, documento que identifica quais dados pessoais são tratados, onde estão e que operações são realizadas com eles pela instituição, em alinhamento ao previsto pelo art. 37 da LGPD.

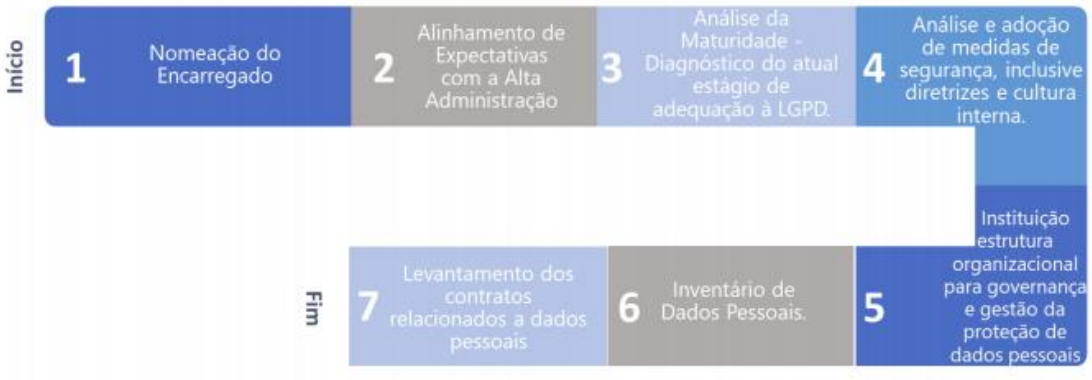

Figura 2 - Etapa de Iniciação e Planejamento. Fonte: SGD/ME

Na etapa de construção e execução, devem ser especificadas políticas e práticas para proteger a privacidade do cidadão, garantindo que todos os usos dos dados pessoais sejam conhecidos. Além disso,

a promoção de uma cultura de segurança e proteção de dados também deve ser objeto de planejamento, divulgando o papel da Administração Pública como custodiante dos dados e sua responsabilidade ao tratar os dados pessoais dos cidadãos. Ações de capacitação e treinamento devem ser planejadas para que uma cultura de Privacidade desde a Concepção (*Privacy by Design*) seja instituída.

É ainda nesta etapa que o Relatório de Impacto à Proteção de Dados Pessoais - RIPD deve ser elaborado, documento previsto na LGPD em vários dos seus dispositivos, em especial, no artigo 38. O RIPD representa um instrumento importante de verificação e demonstração da conformidade do tratamento de dados pessoais realizado pela instituição e serve tanto para a análise quanto para a documentação do tratamento dos dados pessoais.

Também é necessária a elaboração de documentos que visem a transparência com o titular de dados pessoais, comunicando como as atividades de tratamento desses dados observam os princípios dispostos no artigo 6º da LGPD. A Política de Privacidade, documento pelo qual o prestador de serviço formaliza como o serviço realiza o tratamento dos dados pessoais e como ele fornece privacidade ao usuário, e o Termo de Uso, documento que descreve de forma detalhada o serviço, as condições e as regras aplicáveis a ele.

Figura 3 - Etapa de Construção e Execução. Fonte: SGD/ME

Na etapa de monitoramento seria avaliada a execução do PGP através da coleta e análise de indicadores, a elaboração de relatórios e apresentações de resultados, incluindo as medidas de controle para mitigação de riscos. Nesse contexto, é fundamental registrar os incidentes de segurança da informação e de privacidade ocorridos a fim de avaliar e evitar reincidências e aperfeiçoar continuamente o Programa.

Figura 4 - Etapa de Monitoramento. Fonte: SGD/ME

4 REFERÊNCIAS LEGAIS

As normas a seguir estão, em sua maioria, ligadas ao tema de Segurança de Informação e Comunicação, podendo ser aplicadas ao contexto de proteção e mitigação de riscos no tratamento de dados pessoais. Ressalta-se que as normas estão alinhadas com as Instruções Normativas e Normas Complementares elaboradas pelo Departamento de Segurança da Informação (DSI), que integra o Gabinete de Segurança Institucional da Presidência da República (GSI-PR).

- Política de Segurança da Informação e Comunicações (POSIC): https://www.gov.br/ancine/pt-br/acesso-a-informacao/legislacao/resolucoes-diretoria-colegiada/resolucao-no-117

- Política de Gestão de Riscos (PGR): https://www.gov.br/ancine/pt-br/acesso-a-informacao/legislacao/resolucoes-diretoria-colegiada/resolucao-no-107

- Processo Eletrônico (SEI): https://www.gov.br/ancine/pt-br/acesso-a-informacao/legislacao/resolucoes-diretoria-colegiada/resolucao-no-66

- Portaria ANCINE Nº 182-E, de 7 de julho de 2021: Designa os membros da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) da ANCINE;

- Portaria ANCINE N.º 474-E, de 6 de novembro de 2020: Dispõe sobre o Encarregado pelo tratamento de dados pessoais;

- Portaria ANCINE N.º 489-E, de 14 de agosto de 2018: Diretrizes para os processos de Gestão de Riscos, Gestão de Continuidade e Gestão de Mudanças, nos aspectos relativos à Segurança da Informação e Comunicações na ANCINE;

- Portaria ANCINE Nº 292-E, de 19 de setembro de 2017: Regras para a utilização dos recursos computacionais e as diretrizes para a implementação de controles de acesso relativos à Segurança da Informação e Comunicações na ANCINE;

- Portaria ANCINE Nº 237-E, de 08 de agosto de 2017: Política de Utilização de Senhas na ANCINE;

- Portaria ANCINE Nº 42-E, de 18 de julho de 2016: Política de uso de redes sem fio;

- Portaria ANCINE Nº 139, de 6 de julho de 2015, que aprova a instituição e o funcionamento da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) da ANCINE.

5 CULTURA DE PROTEÇÃO DE DADOS PESSOAIS

A entrada em vigor da Lei Geral de Proteção de Dados Pessoais não é apenas a definição de um novo marco regulatório no Brasil, mas também a definição de um novo patamar ético relacionado à privacidade, esta entendida em espectro amplo.

Mais do que definir um programa de proteção de dados pessoais, o desafio está na promoção de uma cultura de proteção de dados pessoais, por meio da qual cada pessoa compreende e colabora para a construção e exercício da privacidade como direito humano fundamental.

Cada pessoa que exerce atividades na ANCINE deve atuar de forma consciente e construtiva para entender o que é privacidade, o que são dados pessoais, quais dados pessoais são tratados na Agência e como a ANCINE deve proteger cada um desses dados.

A publicação "*Privacy by Design: The 7 Foundational Principles*"[3], de Ann Cavoukian, Ph.D., oferece uma ilustração, por meio de princípios, dos valores inerentes à construção de uma proteção de dados pessoais como ética, conforme adaptação abaixo extraída do 'Guia de Elaboração de Programa de Governança em Privacidade'[4]:

1. Proativo, e não reativo; preventivo, e não corretivo

A abordagem de Privacidade desde a Concepção (PdC) antecipa e evita eventos invasivos de privacidade antes que eles aconteçam. Desse modo, não espera que riscos de privacidade se materializem, nem oferece soluções para as infrações de privacidade após a ocorrência, mas visa impedir que eles ocorram.

2. Privacidade deve ser o padrão dos sistemas de TI ou práticas de negócio

Busca-se oferecer o máximo grau de privacidade, garantindo que os dados pessoais sejam protegidos automaticamente em qualquer sistema de TI ou prática de negócios. É uma forma de evitar que qualquer ação seja necessária por parte do titular dos dados pessoais para proteger a sua privacidade, pois ela já estará embutida no sistema, por padrão.

3. Privacidade incorporada ao projeto (design)

A privacidade deve estar incorporada ao projeto e arquitetura dos sistemas de TI e práticas de negócios, não deve ser considerada como complemento adicional, após o sistema, projeto ou serviço já estar em implementação ou em execução. O resultado é que a privacidade se torna um componente essencial da funcionalidade principal que está sendo entregue. A privacidade é parte integrante do sistema, sem diminuir a funcionalidade.

4. Funcionalidade total

A PdC não envolve simplesmente a formalização de declarações e compromissos de privacidade. Refere-se a satisfazer todos os objetivos do projeto, não apenas os objetivos de privacidade, permitindo funcionalidade total com resultados reais e práticos. Ao incorporar privacidade em uma determinada

[3] Disponível em https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf, com acesso em 11 de fevereiro de 2021.
[4] Disponível em https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaProgramaGovernanaemPrivacidade.pdf, com acesso em 11 de fevereiro de 2021.

tecnologia, processo ou sistema, isso é realizado de uma forma que não comprometa a plena funcionalidade e permita que todas as exigências do projeto sejam atendidas.

5. Segurança e proteção de ponta a ponta durante o ciclo de vida de tratamento dos dados

Por ser incorporado ao sistema antes de o primeiro elemento de informação ser coletado, a PdC estende-se por todo o ciclo de tratamento dos dados envolvidos no projeto, sistema ou serviço. Medidas fortes de segurança são essenciais para a privacidade, do início ao fim.

6. Visibilidade e transparência

A PdC objetiva garantir a todos os interessados que, independentemente da prática ou tecnologia comercial envolvida, está de fato operando de acordo com as premissas e objetivos declarados, os quais devem ser objeto de verificação independente. Visibilidade e transparência são essenciais para estabelecer responsabilidade e confiança.

7. Respeito pela privacidade do usuário

Acima de tudo, a privacidade desde a concepção exige que as instituições respeitem os direitos dos titulares dos dados pessoais. Isso é alcançado por meio de medidas como padrões fortes de privacidade, avisos apropriados e interfaces amigáveis que empoderem o titular dos dados. Os melhores resultados da privacidade desde a concepção, geralmente, são aqueles projetados de acordo com os interesses e necessidades dos titulares dos dados pessoais, que têm o maior interesse em gerenciar seus próprios dados.

O plano de comunicação do PGP tem como objetivo promover uma cultura de segurança e proteção de dados no corpo funcional e de colaboradores da Agência. Deve divulgar o papel da Administração Pública como custodiante dos dados e sua responsabilidade ao tratar os dados pessoais dos cidadãos. As ações de capacitação e treinamento devem ser oferecidas para que uma cultura de Privacidade desde a Concepção (*Privacy by Design*) seja instituída.

O desenvolvimento da cultura de proteção de dados pessoais pode ser estruturado a partir de 3 (três) eixos:

- Promover a privacidade
- Qualificar servidores
- Engajar as lideranças

Promover a Privacidade

Para o fortalecimento da privacidade como valor na ANCINE não basta pressupor que os atores envolvidos, como diversos usuários dos serviços da Agência e a totalidade do público interno, compreendem a proteção de dados pessoais de modo uniforme.

Essa posição propicia o fortalecimento das assimetrias dentro e fora da Agência quanto aos aspectos teóricos e às práticas fundamentais da proteção de dados pessoais. Cada indivíduo possui experiências, conhecimentos e concepções sobre privacidade, e tal riqueza deve facilitar o desenvolvimento de um patamar elevado de promoção da privacidade, ao invés de dificultar o exercício contínuo, coerente e racional de políticas de proteção de dados pessoais.

A promoção da cultura de privacidade surge exatamente para disseminar uma compreensão racional e minimamente uniformizada sobre o que é privacidade, a importância da proteção de dados e os efeitos perniciosos do menosprezo à importância do tema.

Promover a privacidade também é motivar as pessoas a agir com cautela nas matérias que se referem a dados pessoais, e parte dessa motivação é atingida com o convencimento e conscientização quanto à importância do tema.

A indicação de casos concretos relacionados à proteção de dados pessoais, e que afetem a vida cidadã em inúmeros aspectos, pode demonstrar a importância do tema em sua perspectiva coletiva e individual.

Neste sentido, recomenda-se a criação de uma nova página/área no Portal do Servidor dedicada a Segurança de Informação e LGPD contendo as referências ligadas ao tema que já foram produzidos na ANCINE. Em paralelo, deve ser criado um FAQ com perguntas e respostas relevantes sobre segurança da informação.

Assim, em caso de dúvida sobre algum aspecto da segurança, os usuários poderiam procurar diretamente no FAQ na Intranet, que seria constantemente alimentado com novas informações. Outra boa prática já utilizada com sucesso na ANCINE é a distribuição de pílulas de conhecimento, endereçando, quando possível, as principais dúvidas e questões identificadas junto ao corpo funcional.

Cabe ressaltar que o uso de material físico, como pôsteres e banners, é um eficiente método de difusão de informação. Em geral, tais peças podem ser dispostas em murais nos corredores, elevadores e recepção, sendo compostas por assuntos que atraiam a atenção dos servidores e colaboradores. SPAM, *phishing* e sequestro de dados são temas que atraem a atenção e são extremamente importantes na mitigação de riscos no ambiente digital.

Outra ação por vezes recomendada por especialistas em segurança da informação é a chamada “blitz da segurança”. Nesse tipo de ação, a área de segurança da ANCINE deve percorrer os escritórios, identificando pontos de vulnerabilidade, tais como: computadores com sistemas abertos, mas sem a presença do usuário no local; pendrives expostos; papéis com anotação de senha; informações restritas disponíveis sobre as mesas.

Tais ações têm apenas função educativa, cujo objetivo é de alertar os usuários sobre os riscos de não considerar a segurança da informação no dia a dia do trabalho na Agência. Ressalta-se que ações desse tipo tem caráter apenas educativo, não sendo consideradas auditoria.

Qualificar os servidores

Não há cultura sem ação humana. Assim, difundida a importância da privacidade não apenas do ponto de vista regulatório, mas também em seu aspecto para a construção de cidadania e em seu patamar ético, é preciso preparar os agentes envolvidos para atuar em suas atividades como agentes que possam promover uma cultura consciente de privacidade.

Cada agente público deve estar ciente sobre os riscos envolvidos em suas ações e sobre as ferramentas e medidas disponíveis para minimizar a possibilidade de materialização de tais riscos, ou mesmo de minimização dos prejuízos advindos de ocorrências adversas ao ambiente de proteção de dados pessoais.

Assim como as melhores práticas e soluções no tratamento de dados pessoais podem derivar diretamente dos agentes da ANCINE, eventos de quebra de privacidade também podem ter como origem diversas condutas dos profissionais envolvidos diariamente nas atividades da Agência.

Nesta temática, cabe lembrar que as ações do PGP seriam derivadas dos seguintes itens previstos no Plano de Desenvolvimento de Pessoas (PDP) de 2021:

- Item 35 “Conhecer a Lei Brasileira de Proteção de Dados Pessoais”;
- Item 38 “Construir conhecimentos acerca de segurança da informação”;
- Item 71 “Promover a segurança da informação e comunicações no âmbito da Ancine”.

Uma importante prática a ser implementada é a capacitação de novos servidores e colaboradores no momento do ingresso na Agência. Essa capacitação deve ser oferecida por meio de cartilhas dedicadas à prática da segurança da informação, cujos assuntos incluam tanto a parte normativa, quanto a parte operacional. Os temas abordados, portanto, incluiriam o rol normas elaboradas pelo CSIC, a proteção de email, cuidados na navegação web, proteção contra phishing, manuseio de documentos físicos/digitais, cuidados com a senha, entre outros.

Além disso, pode-se estender essa capacitação para um ambiente digital, por meio de uma plataforma de aprendizado online como o Moodle, onde, além de conteúdo específico sobre segurança, existe a possibilidade de incluir questionários de avaliação, de forma a comprovar que o material exposto foi absorvido pelos usuários. De modo mais abrangente, tal método de capacitação em formato digital pode servir como capacitação periódica a ser lançada pelo GRH para todos os servidores da ANCINE, sendo contabilizado como horas de treinamento, a fim de motivar o uso da plataforma.

Engajar as lideranças

Por fim, a promoção de uma cultura corporativa exige a participação direta das lideranças envolvidas, seja por meio do reforço contínuo da importância da privacidade como valor institucional, pela capacidade de oferecer respostas às dúvidas que surgirem durante as ações de proteção de dados pessoais, ou mesmo pelo exemplo, demonstrado no interesse e práticas voltadas à construção da privacidade como prática, e não apenas como teoria ou exercício formal.

Esse eixo deve ser trabalhado em conjunto com os eixos anteriores, induzindo o engajamento das diversas lideranças, desde a alta administração até o chefe imediato, em relação à conscientização dos riscos ao longo de todo o ciclo de tratamento da informação e quais boas práticas e controles podem ser incorporados aos processos e a rotina de trabalho.

Neste eixo, é fundamental lembrar a importância do CSIC, responsável pelo monitoramento do PGP, pois tendo representatividade de todas as Secretarias e do Encarregado de tratamento de dados pessoais, pode avaliar os riscos de segurança de informação e acompanhar junto às lideranças a implementação dos controles necessários à sua mitigação.

6 PRÁTICAS PARA PROTEÇÃO DA PRIVACIDADE

Reclamações e Petições dos Titulares

O canal preferencial para recebimento de petições e reclamações do titular de dados pessoais, em atendimento aos art. 18 a 20 da Lei Geral de Proteção de Dados Pessoais, é a plataforma Fala.BR (https://falabr.cgu.gov.br), indicando no campo 'assunto' a opção 'dados pessoais'.

Quaisquer manifestações dentre as disponíveis na plataforma Fala.BR podem ser utilizadas para reivindicação ou exercício dos direitos previstos para os titulares de dados pessoais e o recebimento.

Como canais acessórios para o recebimento de petições e manifestações estão disponíveis a caixa de e-mail encarregado@ancine.gov.br, atendimento telefônico da Ouvidoria-Geral e o atendimento presencial, também pela Ouvidoria-Geral, mediante prévio agendamento.

O tratamento dispensado ao titular de dados pessoais atenderá o disposto na Lei Geral de Proteção de Dados Pessoais e na Lei de Proteção e Defesa do Usuário de Serviços Públicos, de nº 13.460, de 23 de junho de 2017.

Conforme previsto pela Portaria ANCINE nº 474-E, de 6 de novembro de 2020, o Encarregado pelo tratamento de dados pessoais poderá solicitar o apoio das áreas técnicas para o atendimento às demandas dos titulares de dados pessoais.

Divulgação e Privacidade

Segundo o entendimento corrente, ainda a ser confirmado e regulamentado pela Autoridade Nacional de Proteção de Dados – ANPD, eventual divulgação de dados pessoais deve ser cotejada à luz do interesse público, isto é, em situações relacionadas, por exemplo, ao exercício da atividade de controle, ao desenvolvimento e implementação de políticas públicas, à realização de diagnósticos e estudos, com fins jornalísticos, acadêmicos ou estatísticos, ou, de forma geral, à existência de legítimo interesse (Art. 7, IX da LGPD).

Os dados poderão ser compartilhados com outros órgãos públicos em ações de política pública, com órgão de controle e judiciais, para realização de estudos por órgão de pesquisa,

com agentes financeiros contratados para operação de atividades de fomento e com representações diplomáticas para concessão de visto para profissionais estrangeiros atuantes em filmagens em solo nacional.

Seja em função dos pedidos efetuados por meio da Lei de Acesso de Informação - LAI, ou via transparência ativa, com a disponibilização de dados em portais e de relatórios, a abertura de dados pessoais deve sempre seguir os parâmetros de legalidade e razoabilidade. Eventual publicização de dados de pessoas naturais ligadas a agentes econômicos que captam recursos públicos podem permitir a fiscalização cidadã.

A título de exemplo, parte dos dados coletados durante a submissão de projetos em chamadas públicas, quando avaliados para fins de seleção, devido à própria natureza do certame em decorrência da existência de cotas regionais, indutores de gênero e raça e pontuação do histórico profissional, podem ser tornados públicos.

Algumas técnicas podem ser utilizadas para atender o princípio da razoabilidade na publicização dos dados sem ferir a privacidade do titular. De acordo com o artigo 7º, parágrafo 2º, da LAI, "quando não for autorizado acesso integral à informação por ser ela parcialmente sigilosa, é assegurado o acesso à parte não sigilosa por meio de certidão, extrato ou cópia com ocultação da parte sob sigilo".

Para que sejam preservadas a unicidade, autenticidade e integridade dos documentos divulgados, porém ocultando-se estes itens protegidos por sigilo, utiliza-se a técnica de ocultação por aposição de tarjas, na qual as palavras, ou conjuntos de palavras, presentes nos textos são ofuscados com uso de marcação, normalmente uma tarja na cor preta, impossibilitando o seu reconhecimento. Nesse caso deve-se utilizar o Guia de referência de edição de documentos digitais disponível no Portal do Servidor.

Outra técnica disponível é a anonimização, descrita como a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo (Art. 5º, XI da LGPD). Em geral, utiliza-se a supressão, isto é, um ou mais valores são substituídos por algum caractere especial em um conjunto de dados[5]. Por exemplo, CPF 123.456.789-00, se torna 123.45X.XXX-XX, ou ao invés do nome completo, publicar apenas o primeiro nome.

Finalidade de Tratamento dos Dados Pessoais

De uma forma geral, o tratamento de dados pessoais na ANCINE possui a finalidade de cumprir obrigações legais, regulatórias e fiscalizatórias, bem como, para a execução de políticas públicas.

No âmbito da Gestão Interna, o tratamento de dados pessoais se concentra na gestão de recursos humanos (dados pessoais de servidores e colaboradores) e na gestão administrativa

[5] BRITO, Felipe Timbó; MACHADO, Javam Castro. Preservação de privacidade de dados: Fundamentos, técnicas e aplicações. Jornadas de atualização em informática, p. 91-130, 2017.

(gestão documental e arquivística). Além disso, por força da fiscalização da legislação trabalhista, também podem ser tratados dados pessoais de terceirizados.

No âmbito dos processos regulatórios, o tratamento de dados pessoais se dá para adimplemento das competências de regulação e de fiscalização de agentes econômicos que exerçam atividade econômica em segmentos de mercado audiovisual regulados no país (exibição, programação/veiculação e distribuição de conteúdos audiovisuais) em benefício da promoção e da difusão do conteúdo audiovisual brasileiro em um ambiente regulatório desenvolvido e equilibrado.

No âmbito dos processos de fomento, o tratamento de dados pessoais se dá para viabilizar as ações de fomento por meio de leis de incentivo e de editais e programas do Fundo Setorial do Audiovisual, visando promover a produção e circulação do audiovisual independente no Brasil e internacionalmente; a diversidade de regional, de gênero e raça no audiovisual; a expansão do parque exibidor; e o fortalecimento das programadoras e distribuidoras brasileiras.

Grande parte dos dados pessoais coletados pela ANCINE vem na forma documental, em meio físico ou digital, e são armazenados via Sistema de processo eletrônico (SEI), ou obtidos via formulários eletrônicos nos serviços digitais disponibilizados por meio do Sistema Ancine Digital (SAD).

O compartilhamento de dados com terceiros poderá ser realizado, desde que obtido o consentimento específico do titular das informações, ressalvadas as hipóteses de dispensa desse consentimento dispostas em Lei. Nesse contexto, destaca-se o compartilhamento com os órgãos de controle como TCU e CGU.

O período de armazenamento e a exclusão dos dados obedecem à tabela de temporalidade de documentos aprovada pelo Arquivo Nacional, às normas vigentes de gestão arquivística e ao disposto nos Artigos 15 e 16 da LGPD.

Mecanismos de Supervisão e Mitigação de Riscos

A mitigação de riscos no tratamento de dados pessoais se dá através de 3 eixos principais: Capacitação e conscientização, Gestão de tecnologia de informação e comunicação - TIC e Processo de avaliação de riscos.

- Capacitação e conscientização: difusão na cultura organizacional sobre a importância da LGPD aplicável ao setor público. Comunicação interna voltada às “boas práticas” para proteção de dados pessoais, inclusive em contexto de teletrabalho. Difusão das regras de responsabilização aplicáveis em caso de violação à legislação de proteção de dados pessoais. Termo de Responsabilidade para utilização dos recursos computacionais.

- Gestão de TIC: Contínuo investimento em soluções que aprimorem a segurança computacional (Antivírus, *Firewall*, Controle de *Logs*, entre outros). Além disso, deve-se reavaliar as soluções e o processo de controle de acesso aos sistemas e às bases de dados nos quais

estão armazenados os dados recebidos pela Agência, de forma a garantir que apenas servidores próprios ou profissionais contratados pela Agência tenham acesso aos dados restritos. Outro aspecto é o reforço no papel da ETIR – Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais e, em especial, o detalhamento do processo de tratamento de incidentes relacionados à LGPD.

- Processo de Avaliação de Riscos: a avaliação dos riscos da LGPD deve estar integrada à Política de Gestão de Riscos definida pela RDC nº 107, com foco nos riscos de mais alto impacto que possam comprometer a imagem da Agência. A elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), prevista no Art. 5º, XVII da LGPD, permitirá o monitoramento dos riscos pelas unidades de governança competentes.

Adequação Contratual

Na etapa de construção e execução do modelo sugerido pela SGD/ME, uma das ações recomendadas é realizar a adequação das cláusulas contratuais conforme os princípios da LGPD e dos requisitos do PGP. O objetivo é adaptar os contratos, convênios e outros instrumentos que impliquem no tratamento de dados pessoais mapeados pelo Inventário.

Nesse contexto, para aqueles cenários onde existem operadores de tratamento de dados pessoais contratados pela Administração Pública, se faz necessária tal adequação para garantir os direitos do titular, assegurar as medidas de proteção e segurança dos dados coletados e armazenados pela contratada e delimitar de forma objetiva as responsabilidades do controlador e operador.

A princípio, no âmbito do PGP, não foram identificados operadores, pois a execução das políticas públicas e o tratamento de dados pessoais utiliza majoritariamente o ambiente de infraestrutura da própria ANCINE.

No entanto, na operação de recursos do Fundo Setorial do Audiovisual - FSA que é, em parte, descentralizada para agentes financeiros e outros entes federativos, pode ocorrer o tratamento de dados pessoais por estes terceiros, eventualmente havendo o enquadramento no perfil de operador. Para essa finalidade, optou-se por aguardar uma eventual regulamentação da Autoridade Nacional de Proteção de Dados – ANPD quanto a caracterização dos operadores, e da Advocacia Geral da União (AGU), sobre a necessidade de adequação das cláusulas contratuais aos princípios da LGPD apresentados em seu art. 6º.

Dessa forma, a atividade de adequação contratual pode ser revista durante a execução do PGP de acordo com novas orientações e normativos sobre o tema, razão pela qual esse aspecto deve ser continuamente avaliado pelo CSIC.

7 PLANO DE AÇÃO

A partir da elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) e a análise dos controles necessários à mitigação dos riscos de segurança e privacidade, foram identificados uma série de ações que devem ser realizadas. Além disso, o próprio PGP sugere ações de promoção da cultura de proteção de dados através da conscientização e capacitação dos servidores e colaboradores. Dessa forma, o quadro abaixo procura estruturar um plano de ação com prazos e responsáveis para implementação das medidas.

Ação#	Tema	Descrição	Responsável	Prazo
1	Cultura	Promover a Privacidade Qualificar os Servidores Engajar as Lideranças	CSIC, GRH, Encarregado	2022
2	Processo	Adequar rotinas e procedimentos da SGI à LGPD/PGP	SGI	2022
3	Processo	Adequar rotinas e procedimentos da SRG à LGPD/PGP	SRG	2022
4	Processo	Adequar rotinas e procedimentos da SEF à LGPD/PGP	SEF	2022
5	Processo	Integrar processo de inventário organizacional de ativos	SGI, GTI, GAD	2022
6	Processo	Implementar avaliação de segurança quando for identificada necessidade de mudanças (Infra e Sistemas)	GTI	2022
7	Processo	Implementar processo periódico de análise e monitoramento de vulnerabilidades	GTI	2022
8	Normas	Elaborar Plano de Gerenciamento de Incidentes	CSIC, GTI	2022
9	Processo	Definir a abrangência dos testes de backup e sua periodicidade	GTI	2022
10	Processo	Definir o período de retenção das cópias de segurança e os requisitos de releitura	GTI	2022
11	Processo	Elaborar Plano de adequação da MDS ANCINE às normas e melhores práticas de desenvolvimento seguro	GTI	2022
12	Software	Planejar realização de testes de invasão e de segurança no ambiente de infraestrutura corporativo	GTI	2022
13	Processo	Definir e implementar política de controle de acesso e atualização periódica dos direitos de acesso	GRH, GAD, GTI, SGI	2022
14	Software	Implementar mecanismo de encerramento de sessão	GTI	2022
15	Software	Implementar mecanismo de limitação de sessão simultânea	GTI	2022
16	Software	Implementar prática de armazenar credenciais de acesso e logs separadamente das aplicações	GTI	2022
17	Software	Verificar mensagens não tratadas do SEI e SAD	GTI	2022

18	Software	Implementar controle na infraestrutura ANCINE (controles 68 a 75 tratamento de riscos do RIPD)	GTI	2022
19	Normas	Definir e implementar norma interna sobre fornecimento de bases de informações	CSIC, Encarregado	2022
20	Processo	Definição do Plano de Classificação Documental e Tabela de Temporalidade das unidades finalísticas	CPAD	2022

8 INDICADORES E METAS

A utilização de indicadores e metas é fundamental para determinar o progresso no cumprimento dos requisitos de conformidade com a proteção de dados pessoais e dos controles de proteção de dados pessoais, comparar o desempenho em toda a organização, identificar vulnerabilidades e lacunas na política e na implementação e identificar modelos de sucesso.

Nesse sentido, foi aplicada uma ferramenta de diagnóstico disponibilizada pela SGD/ME[6], estruturada a partir de uma série de questões de autoavaliação organizacional que, ao final, geram um indicador de adequação aos requisitos da LGPD, conforme quadro a seguir:

Índice	Nível de Adequação
0,00 a 0,29	Inicial
0,30 a 0,49	Básico
0,50 a 0,69	Intermediário
0,70 a 0,89	Em Aprimoramento
0,90 a 1,00	Aprimorado

Tabela 1 - Indicador de Adequação à LGPD. Fonte SGD/ME

Dessa forma, avalia-se que a utilização desse índice é adequada para estabelecer metas de cumprimento do PGP à medida que possibilita a comparação do nível de maturidade organizacional da ANCINE com outras Agências e órgãos.

Para estabelecer uma linha de base inicial, foi realizada após a elaboração PGP, uma avaliação do diagnóstico de adequação à LGPD da ANCINE, sendo seu resultado apresentado conforme quadro-resumo a seguir:

Dimensão	Índice
Governança	0.79
Conformidade Legal e respeito aos princípios	0.58
Transparência e direitos do titular	0.89
Rastreabilidade	0.74
Adequação de contratos e de relações com parceiros	0.2
Segurança da Informação	0.2
Violações de dados	0.44
Índice de Adequação à LGPD (Inicial)	**0.57 (Intermediário)**

Tabela 2 - Diagnóstico de Referência

Foi estabelecida a meta de 0,70 (Em Aprimoramento) para o final de 2021, quando se esperava que grande parte das ações planejadas na seção “Plano de Ação” já estivessem implementadas.

[6] https://limesurvey.sgd.nuvem.gov.br/index.php/798411?lang=pt-BR

Ao final do ciclo de 2021, um novo diagnóstico foi realizado e o resultado da ANCINE está apresentado abaixo:

Dimensão	Índice
Governança	1.00
Conformidade Legal e respeito aos princípios	0.78
Transparência e direitos do titular	1.00
Rastreabilidade	0.84
Adequação de contratos e de relações com parceiros	0.2
Segurança da Informação	0.46
Violações de dados	0.65
Índice de Adequação à LGPD (Final de 2021)	**0.74 (Em Aprimoramento)**

Tabela 3 - Diagnóstico 2021

Importante notar que apesar da meta de 0,70 ter sido cumprida, mostrando que a ANCINE já se encontra no nível de "Em Aprimoramento" da LGPD, as dimensões de "Adequação de contratos e de relações com parceiros" e "Segurança da Informação" ainda precisam evoluir para o próximo período. Em termos práticos, isso significa avançar nas ações de adequação dos instrumentos contratuais da ANCINE em relação à LGPD, na definição de normativos para o compartilhamento de dados pessoais custodiados pela ANCINE com terceiros, e em processos e ferramentas para melhoria da segurança de informação da Agência.

Meta em 31 de dezembro de 2022: Índice de Adequação à LGPD = 0,90 (Aprimorado).

9 ANEXO I – INVENTÁRIO DE DADOS PESSOAIS

Documento SEI 2219191 e 2219192

10 ANEXO II – RELATÓRIO DE IMPACTO À PROTEÇÃO DADOS PESSOAIS (RIPD)

Documento SEI 2219189 e 2219190

11 ANEXO II – POLÍTICA DE PRIVACIDADE E TERMO DE USO

Documento SEI 2219187 e 2219188